Vendor Landscape: Security Information & Event Management

Optimize IT security management and simplify compliance with SIEM tools.
Introduction

Understand your organization’s requirements for Security Information & Event Management (SIEM) to ensure product selection achieves key goals.

This Research Is Designed For:

✓ Organizations seeking a SIEM solution.

✓ Their SIEM use case may include:
  • IT leaders considering SIEM technology to reduce the cost of meeting ever-increasing compliance requirements.
  • IT leaders looking to enhance the effectiveness of existing IT security operations.
  • Organizations seeking to improve risk management processes.

This Research Will Help You:

✓ Understand the capabilities of SIEM technologies, and their potential use cases.

✓ Differentiate between vendor offerings and identify what aligns with your organization’s requirements.

✓ Shortlist vendors, prepare a Request for Proposal (RFP), and score RFP responses to select a SIEM solution.

✓ Develop an implementation strategy and maximize your investment in SIEM.
Executive Summary

Understand SIEM Trends and Considerations

- Security Information & Event Management (alternatively known as Security Incident & Event Management) technologies have evolved from point solutions into comprehensive systems that allow organizations to optimize any or all of the following important security-related functions:
  - Collection and management of critical system and network log data.
  - Execution of processes in support of regulatory and policy compliance obligations.
  - Identification of information security threats and responses to them.
  - Continuous information security risk management processes.
- Understand your organization’s needs, potential costs, and readiness to undertake a SIEM deployment before taking the leap.

Evaluate SIEM Vendors

- Vendor offerings target these security functions in substantially different ways based on their SIEM product origins, integration with their broader security offerings, architectural deployment options, and specific market focus.
- Map your organization’s immediate and future requirements for SIEM against vendor and product capabilities, and leverage the tools and templates included in this solution set to accelerate selection of a SIEM technology.

Develop a SIEM Implementation Strategy

- Understand options for managed versus self-staffed SIEM implementations and their pros and cons.
- Design a deployment architecture and capture additional implementation and operational costs and benefits, based on addressing your organization’s specific security and compliance requirements.
- Develop a plan for a phased implementation of the selected SIEM product and architecture, ensuring that you realize both short and long-term objectives and benefits.
LogLogic leads a strong group of SIEM offerings

Info-Tech evaluated ten competitors in the SIEM market, including the following notable performers:

**Champions:**
- **LogRhythm** delivers a strong SIEM product with built-in file integrity monitoring and host intrusion detection capabilities.
- **Sensage** offers big data management capabilities to a growing list of impressive clients with stringent security requirements.
- **Q1Labs**, through its acquisition by IBM, has joined its quality SIEM solution with a vendor that can raise its profile substantially.

**Value Award:**
- **SolarWinds** provides a solid feature set at a price point that can’t be beaten, targeted at the small/medium enterprise (SME) market.

**Trend Setter Award:**
- **NitroSecurity**, with its unparalleled set of advanced features, is an appealing solution on its own. With NitroSecurity’s recent acquisition by McAfee (Intel), the future looks bright.

---

**Info-Tech Insight**

1. **Focus on business requirements:**
   Identify the functionality that your organization requires to meet business needs or to justify an investment in SIEM technology.

2. **Consider future requirements:**
   Keep in mind all potential benefits of a SIEM deployment, whether you are focused primarily on simplifying compliance, speeding event management and incident response, or reducing overall risk. But don’t underestimate the effort – and cost – of operating your SIEM.

3. **Go for good enough for you:**
   Align current and future requirements with the capabilities and solution feature-sets of vendors. While Champions stand out among the products reviewed, another solution that better complements other security tools in your arsenal may be a more appropriate choice.
Understand SIEM Trends and Considerations

What’s in this Section:

• What SIEM is – and what it isn’t
• The role of SIEM in managing risk
• Key deciding factors for SIEM
• Assessing the appropriateness of SIEM

Sections:

» Understand SIEM Trends and Considerations
  Evaluate SIEM Vendors
  Develop Your SIEM Implementation Strategy
  Appendices
Understand what SIEM does, and what it doesn’t do

SIEM technology is not a panacea, but adds value by extending visibility across existing information security and system management tools.

**SIEM Tools DO:**

At a minimum, SIEM tools enable IT security organizations to:

- Leverage central log management to simplify correlation, alerting, and reporting of security events;
- Streamline compliance, incident response, and risk management processes;
- Baseline threat levels and normal network security activity;
- Increase efficiency and effectiveness of security and system administrators, internal and external auditors, and senior management involved in risk management;
- Pursue a continuous risk management strategy, prioritizing attention to specific vulnerabilities based on observed threats across multiple control systems.

**SIEM Tools DO NOT:**

Contrary to past hype and misconceptions, SIEM tools **do not**:

- Eliminate the need for other IT security systems – rather, SIEM enhances the value of each of those tools;
- Directly prevent compromises – instead, SIEM provides the cross-system visibility to identify areas of elevated risk and focus security efforts (proactive), and reduces the cost and time for incident response (reactive);
- Eliminate the role of security administrators and operations personnel – SIEM maximizes the value of such staff.
Like every tool, SIEM has limitations; expect too much you will be disappointed

Focus your SIEM implementation where it is most urgently needed, and be realistic about its overall benefits – and costs.

- When clients using SIEM solutions were asked about their expectations for the solution, they almost universally indicated that they had very high expectations prior to deployment.
- Those same clients indicated that their SIEM solution failed to meet expectations in almost every measure.
- Failure to meet expectations should not be held against the tools since in almost every measurable category, the tools delivered Moderately Significant to Significant positive Impact to the enterprise.
- The moral: oversetting expectations can lead to let-down even with deployments that are successful and improve enterprise security, compliance, and overall risk management.

### SIEM Results Generally Fall Short of Expectations

<table>
<thead>
<tr>
<th></th>
<th>Expected Impact</th>
<th>Realized Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced Log Management Effort</td>
<td>4.3</td>
<td>3.9</td>
</tr>
<tr>
<td>Reduced Compliance Management Effort</td>
<td>4.2</td>
<td>3.9</td>
</tr>
<tr>
<td>Reduced Security Management Effort</td>
<td>4.2</td>
<td>4.2</td>
</tr>
<tr>
<td>Increased Threat Visibility</td>
<td>5.1</td>
<td>4.7</td>
</tr>
<tr>
<td>Increased Breach Response</td>
<td>4.8</td>
<td>4.7</td>
</tr>
<tr>
<td>Reduced Enterprise Risk</td>
<td>4.8</td>
<td>4.4</td>
</tr>
</tbody>
</table>

Impact was measured on a scale of 1 (No Impact) to 6 (Very Significant Impact) and averaged across all respondents.
Take stock of the serious threats to systems and the business; ensure threats can be contained or costs can be managed

The cost of a major and persistent system compromise can be substantial. Standalone security tools provide *some* visibility; SIEM tools do much more.

- Several well-publicized breaches in recent years highlight the scale of potential impacts, including:
  - Direct costs for TJX (2007) have *exceeded $250M*.
  - Heartland Payment Systems (2009) has reported *over $140M* in direct costs.
  - Sony (2011) has already booked *$171M in direct costs*.
  - Even security firms have not been immune (*RSA*, 2011).
- Each of these breaches involved repeated system compromises crossing multiple systems over an extended period – precisely the types of activities that are made more visible through SIEM.
- Total costs (direct and indirect) per compromised customer record continue to rise, and in 2009 averaged over *$200 per affected customer*.
  - Costs *per customer* are typically much higher for smaller organizations and smaller-scale breaches than for the massive breaches noted above, as enterprise-wide expenditures are spread across a smaller number of affected accounts.

**Info-Tech Insight**

SIEM alone cannot *eliminate* similar breaches, but enhanced visibility reduces the risk to exposure in many ways:

- Identify sophisticated attacks earlier using event data correlated across multiple systems;
- Support more rapid and more thorough forensics during and after initial incident response;
- Enable continuous feedback from observed threats into security and system controls to achieve optimal protection and reduce the risk of future compromises.

When deployed & operated properly, SIEM can reduce the risk and impact of catastrophic breaches.
Determine how and where SIEM will help you manage risk

Adopting the right SIEM tool depends on what risk-related focus is most important to your organization.

All SIEM tools provide log management functionality – collecting, aggregating, and normalizing log data from diverse sources. Whether the enterprise chooses to move further or not, every organization can benefit from Log Management.

Many organizations look to SIEM primarily as a way to reduce the cost of meeting internal and external/regulatory compliance requirements:
Consolidated logs feed out-of-the-box and custom compliance reports. In some cases, SIEM workflow capabilities add value by tracking mandatory log review processes.

Typically, organizations see both compliance and event management-related benefits as SIEM is integrated into the risk management toolbox.

Other organizations look to SIEM primarily as a means to reduce the effort expended when responding to individual security events and incidents:
Correlated events provide earlier visibility into active threats. Consolidated logs allow more rapid and thorough investigation of events either in progress, or after the fact.

Many organizations take a final step, leveraging the information provided by the SIEM tool to target specific changes to (or investments in) system security and operational controls as a key component of a continuous risk management program.
Compare approaches to managing key information security processes, with or without SIEM

Get a sense of how far you intend to go with SIEM to help focus setting your organization’s requirements. Look for the SIEM you need, and no more.

<table>
<thead>
<tr>
<th>SIEM Approach</th>
<th>Security Management Focus Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Log Management</td>
</tr>
<tr>
<td>No SIEM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Storage, backup, retention, and archival settings must be configured and managed for each key system.</td>
</tr>
<tr>
<td>Basic SIEM (Compliance or Event Focus)</td>
<td>Central log management optimizes the time and cost of managing key system logs, enabling greater opportunities for using such data.</td>
</tr>
<tr>
<td>Advanced SIEM (Compliance and Event Focus)</td>
<td></td>
</tr>
</tbody>
</table>
Be clear about the impact of SIEM-enhanced security visibility

Be prepared for dealing with issues and events that you might have been unaware of without SIEM.

1. **Pre-SIEM**: Information risks and associated security management costs increase over time as new threats appear.

2. **Immediately Post-SIEM**: Increased visibility into extant threats results in increased cost of managing those threats – ignorance can no longer justify inaction.
   - Per event/incident costs will decline through earlier detection opportunities and investigation efficiencies provided by the SIEM tool.
   - Since those threats always existed, and are now being acted upon, overall risk begins to decline.
   - As SIEM-based efficiencies are realized, the cost of managing visible threats returns to baseline levels.

3. **Long-Term Post-SIEM**: Both risk and security costs can be driven down further through feedback from SIEM into technical and procedural controls.
SIEM may make life harder before it makes it easier; if you can’t handle the bump, don’t invest in SIEM

Improving organizational security stance is not an overnight process; SIEM will help but things will get worse before they get better.

1. When first deployed, a SIEM solution will expose the enterprise to all the risk it was missing but that was there anyway. In today’s regulated world, if you’re not prepared to address that increased risk, you’d best just stay unaware.

2. As visibility into risk increases, security spending will, by necessity, increase as new tools and/or time need to be expended to combat identified risks. Most enterprises don’t have unlimited security budgets, so spending initially trails behind threat exposure.

3. As the most serious threats are addressed, risk tapers off fairly quickly. At this point perceived risk and actual risk are being reduced, though levels are likely to be higher than what was perceived for some time.

4. Spending remains higher for longer as solution deployments must be rationalized and staffing levels finalized. Spending begins to go down when the costs associated with breaches and other threats are eliminated.

5. In time, and with concentrated effort, SIEM can enable the enterprise to drive risk and spending to lower levels than were previously experienced. As a side benefit, while risk is being addressed, SIEM is also providing compliance reporting benefits that help in other ways.
Evaluate SIEM Vendors

What’s in this Section:
• Info-Tech’s Vendor Landscape for ten SIEM vendors
• Shortlisting SIEM vendors through scenario analysis
• Developing and executing a SIEM RFP

Sections:
Understand SIEM Trends and Considerations
Evaluate SIEM Vendors
Develop Your SIEM Implementation Strategy
Appendices
Market Overview

**How it got here**


- The space was founded just prior to the 2000s but has yet to catch on in a significant way in the mid-market; even the leading vendors claim less than 2,000 clients each.

- SIEM solutions have historically focused on the largest and most heavily-regulated enterprises, but in recent years vendors have started producing simplified, streamlined, all-in-one solutions aimed at the SME space.

- With the largest security tech firms’ investments, and with a host of innovative independents in the mix, it appears that the future is bright for SIEM.

**Where it’s going**

- Three factors continue to drive awareness and adoption of SIEM: the first is the push into the SME space that began a few years ago, while the second is the increasing amount of regulatory and industry compliance and associated auditing demands. Lastly, there has been an increase in awareness about the prevalence and potential damage from hackers, courtesy of high-profile hacking activities in 2011.

- The space was once dominated by smaller dedicated players, but larger players in the security space have taken centre stage through acquisitions and continued development of their own solutions. SIEM solutions will become more tightly integrated with other security tools as this trend continues.

- Managed SIEM services will take on increasing importance as smaller organizations seek out third-party support to monitor SIEM on a continuous basis.

**Info-Tech Insight**

As the market evolves, capabilities that were once cutting edge become the default and new functionality becomes differentiating. Pay close attention to enhanced correlation and automated response capabilities, and the adoption of truly open standards for event data records and compliance reporting.
SIEM Vendor selection / knock-out criteria: market share, mind share, and platform coverage

- The SIEM space is now over ten years old and through acquisitions, solutions are transitioning from mainly independent, SIEM-focused technology vendors to larger vendors with broad portfolios of security and related technology solutions.

- For this Vendor Landscape, Info-Tech focused on those vendors that offer broad capabilities across multiple platforms and that have a strong market presence and/or reputational presence among small to mid-sized enterprises.

### Included in this Vendor Landscape:

- **ArcSight (HP).** The market leader with enterprise-focused Enterprise Systems Management (ESM), ArcSight continues its push into SME SIEM with its Express system.

- **LogLogic.** An independent SIEM and log management provider with a modular platform that offers flexibility to enterprises of all sizes.

- **LogRhythm.** An independent player with a strong platform that allows for granular management of log data, LogRhythm offers a SIEM solution that can do even more.

- **NitroSecurity (McAfee).** Recently acquired by McAfee, Nitro Security has added its highly capable SIEM solution to McAfee’s broad portfolio.

- **Q1 Labs (IBM).** Formerly the largest independent player in the SIEM space, Q1 Labs QRadar anchors a capable suite of SIEM tools, now under the IBM umbrella.

- **RSA (EMC).** RSA’s fusion of NetWitness and enVision solutions provides a fully integrated platform that offers a traditional SIEM system complete with a focus on identifying advanced threats.

- **Sensage.** One of the smaller vendors in this evaluation and still primarily focused on the large enterprise and highly-regulated verticals.

- **SolarWinds (formerly TriGeo SIM).** SolarWinds has a strong handle on compliance and is looking to become more focused on security over the coming year.

- **Symantec.** The world’s largest security vendor markets a flexible platform to clients of all sizes, enriching raw log data with geolocation and reputation-based information.

- **Trustwave.** Trustwave entered the SIEM market as they have done in other spaces: through acquisition. Trustwave features a wide range of managed services.
## The Table Stakes

### Product Evaluation Criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td>The solution provides basic and advanced feature/functionality.</td>
</tr>
<tr>
<td>Usability</td>
<td>The solution’s dashboard and reporting tools are intuitive and easy to use.</td>
</tr>
<tr>
<td>Affordability</td>
<td>The three year Total Cost of Ownership (TCO) of the solution is economical.</td>
</tr>
<tr>
<td>Architecture</td>
<td>The delivery method of the solution aligns with what is expected within the space.</td>
</tr>
</tbody>
</table>

### Vendor Evaluation Criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viability</td>
<td>Vendor is profitable, knowledgeable, and will be around for the long-term.</td>
</tr>
<tr>
<td>Strategy</td>
<td>Vendor is committed to the space and has a future product and portfolio roadmap.</td>
</tr>
<tr>
<td>Reach</td>
<td>Vendor offers global coverage and is able to sell and provide post-sales support.</td>
</tr>
<tr>
<td>Channel</td>
<td>Vendor channel strategy is appropriate and the channels themselves are strong.</td>
</tr>
</tbody>
</table>

### Criteria Weighting:

#### Features
- 20%

#### Usability
- 20%

#### Architecture
- 20%

#### Affordability
- 40%

#### Product
- 50%

#### Vendor
- 50%

#### Strategy
- 30%

#### Channel
- 25%

#### Reach
- 25%
The Info-Tech SIEM Vendor Landscape

**The Zones of the Landscape**

**Champions** receive high scores for most evaluation criteria and offer excellent value. They have a strong market presence and are usually the trend setters for the industry.

**Market Pillars** are established players with very strong vendor credentials, but with more average product scores.

**Innovators** have demonstrated innovative product strengths that act as their competitive advantage in appealing to niche segments of the market.

**Emerging Players** are newer vendors who are starting to gain a foothold in the marketplace. They balance product and vendor attributes, though score lower relative to market Champions.

For an explanation of how the Info-Tech Vendor Landscape is created, please see [Vendor Landscape Methodology: Information Presentation](#) in the Appendix.
Balance individual strengths to find the best fit for your enterprise

<table>
<thead>
<tr>
<th>Product</th>
<th>Features</th>
<th>Usability</th>
<th>Afford.</th>
<th>Arch.</th>
<th>Overall</th>
<th>Viability</th>
<th>Strategy</th>
<th>Reach</th>
<th>Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArcSight</td>
<td><img src="exemplary.png" alt="Exemplary" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="poor.png" alt="Poor" /></td>
<td><img src="exemplary.png" alt="Exemplary" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="poor.png" alt="Poor" /></td>
<td><img src="poor.png" alt="Poor" /></td>
</tr>
<tr>
<td>LogLogic</td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
</tr>
<tr>
<td>LogRhythm</td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
</tr>
<tr>
<td>NitroSecurity (McAfee)</td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
</tr>
<tr>
<td>Q1 Labs (IBM)</td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
</tr>
<tr>
<td>RSA (EMC)</td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
</tr>
<tr>
<td>Sensage</td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
</tr>
<tr>
<td>SolarWinds</td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
</tr>
<tr>
<td>Symantec</td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
</tr>
<tr>
<td>Trustwave</td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="good.png" alt="Good" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
<td><img src="inadequate.png" alt="Inadequate" /></td>
</tr>
</tbody>
</table>

For an explanation of how the Info-Tech Harvey Balls are calculated, please see [Vendor Landscape Methodology: Information Presentation](#) in the Appendix.
**What is a Value Score?**

The Value Score indexes each vendor’s product offering and business strength **relative to their price point.** It **does not** indicate vendor ranking.

Vendors that score high offer more **value for the cost** (e.g. features, usability, stability, etc.) than the average vendor, while the inverse is true for those that score lower.

Price-conscious enterprises may wish to give the Value Score more consideration than those who are more focused on specific vendor/product attributes.

For an explanation of how Price is determined, please see [Vendor Landscape Methodology: Information Presentation](#) in the Appendix.

For an explanation of how the Info-Tech Value Index is calculated, please see [Vendor Landscape Methodology: Information Presentation](#) in the Appendix.

On a relative basis, SolarWinds maintained the highest Info-Tech **Value Score**™ of the vendor group. Vendors were indexed against SolarWinds’ performance to provide a complete, relative view of their product offerings.

* Vendor was unable to provide cost information based on the scenario provided.

**Average Score: 58**
Table Stakes represent the minimum standard; without these, a product doesn’t even get reviewed

**The Table Stakes**

<table>
<thead>
<tr>
<th>Feature</th>
<th>What it is:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Collection, Aggregation, Normalization (CAN)</td>
<td>Collection from firewall and network logs, IDS logs, Windows server logs, web server logs and various syslog sources.</td>
</tr>
<tr>
<td>Basic Correlations</td>
<td>Out-of-the-box correlation policies for basic CAN data, acting in near real-time.</td>
</tr>
<tr>
<td>Basic Alerting</td>
<td>Logging for all correlated events and alerting via pager/email/text for those that exceed a given threshold or meet specific alert criteria.</td>
</tr>
<tr>
<td>Basic Reporting</td>
<td>Availability of a variety of out-of-the-box reports that can be run on a scheduled and ad hoc basis.</td>
</tr>
</tbody>
</table>

**What Does This Mean?**

The products assessed in this Vendor Landscape™ meet, at the very least, the requirements outlined as Table Stakes.

Many of the vendors go above and beyond the outlined Table Stakes, some even in multiple categories. This section aims to highlight the products’ capabilities *in excess* of the criteria listed here.

If Table Stakes are all you need from your SIEM solution, the only true differentiator for the organization is price. Otherwise, dig deeper to find the best price to value for your needs.
**Scoring Methodology**

Info-Tech scored each vendor’s features offering as a summation of their individual scores across the listed advanced features. Vendors were given 1 point for each feature the product inherently provided. Some categories were scored on a more granular scale with vendors receiving half points.

<table>
<thead>
<tr>
<th>Advanced Features</th>
<th>What we looked for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Data Enrichment</td>
<td>Advanced CAN from Net Flow, Identity, Database, Application, Config &amp; File Integrity data sources.</td>
</tr>
<tr>
<td>Advanced Correlation</td>
<td>Advanced canned policies, user-defined policies, &amp; adaptive/heuristic policies.</td>
</tr>
<tr>
<td>Advanced Alerting</td>
<td>Programmable/customizable alerting responses &amp; injection into native or third-party workflow tools.</td>
</tr>
<tr>
<td>Advanced Reporting</td>
<td>Flexible dashboards, custom reporting capabilities, &amp; ability to export to external reporting infrastructure.</td>
</tr>
<tr>
<td>Forensic Analysis Support</td>
<td>Ability to generate custom data queries with flexible drill-down capabilities.</td>
</tr>
<tr>
<td>Data Management - Security</td>
<td>Granular access controls to system &amp; log data, encryption of SIEM data (in storage &amp; transmission).</td>
</tr>
<tr>
<td>Data Management - Retention</td>
<td>Notable storage capacity, data compression, &amp; inherent hierarchical storage management.</td>
</tr>
<tr>
<td>Unified Compliance Framework</td>
<td>Solution leverages the UCF to enable advanced compliance reporting.</td>
</tr>
<tr>
<td>MITRE Common Event Expression</td>
<td>Solution supports Common Event Expression log formatting.</td>
</tr>
</tbody>
</table>

For an explanation of how Advanced Features are determined, please see [Vendor Landscape Methodology: Information Presentation](#) in the Appendix.
Each vendor offers a different feature set; concentrate on what your organization needs

<table>
<thead>
<tr>
<th>Evaluated Features</th>
<th>Log Data Enrichment</th>
<th>Advanced Correlation</th>
<th>Advanced Alerting</th>
<th>Advanced Reporting</th>
<th>Forensic Analysis</th>
<th>Data - Security</th>
<th>Data - Retention</th>
<th>UCF</th>
<th>MITRE CEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArcSight</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LogLogic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LogRhythm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NitroSecurity (McAfee)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q1 Labs (IBM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA (ESM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SolarWinds</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symantec</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trustwave</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- ✅ = Feature fully present
- 🔴 = Feature partially present/pending
- ⚫ = Feature Absent

For an explanation of how Advanced Features are determined, please see [Vendor Landscape Methodology: Information Presentation](#) in the Appendix.
LogRhythm’s comprehensive SIEM features highly configurable options for the mid-market

**Champion**

- **Product:** LogRhythm SIEM
- **Employees:** 160
- **Headquarters:** Boulder, CO
- **Website:** [LogRhythm.com](https://www.logrhythm.com)
- **Founded:** 2003
- **Presence:** Privately Held

**Overview**

- LogRhythm is one of the few remaining SIEM-specific vendors in the space that has managed to avoid acquisition in an increasingly consolidated market.

**Strengths**

- Highly configurable dashboard that allows users to set up different layouts based on the data they want to see: if all you want to see is data relating to PCI compliance, it’s as easy as making a selection from a drop-down menu.
- LogRhythm includes an integrated File Integrity Monitoring feature, in addition to supporting FIM data feeds from solutions like TripWire and others.

**Challenges**

- Though an automated response can be configured, those customers that wish to manually approve and initiate SmartResponse tasks will need to login to the system via a 3-step authorization process. Future versions will allow for emailed responses instead.
- LogRhythm is participating in neither UCF nor MITRE CEE efforts at this time, which may limit future compliance reporting or security system integration capabilities.

**LogRhythm SIEM**

- **Employees:** 160
- **Headquarters:** Abingdon, UK
- **Website:** Sophos.com
- **Founded:** 1985
- **Presence:** Privately Held

3 year TCO for this solution falls into pricing tier 3, between $5,000 and $10,000.

Pricing provided by vendor.

Champion 3 year TCO for this solution falls into pricing tier 7, between $100,000 and $250,000.

Pricing provided by vendor.
LogRhythm makes advanced features easy to use

What we’re hearing

“It has more features than we have a need for. It’s easy to set up...easy to configure. We had it rolled out very quickly.”

Rik Steven, Manager, Project Management Office, Cara Operations Limited

“One of the things I’d like to see is more batch-style features. If I want to add a log source to agents, I have to do them one at a time.”

Anonymous, Food Services

Info-Tech Recommends:

LogRhythm’s SIEM solution offers both administrator and end-user ease of use and strong feature-functionality. It is pricier than other solutions, but users getting started in SIEM will appreciate its many features and uncomplicated installation.
Sensage is a small company that easily handles the “big data” challenges

**Champion**

<table>
<thead>
<tr>
<th>Product</th>
<th>Sensage Swift</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees</td>
<td>50+</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Redwood City, CA</td>
</tr>
<tr>
<td>Website</td>
<td>Sensage.com</td>
</tr>
<tr>
<td>Founded</td>
<td>2000</td>
</tr>
<tr>
<td>Presence</td>
<td>Privately Held</td>
</tr>
</tbody>
</table>

**Overview**

- Sensage focuses on those clients with large scale data collection, analysis, and storage requirements. Despite the company’s smaller size, it has built a strong network of high-profile channel partners with a solid support organization.

**Strengths**

- Sensage features a purpose-built event data warehouse with massively parallel processing and a patented querying engine that allows it to manage significant alert volumes. It pairs this with customizable dashboards geared to organization needs that are adjustable based on SIEM user roles.
- As part of its Open Security Intelligence initiative, Sensage offers a security analytics repository/community where mature customers can interact with peers to solicit and provide insight and assistance.

**Challenges**

- With a client base in the mid-hundreds, focusing primarily on industry verticals, Sensage is one of the smaller players in this evaluation in terms of overall market share. Increasing its client count is imperative, particularly in the SME space.

**Pricing**

- 3 year TCO for this solution falls into pricing tier 7, between $100,000 and $250,000

- Pricing provided by vendor
Sensage may be small, but its SIEM solution and support offerings are on par with the big companies.

What we’re hearing

“(Sensage) stayed up with us one night when we were fixing an issue. We had implemented a near-line storage solution, and we had performance issues. It was a solution we chose and didn’t do a good job consulting with Sensage on, but they stayed up to fix it even though it wasn’t their issue. They took it on to do the right thing.”

“They need more opportunities to expand in real-time alerting capabilities. Because you can get into the guts area (with the solution), it does take some effort. I’m excited for the new version, (as) they’ve made enhancements in that area.

Jason Stead, Director of Information Security, Choice Hotels

Info-Tech Recommends:

Sensage remains a leader in the space, expanding its capabilities to handle big data and continuing to offer top-notch support for its users. Sensage boasts a small but impressive (and growing) client list. Users wanting a consistently strong solution from a dedicated vendor should consider Sensage.
Q1 Labs QRadar: a quality product line, now part of the IBM portfolio

**Champion**

- **Product:** QRadar SIEM
- **Employees:** 400000 (IBM)
- **Headquarters:** Armonk, NY
- **Website:** Q1Labs.com
- **Founded:** 2001
- **Presence:** NASDAQ: IBM FY10
- **Revenue:** $95.8B

3 year TCO for this solution falls into pricing tier 7, between $100,000 and $250,000

<table>
<thead>
<tr>
<th>Pricing solicited from public sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1</td>
</tr>
<tr>
<td>$1M+</td>
</tr>
</tbody>
</table>

**Overview**

- Q1 Labs was the largest independent player in the SIEM space prior to its acquisition by IBM. Q1 Labs supplements its SIEM play with a broad suite of products to allow for comprehensive security management.

**Strengths**

- The broadest and most comprehensive set of internal reporting capabilities of any product in this test; integration to third-party reporting solutions is usually unnecessary.
- Cleanly integrated set of hierarchical products allows enterprises to grow their security management capabilities in an additive, not rip-and-replace manner.

**Challenges**

- Q1 Labs is participating in neither UCF nor MITRE CEE efforts at this time, which may limit future compliance reporting or security system integration capabilities.

Champion

- **Product:** QRadar SIEM
- **Employees:** 400000 (IBM)
- **Headquarters:** Armonk, NY
- **Website:** Q1Labs.com
- **Founded:** 2001
- **Presence:** NASDAQ: IBM FY10
- **Revenue:** $95.8B

3 year TCO for this solution falls into pricing tier 7, between $100,000 and $250,000

<table>
<thead>
<tr>
<th>Pricing solicited from public sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1</td>
</tr>
<tr>
<td>$1M+</td>
</tr>
</tbody>
</table>

Overview

- Q1 Labs was the largest independent player in the SIEM space prior to its acquisition by IBM. Q1 Labs supplements its SIEM play with a broad suite of products to allow for comprehensive security management.

Strengths

- The broadest and most comprehensive set of internal reporting capabilities of any product in this test; integration to third-party reporting solutions is usually unnecessary.
- Cleanly integrated set of hierarchical products allows enterprises to grow their security management capabilities in an additive, not rip-and-replace manner.

Challenges

- Q1 Labs is participating in neither UCF nor MITRE CEE efforts at this time, which may limit future compliance reporting or security system integration capabilities.
Q1 Labs features strong correlation capabilities for a mid-range price

“… It offers the most amount of functional flexibility. And, second it provides the most effective correlation rule set right out of the box. The Q1 Labs' product simply offered the greatest amount of visibility into our environment with the least amount of headache.

“Our biggest complaints with QRadar are that we struggled when performing certain tasks and felt a number of things simply weren't intuitive from within the user interface.”

Greg Shipley, “Q1Labs QRadar provides effective security event correlation.”

NetworkWorld.com

Info-Tech Recommends:

Q1 Labs’ solution features solid functionality at a mid-range price, but lacks in the interface intuitiveness of some of its competitors. However, users looking for a continually strong player in the SIEM space will find one in Q1 Labs.
LogLogic provides a strong solution with a growing SME focus

**Innovator**

- **Product:** MX
- **Employees:** 165
- **Headquarters:** San Jose, CA
- **Website:** LogLogic.com
- **Founded:** 2002
- **Presence:** Privately Held

**Overview**

- Recently acquired by TIBCO, LogLogic approaches the SIEM space with a clear focus on compliance, applying its Collect-Centralize-Contextualize-Consume philosophy to improve compliance, security, and even operational performance.

**Strengths**

- A feature-rich solution, and one of the few that fully addresses system configuration data as an input source. Coupled with the cleanest interface, this is the solution that delivers the most SIEM capability.
- LogLogic has enhanced its SME strategy with a virtualized version of their product called EVA (Enterprise Virtualized Appliance) that, while cheaper and able to support a smaller number of sources, still retains the strong features of LogLogic’s appliance products.

**Challenges**

- LogLogic is one of the smaller vendors in this review, and only one-third of its client base are SMEs. As one of the remaining independent vendors, growth may be a challenge for the company if its SME strategy does not succeed, with the large enterprise market being targeted by larger security vendors.
- LogLogic’s solutions include a range of architectural options, providing flexibility but also leading to higher than average pricing.

3 year TCO for this solution falls into pricing tier 7, between $100,000 and $250,000

Pricing provided by vendor
LogLogic covers the breadth of SIEM features in solution that is easy to install, and use

Info-Tech Recommends:

LogLogic offers great functionality at a mid-range price. Users able to afford a higher priced solution, those that seek straightforward set-up and configuration, and those seeking broader non-security IT operational visibility will find a solid solution in LogLogic.
NitroSecurity continues to bring a solid SIEM background to a feature-rich solution

**Innovator**

- **Product:** NitroView ESM
- **Employees:** 6737 (McAfee)
- **Headquarters:** Santa Clara, CA
- **Website:** NitroSecurity.com
- **Founded:** 1987
- **Presence:** NASDAQ: ITNC (Intel)

3 year TCO for this solution falls into pricing tier 7, between $100,000 and $250,000

**Overview**


**Strengths**

- The most feature-rich solutions in this roundup, and likely to benefit substantially from McAfee's global reach.
- NitroSecurity falls between the pure-play SIEM providers and the broader security vendors, meaning it has good focus on the space, but isn't solely reliant on SIEM sales for its revenue.
- NitroSecurity, with its new McAfee connections, is the only player in the SIEM space that leverages the UCF and participates in MITRE CEE efforts.

**Challenges**

- NitroSecurity includes virtual appliance deployment options, but these are currently scaled only at smaller enterprises and remote sites; increasing performance will expand their applicability.
- Long-term, McAfee looks to extend its common architecture to include NitroSecurity. For now, SMEs looking for a McAfee centrally-managed system that includes NitroSecurity SIEM will need to wait.
NitroSecurity’s SIEM features a powerful and intuitive interface

Vendor Landscape

Value Index

67
7th out of 10

What we’re hearing

“I’m happy with things like base-lining, notifications and reports, get down to packet level which is one of the coolest things we can do and it’s very fast.”

Senior Security Engineer, Insurance

“IT is a near real-time logging tool that excels at taking gobs and gobs of data, correlates it, creates baselines for that data, with alerting and reporting all in a single pane of glass. My number 1 complaint is that I wish it had real-time tail logging ability for troubleshooting purposes.”

Network Engineer, Food Industry Production

Info-Tech Recommends:

NitroSecurity’s SIEM interface is above and beyond the competition in terms of fluidity and capability to drill down into the data. Users wanting a breadth of features, complete with the most attractive and intuitive interface, will find an ideal solution with NitroSecurity.
SolarWinds is a newer face in the market, but already a strong competitor

**Innovator**

<table>
<thead>
<tr>
<th>Product:</th>
<th>SolarWinds LEM (formerly TriGeo SIM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees:</td>
<td>600+</td>
</tr>
<tr>
<td>Headquarters:</td>
<td>Austin, TX</td>
</tr>
<tr>
<td>Website:</td>
<td>SolarWinds.com</td>
</tr>
<tr>
<td>Founded:</td>
<td>1999</td>
</tr>
<tr>
<td>Presence:</td>
<td>NYSE: SWI FY11: $198M</td>
</tr>
</tbody>
</table>

**Overview**

- SolarWinds has taken TriGeo’s compliance-focused solution and added in operational capabilities for full-featured, but affordable, solution.

**Strengths**

- SolarWinds aims to solve the “enterprise SIEM” problem for the mid-market by offering basic features in reporting, correlations and endpoint coverage, a drag and drop rule builder, and by bringing information to user’s fingertips instead of making them dig deep.
- With a price point that is unmatched by its competitors, SolarWinds offers exceptional value for users without sophisticated SIEM needs.

**Challenges**

- SolarWinds’ focus on supporting compliance requirements is clear; however, they currently lack in advanced security-oriented capabilities.
- SolarWinds LEM lacks internal retention management: though data can be archived to a network share, the general storage limit inherent within the product is 2TB. If a system reaches full storage and external shares are not used, data simply expires out.

3 year TCO for this solution falls into pricing tier 5, between $25,000 and $50,000

Pricing provided by vendor
SolarWinds is a strong contender with its fluid drill down capabilities and remarkable price

Info-Tech Recommends:
Formerly TriGeo, SolarWinds has kept the solution’s solid processing capabilities, and managed to lower the already-best-in-class price. An affordable solution for users looking for a basic SIEM solution, and a growing player in this space.
RSA has a solid solution, but also the most expensive

Market Pillar

Product: enVision

Employees: 40,000+ (EMC)
Headquarters: Bedford, MA
Website: RSA.com
Founded: 1982
Presence: NYSE:EMC
FY10: $20B

Overview

• RSA, the security division of EMC, focused on compliance with its enVision solution. With the recent acquisition of NetWitness, RSA is looking to address the increasing needs of customers for security against advanced threats.

Strengths

• RSA has taken a holistic view of security management and the integration of its three security management platforms (SIEM, DLP, eGRC) is visionary.
• The company is now looking to further integrate NetWitness’ network packet forensics into the enVision platform, creating a product that addresses the long-term focus of compliance, and the short-term view of log management and analytics.

Challenges

• The fusion of the enVision and NetWitness product lines has already begun, but integration efforts may not be fully completed for up to 12 months.
• RSA has the most costly solution of those that were priced out, but new “smart pricing” options may allow more economical pricing for users based on data capacity requirements.
RSA brings a lot to the table, but at a premium cost

Info-Tech Recommends:

RSA’s SIEM product has a solid set of advanced features and comes with tremendous vendor stability; however, it is the most expensive solution. Users able to afford the price and who want a strong vendor can find a good solution with RSA.

What we’re hearing

“The latest security investigation and analytics module based on NetWitness technology called RSA NetWitness Panorama, … allows customers to use NetWitness Decoders to collect and analyze log information along with content of network capture to give users a powerful advantage during an overall security investigation.”


“It enables us to go beyond the typical web interface for monitoring log data. We can now carry out forensic tasks that had always been difficult before.”

Charles Beierle, Director of Information Security, RBFCU

Features

Log Data Enrichment | Advanced Correlation | Advanced Alerting | Advanced Reporting | Forensic Analysis | Data-Security | Data-Retention | UCF | MITRE CEE
---|---|---|---|---|---|---|---|---
🌟 | 🟠 | 🟠 | 🟠 | 🟠 | 🟠 | 🟠 | 🟠 | 🟠

Value Index

33

8th out of 10

Vendor Landscape

Product

---|---|---|---|---
🌟 | 🟠 | 🟠 | 🟠 | 🟠

Vendor

Overall | Via. | Strat. | Reach | Chan.
---|---|---|---|---
🌟 | 🟠 | 🟠 | 🟠 | 🟠
Symantec offers vendor stability and different deployment options

**Market Pillar**

- **Product:** Security Information Manager
- **Employees:** 17,500
- **Headquarters:** Mountain View, CA
- **Website:** Symantec.com
- **Founded:** 1982
- **Presence:** NASDAQ:SYMC
- **FY11:** $6B

**Overview**

- In contrast to most players in the space, Symantec positions its SIEM solution as a security tool first, and compliance tool second. Its integration into other product lines backs this up and makes it a good choice for the security conscious.

**Strengths**

- Symantec offers the broadest base of deployment types – software, hardware, virtual hardware, and managed service offerings, allowing every enterprise to find a fit.
- Security Information Manager is integrated into Symantec’s Global Intelligence Network, meaning system configuration can be adjusted based on more than just local event data.
- Symantec is splitting their product into separately licensable components, so log management can be deployed to feed cloud SIEM services.

**Challenges**

- Symantec misses on a number of advanced features, most notably associated with compliance reporting. However, Symantec does leverage the UCF in its separate Control Compliance Suite, providing its users with a way to supplement their security-focused SIM solutions.

3 year TCO for this solution falls into pricing tier 7, between $100,000 and $250,000

Pricing solicited from public sources
Symantec provides a stable solution, but lacks in innovation

Info-Tech Recommends:

Symantec remains a stable security vendor, but its SIEM solution lacks advanced features. Users able to afford a mid-range price and that want a well-known vendor behind their SIEM product will find that in Symantec.
ArcSight offers both enterprise- and SME-focused SIEM solutions

### Market Pillar

<table>
<thead>
<tr>
<th>Product</th>
<th>Express</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees</td>
<td>324,600 (HP)</td>
</tr>
<tr>
<td>Headquarters</td>
<td>Palo Alto, CA</td>
</tr>
<tr>
<td>Website</td>
<td>ArcSight.com</td>
</tr>
<tr>
<td>Founded</td>
<td>2000</td>
</tr>
<tr>
<td>Presence</td>
<td>NASDAQ: HPQ FY11 Revenue: $127B</td>
</tr>
</tbody>
</table>

---

### Overview

- Acquired by HP in 2010, ArcSight became the most valuable asset in the company’s focused security strategy. ArcSight is the largest player in the SIEM space and has recently expanded its portfolio to be more applicable to the mid-market.

### Strengths

- An architecturally sound solution allowing for widely varying deployment models; the ability to mix and match Collectors and Loggers with a core Express device offers great flexibility.
- Offers the ability to tightly correlate security events to users via IdentityView, an add-on capability that monitors user activity across all accounts, applications, and systems.

### Challenges

- ArcSight has trimmed its impressive enterprise-focused ESM solution to build Express, but in doing so has left out some of ESM’s differentiating advanced capabilities.

---

The vendor declined to provide pricing, and publicly available pricing could not be found.

---

<table>
<thead>
<tr>
<th>$1</th>
<th>$1M+</th>
</tr>
</thead>
</table>

---

Info-Tech Research Group 39
ArcSight offers easy-to-use solutions from a strong vendor

ArcSight started as a leader in the space, but has lost ground as other products have matured. Those familiar with the vendor may want to stick with ArcSight, given its stability.
Trustwave’s strength is in their managed services

**Emerging Player**

- **Product:** Trustwave SIEM
- **Employees:** 650+
- **Headquarters:** Chicago, IL
- **Website:** [Trustwave.com](http://Trustwave.com)
- **Founded:** 1995
- **Presence:** Privately Held

**Overview**

- Trustwave has a strong global presence and strong footing in managed services, offering it for many of its technologies, including its SIEM solution.

**Strengths**

- Trustwave offers a range of managed services, such as self-service allowing clients to conduct their own daily log review and analysis, while leaving building and maintaining the infrastructure, correlation, and normalization in Trustwave’s hands.
- With its strong PCI compliance background, Trustwave’s solution offers PCI Logging Guides. These QSA-developed guidelines allow organizations to rapidly configure their audit/logging settings to address PCI compliance requirements.

**Challenges**

- Trustwave has built its portfolio based on acquisitions, and integration of all of its diverse products proves to be a common issue with this vendor.
- Similarly, Trustwave’s lack of UCF and CEE participation are symptoms of the early stages of its efforts to build an integrated set of security solutions.

3 year TCO for this solution falls into pricing tier 8, between $250,000 and $500,000

Pricing provided by vendor
Trustwave lacks in advanced features but has PCI compliance down to a science

Info-Tech Recommends:

Trustwave’s SIEM solution is basic, but challenging to configure. To be a contender in this space, they will need to determine a way to differentiate themselves feature-wise, or develop more SME focus. Organizations facing only PCI compliance obligations may find Trustwave SIEM a good fit.
Streamline monitoring, alerting, and incident response processes to minimize the cost of individual security events.

Security Event Management relies on strong correlation and deep forensic analysis.

**Why Scenarios?**

In reviewing the products included in each Vendor Landscape™, certain use-cases come to the forefront. Whether those use-cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use-cases as Scenarios, and calls attention to them where they exist.

For an explanation of how Scenarios are determined, please see [Vendor Landscape Methodology: Information Presentation](#) in the Appendix.
Reduce the cost of demonstrating regulatory and policy compliance by simplifying reporting and log review functions.

Compliance capabilities are defined by broad and deep reporting.

### Why Scenarios?

In reviewing the products included in each Vendor Landscape™, certain use-cases come to the forefront. Whether those use-cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use-cases as Scenarios, and calls attention to them where they exist.

<table>
<thead>
<tr>
<th>Exemplary Performers</th>
</tr>
</thead>
<tbody>
<tr>
<td>loglogic</td>
</tr>
<tr>
<td>LogRhythm</td>
</tr>
<tr>
<td>nitrosecurity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Viable Performers</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArcSight</td>
</tr>
<tr>
<td>Labs</td>
</tr>
<tr>
<td>SENSAGE</td>
</tr>
<tr>
<td>solarwinds</td>
</tr>
<tr>
<td>Trustwave</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Adequate Performers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec</td>
</tr>
</tbody>
</table>

For an explanation of how Scenarios are determined, please see [Vendor Landscape Methodology: Information Presentation](#) in the Appendix.
Ensure the reduction of enterprise risk by putting broad-based collection, aggregation, and response abilities to good use

The broadest possible feature-functionality is required for true Risk Reduction.

**Why Scenarios?**

In reviewing the products included in each Vendor Landscape™, certain use-cases come to the forefront. Whether those use-cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use-cases as Scenarios, and calls attention to them where they exist.

For an explanation of how Scenarios are determined, please see [Vendor Landscape Methodology: Information Presentation](#) in the Appendix.
Identify leading candidates with the **SIEM Vendor Shortlist Tool**

The Info-Tech **SIEM Vendor Shortlist Tool** is designed to generate a customized shortlist of vendors based on your key priorities.

This tool offers the ability to modify:

- Overall Vendor vs. Product Weightings
- Individual product criteria weightings:
  - Features
  - Usability
  - Affordability
  - Architecture
- Individual vendor criteria weightings:
  - Viability
  - Strategy
  - Reach
  - Channel
Issue an RFP to ensure SIEM vendors will fit your needs

Use Info-Tech’s **Security Information & Event Management RFP Template** to conduct this critical step in your vendor selection process.

Info-Tech's SIEM RFP Template is populated with critical elements, including:

- The Statement of Work
- Proposal Preparation Instructions
- Scope of Work
- Functional Requirements
- Technical Specifications
- Operations & Support
- Sizing & Implementation
- Vendor Qualifications & References
- Budget & Estimated Pricing
- Vendor Certification
To get the most value out of the RFP process, use the **SIEM RFP Scoring Tool**

A standard & transparent process for scoring individual vendor RFP responses will help ensure that internal team biases are minimized.

**Use Info-Tech’s SIEM RFP Scoring Tool to:**

**Evaluate RFP Responses**
The [Security Information & Event Management RFP Scoring Tool](#) is pre-built with essential criteria complementing the [SIEM RFP Template](#) from the previous slide.

**Accelerate Procurement**
Use the tool to drive the meeting with your procurement department.

---

<table>
<thead>
<tr>
<th>Feature</th>
<th>Requirements Criteria</th>
<th>Name of Vendor 1</th>
<th>Name of Vendor 2</th>
<th>Name of Vendor 3</th>
<th>Name of Vendor 4</th>
<th>Name of Vendor 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAC</td>
<td>The solution supports File Integrity data collection.</td>
<td>Mandatory Yes - Complete</td>
<td>Yes - Complete</td>
<td>Yes - Complete</td>
<td>Yes - Complete</td>
<td>Yes - Complete</td>
</tr>
<tr>
<td>EDR</td>
<td>The solution supports correlation against pre-defined policies.</td>
<td>Mandatory Yes - Partial</td>
<td>Yes - Partial</td>
<td>Yes - Partial</td>
<td>Yes - Partial</td>
<td>Yes - Partial</td>
</tr>
<tr>
<td>CAS</td>
<td>The solution supports correlation against user-defined policies.</td>
<td>Mandatory Yes - Partial</td>
<td>Yes - Partial</td>
<td>Yes - Partial</td>
<td>Yes - Partial</td>
<td>Yes - Partial</td>
</tr>
<tr>
<td>SIEM</td>
<td>The solution supports correlation against adaptively configured</td>
<td>Mandatory Yes - Partial</td>
<td>Yes - Partial</td>
<td>Yes - Partial</td>
<td>Yes - Partial</td>
<td>Yes - Partial</td>
</tr>
</tbody>
</table>
Take charge of vendor demonstrations with a Vendor Demonstration Script

An onsite product demonstration will help enterprise decision-makers better understand the capabilities and constraints of various solutions.

This tool is designed to provide vendors with a consistent set of instructions for demonstrating key scenarios for the SIEM implementation.

The Security Information & Event Management Vendor Demo Script covers:

• Standard and advanced log source and log management/retention configurations.
• Default and custom event correlation and alerting capabilities.
• Default and custom reporting functionality.
• Forensic log analysis and incident management tools.
• Custom dashboard and granular system access features.

Security Information & Event Management (SIEM) Vendor Demo Script

Introduction: How to Use This Tool

This demonstration script template is designed to help the IT department provide a vendor with a consistent set of instructions on how to conduct a demonstration. The demonstration includes descriptions of the key scenarios and includes the following:

1. Introduction to the SIEM solution.
2. Setup and configuration.
3. Demonstration of key scenarios.
4. Q&A session.

Scenario 1 - Log source configurations

Goal: To demonstrate the process of adding and configuring various log data source systems.

1. Adding log sources:
   a. Demonstrate the process of adding a log source to the SIEM system.
   b. Demonstrate the configuration of the log source.
   c. Demonstrate the testing of the log source.

2. Enriched log data sources:
   a. Demonstrate the process of enriching log data sources.
   b. Demonstrate the configuration of enriched log data sources.
   c. Demonstrate the testing of enriched log data sources.

3. Customizing log data source settings:
   a. Demonstrate the process of customizing log data source settings.
   b. Demonstrate the configuration of customized log data sources.
   c. Demonstrate the testing of customized log data sources.

Scenario 2 - Event correlation, alerting, log analysis, and incident management

Goal: To demonstrate product capabilities for event correlation, alerting, and incident management.

1. Event correlation:
   a. Demonstrate the process of correlating events.
   b. Demonstrate the configuration of event correlation rules.
   c. Demonstrate the testing of event correlation rules.

2. Alerting:
   a. Demonstrate the process of setting up alerts.
   b. Demonstrate the configuration of alerting rules.
   c. Demonstrate the testing of alerting rules.

3. Log analysis:
   a. Demonstrate the process of analyzing log data.
   b. Demonstrate the configuration of log analysis rules.
   c. Demonstrate the testing of log analysis rules.

4. Incident management:
   a. Demonstrate the process of managing incidents.
   b. Demonstrate the configuration of incident management rules.
   c. Demonstrate the testing of incident management rules.

5. Compliance:
   a. Demonstrate the process of ensuring compliance.
   b. Demonstrate the configuration of compliance rules.
   c. Demonstrate the testing of compliance rules.

Conclusion:

Thank you for using the Security Information & Event Management Vendor Demo Script. We hope this tool has been helpful in demonstrating the capabilities and constraints of various SIEM solutions.
Develop Your SIEM Implementation Strategy

What’s in this Section:

- SIEM implementation architectures
- Assessing the total cost of SIEM
- Understanding the staffing impacts of SIEM
- Moving forward with your SIEM implementation

Sections:

- Understand SIEM Trends and Considerations
- Evaluate SIEM Vendors
- Develop Your SIEM Implementation Strategy
- Appendices
Getting to a SIEM implementation strategy

Get a handle on overall costs, understand the resource implications, and develop a plan to realize immediate and long-term benefits of SIEM.

• Hard implementation costs:
  ◦ Design and size a SIEM solution that meets operational requirements.
  ◦ Include the costs of additional hardware components.

• Soft implementation costs:
  ◦ Identify and track the resources consumed in system implementation and training.

• Ongoing staffing costs:
  ◦ Understand the immediate and ongoing impact on existing compliance and security management staffing.

• Getting approval and moving ahead:
  ◦ Stay attuned to the decision makers’ requests and grow use of the SIEM tool methodically.
Consider the available SIEM deployment options

Each SIEM appliance model has its own merits and faults.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Appliance</td>
<td>Simplified management maximizes focus on SIEM operations.</td>
<td>Dedicated onboard storage is unavailable for other uses.</td>
</tr>
<tr>
<td></td>
<td>Simplified support – no vendor concerns about underlying hardware.</td>
<td>Scalloplity limited by appliance capabilities.</td>
</tr>
<tr>
<td>Virtual Appliance</td>
<td>Leverages existing server virtualization and shared storage (SAN) investments.</td>
<td>High-performance requirements consume virtual server resources.</td>
</tr>
<tr>
<td></td>
<td>Scalability and resiliency limited only by those environments.</td>
<td>Requires additional virtual server management.</td>
</tr>
<tr>
<td>Software-only Solutions</td>
<td>Allows wider choice of hardware.</td>
<td>Requires dedicated server hardware and ongoing server management.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elevates risk of HW vs. SW finger-pointing during support calls.</td>
</tr>
</tbody>
</table>

Regardless of the choice – or mix – of platforms, don’t forget to plan for log data backup to meet regulatory and internal policy requirements.
Identify constraints for your SIEM architecture

Consider performance, capacity, and regulatory inputs in your design process.

• SIEM vendors offer a variety of centralized and distributed deployment options – sometimes the best design is a mix of both.

• Centralized components typically include log collectors, event correlation engines, and functions including alerting, reporting, and incident management tools.
  ◦ Whether all-in-one or separate but adjacent devices, deploying these components centrally reduces the management burden for SIEM.

• Distributed designs may include single-purpose collectors and combination collector/correlation devices, which can support:
  ◦ Regulatory requirements (e.g. EU Safe Harbour) that restrict offshore movement of private/sensitive data.
  ◦ Performance and scalability needs by aggregating data from log sources at remote sites and offloading event correlation processing.

Info-Tech Insight

Cloud-based SIEM solutions (aka SIEMaaS) are maturing, but have yet to take over the market. Regulatory restrictions may limit the applicability of such services.

In contrast, managed security service provider (MSSP) solutions, in which a third party maintains and monitors a SIEM system housed on customer premises, offer greater promise today:
  • Customer control over sensitive data.
  • Shared access to 24/7 monitoring at a fraction of the cost.
Optimize the SIEM solution design

Understand your current IT environment in order to size the SIEM solution properly and minimize WAN impact.

- SIEM deployments are sized based on two key factors: logging rate and storage capacity.

- Logging rates, or the number of log records that the system can process, are measured in events or messages per second (eps or MPS):
  - Collectors must be sized to handle the peak number of events per second, or risk losing critical log records.
  - **Peak eps** requirements for a SIEM solution are determined by summing the peak logging rates of all source devices. Though it is unlikely that all devices will hit peak rates simultaneously, this provides the capacity to handle elevated logging demands from extraordinary events such as denial of service attacks and malware outbreaks.

- Storage capacity requirements depend on logging rates, but with a little math:
  - All SIEM solutions perform some level of log file compression, typically ranging between a 20 to 40-fold reduction in log file sizes.
  - **Total storage capacity** requirements can be calculated by summing the average daily log file size of each source device, multiplying by the required retention period, and dividing by the SIEM compression rate.
  - Some SIEM solutions allow retention periods to be defined by device (or group of devices), while others establish a single, default retention period.

---

**Info-Tech Insight**

For multi-site deployments, look to distributed components to optimize SIEM and network performance:

- Distributed log collectors:
  - Spread the peak eps load across multiple devices.
  - Compress log data before forwarding on to a central collector, saving considerably on WAN traffic.
Success with SIEM involves more than just the Security team. Make sure all the right parties are engaged up front.

**Project Team Composition**

- Security, network, and system administrators all have substantial involvement:
  - Identifying and configuring log data sources.
  - Defining event severity levels; monitoring, alerting & escalation processes; and reporting formats & schedules.
- Internal auditors and other compliance personnel also play key roles:
  - Designing dashboards and reports to simplify compliance management efforts.
  - Specifying elevated requirements for regulated systems – architectural or procedural.

**Training Considerations**

- Training is critical for project team members and the groups they represent.
- System training is necessary for all those who use SIEM directly (e.g. security operators, compliance auditors); process training is appropriate for those who only use SIEM outputs.
Understand the ongoing staffing impacts, both positive and negative

Examine compliance and incident management savings against increased monitoring costs.

- For incident response staff and supporting system administrators, SIEM is a double-edged sword:
  - Increased incident response efficiencies are countered by increased event visibility, until and unless SIEM-driven improvements are made to key security and system controls.
  - In the short term, this typically means a greater burden on security staff.

- Organizations facing regular and/or diverse regulatory requirements can reduce their associated reporting burdens substantially:
  - In many cases, required reports can be generated automatically and consistently across multiple systems, without burdening the system admins.
  - Many SIEM solutions offer reports on internal SIEM activity. Such reports can be used to demonstrate compliance with various regulatory log review requirements.
    - If this capability is needed, make sure to configure your SIEM system to send links to the reports that will be viewed by system administrators, as opposed to sending the entire report.
    - This forces sysadmins to log into the SIEM solution directly to access reports, which in turn generates the audit record necessary for demonstrating that the logs have been reviewed.
Determine how you intend to staff SIEM monitoring and alerting functions

“Once there is seeing, there must be acting. Otherwise, what is the use of seeing?” (Thich Nhat Hanh, Vietnamese Zen Buddhist Monk)

• **Real-time event monitoring** can be a huge cost driver for SIEM:
  ◦ For organizations lacking a dedicated Security Operations Center (SOC), adding a dedicated 24/7 monitoring capability could equate to an increase of 5 Full Time Equivalents.
  ◦ Consider adding a “best effort” event monitoring responsibility to existing security staff – a 10-20% rise in staffing levels could enable much better incident response outcomes.

• Alternatively, consider a Managed Security Service Provider (MSSP) approach to staffing your SIEM solution:
  ◦ MSSPs can provide 24/7/365 monitoring and alerting at a fraction of the cost of providing the service yourself.
  ◦ Many MSSPs also provide incident response services that can supplement on-staff personnel during off hours.
  ◦ The trade-off: your SIEM data is either stored off-site (with associated bandwidth impacts), or accessible to 3rd parties, or both. Be sure to address these security and confidentiality issues in your MSSP contract.

---

**Info-Tech Insight**

SIEM monitoring through an MSSP can provide cost-effective alternatives for real-time event monitoring:

• MicroAge, an IT services firm, opted for an MSSP to provide on-premise SIEM equipment and remote monitoring services.
• For a monthly fee, MicroAge avoided the capital cost of a SIEM solution supporting 120 log sources.
• In the same monthly fee, MicroAge receives 24/7 real-time event monitoring, with serious events escalated to internal IT staff, at a small fraction of the cost of staffing such a capability internally.

“**You get an alarm system for your network, but you don’t get the cops to go with it.**

- Perry Kuhnen, IT Manager, MicroAge (about SIEM without real-time monitoring)
Factor decision-makers’ concerns into the SIEM proposal

**Perspective matters: position initial SIEM plans based on what’s most important to leadership, and focus on relevant cost reduction opportunities.**

- Where leadership has a strong focus on information risk management, pitching event-focused SIEM is easier:
  - Even without 24/7 monitoring, event-focused SIEM enables risk reduction simply through enhanced visibility.
  - Reducing incident-related costs can offset SIEM investments.
- Where that strong risk focus is missing, compliance-focused SIEM may be the more effective route to approval:
  - Reducing the costs of demonstrating compliance can offset SIEM investments.
  - Leverage enhanced visibility to elevate information risk to a leadership level, and evolve SIEM toward a greater focus on event and risk management.

![Executive Focus on Risk Is Key to SIEM Approval](chart)

Significance was measured on a scale of 1 (No Significance) to 6 (Very High Significance) and averaged across all respondents.
Start modestly, but keep the final objective in mind

Don’t try to execute the whole SIEM vision at once. Learn from early stages, and build capabilities & benefits incrementally.

• Embarking on a SIEM initiative requires a serious investment of time and money. Implementation can be phased in two distinct, but complementary, ways.
  ◦ Phased by SIEM function:
    – Start with a compliance management focus, but explore the benefits of enhanced event visibility or
    – Start with an event management focus, but take advantage of compliance reporting for internal purposes.
    – Once both are implemented, look at continuous risk management opportunities – demonstrated benefits from past experiences might even outweigh the cost of adding 24/7 monitoring.
  ◦ Phased by source system:
    – Start with the most critical systems (key applications, core infrastructure, regulated environments).
    – Expand to other log data sources as the benefits of SIEM are demonstrated for those key assets.
• Mix and match these approaches to minimize initial costs, maximize the benefits delivered, and build additional support for broader SIEM deployments:
  ◦ Later stages may not deliver the same magnitude of benefits, but they involve lower equipment and configuration costs, as they leverage initial investments made in earlier stages.
Appendix

1. Vendor Landscape Methodology: Overview
2. Vendor Landscape Methodology: Product Selection & Information Gathering
3. Vendor Landscape Methodology: Scoring
4. Vendor Landscape Methodology: Information Presentation
5. Vendor Landscape Methodology: Fact Check & Publication
6. Product Pricing Scenario
7. Survey Demographics
Vendor Landscape Methodology: Overview

Info-Tech’s Vendor Landscapes are research materials that review a particular IT market space, evaluating the strengths and abilities of both the products available in that space as well as the vendors of those products. These materials are created by a team of dedicated analysts operating under the direction of a senior subject matter expert over the period of six weeks.

Evaluations weigh selected vendors and their products (collectively “solutions”) on the following eight criteria to determine overall standing:
- Features: The presence of advanced and market-differentiating capabilities.
- Usability: The intuitiveness, power, and integrated nature of administrative consoles and client software components.
- Affordability: The three-year total cost of ownership of the solution.
- Architecture: The degree of integration with the vendor’s other tools, flexibility of deployment, and breadth of platform applicability.
- Viability: The stability of the company as measured by its history in the market, the size of its client base, and its financial performance.
- Strategy: The commitment to both the market-space as well as to the various sized clients (small, mid-sized and enterprise clients).
- Reach: The ability of the vendor to support its products on a global scale.
- Channel: The measure of the size of the vendor’s channel partner program as well as any channel strengthening strategies.

Evaluated solutions are plotted on a standard two by two matrix:
- Champions: Both the product and the vendor receive scores that are above the average score for the evaluated group.
- Innovators: The product receives a score that is above the average score for the evaluated group, but the vendor receives a score that is below the average score for the evaluated group.
- Market Pillars: The product receives a score that is below the average score for the evaluated group, but the vendor receives a score that is above the average score for the evaluated group.
- Emerging Players: Both the product and the vendor receive scores that are below the average score for the evaluated group.

Info-Tech’s Vendor Landscapes are researched and produced according to a strictly adhered to process that includes the following steps:
- Vendor/product selection
- Information gathering
- Vendor/product scoring
- Information presentation
- Fact checking
- Publication

This document outlines how each of these steps is conducted.
Vendor Landscape Methodology: Vendor/Product Selection & Information Gathering

Info-Tech works closely with its client base to solicit guidance in terms of understanding the vendors with whom clients wish to work and the products that they wish evaluated; this demand pool forms the basis of the vendor selection process for Vendor Landscapes. Balancing this demand, Info-Tech also relies upon the deep subject matter expertise and market awareness of its Senior and Lead Research Analysts to ensure that appropriate solutions are included in the evaluation. As an aspect of that expertise and awareness, Info-Tech’s analysts may, at their discretion, determine the specific capabilities that are required of the products under evaluation and include in the Vendor Landscape only those solutions that meet all specified requirements.

Information on vendors and products is gathered in a number of ways via a number of channels.

Initially a request package is submitted to vendors to solicit information on a broad range of topics. The request package includes:

- A detailed survey
- A pricing scenario (see Vendor Landscape Methodology: Price Evaluation and Pricing Scenario below)
- A request for reference clients
- A request for a briefing and, where applicable, guided product demonstration

These request packages are distributed approximately twelve weeks prior to the initiation of the actual research project to allow vendors ample time to consolidate the required information and schedule appropriate resources.

During the course of the research project briefings and demonstrations are scheduled (generally for one hour each session, though more time is scheduled as required) to allow the analyst team to discuss the information provided in the survey, validate vendor claims, and gain direct exposure to the evaluated products. Additionally, an end-user survey is circulated to Info-Tech’s client base and vendor-supplied reference accounts are interviewed to solicit their feedback on their experiences with the evaluated solutions and with the vendors of those solutions.

These materials are supplemented by a thorough review of all product briefs, technical manuals, and publicly available marketing materials about the product as well as about the vendor itself.

Refusal by a vendor to supply completed surveys or submit to participation in briefings and demonstrations does not eliminate a vendor from inclusion in the evaluation. Where analyst and client input has determined that a vendor belongs in a particular evaluation, they will be evaluated as best as possible based on publicly available materials only. Because these materials are not as comprehensive as a survey, briefing, and demonstration, the possibility exists the evaluation may not be as thorough or accurate. Because Info-Tech includes vendors regardless of vendor participation, it is always in the vendor’s best interest to participate fully.

All information is recorded and catalogued to facilitate scoring and for future reference, as required.
Vendor Landscape Methodology: Scoring

Once all information has been gathered and evaluated for all vendors and products, the analyst team moves to scoring. All scoring is performed at the same time so as to ensure as much consistency as possible. Each criterion is scored on a 10 point scale, though the manner of scoring for criteria differs slightly:

• Features is scored via **Cumulative Scoring**.
• Affordability is scored via **Scalar Scoring**.
• All other criteria are scored via **Base5 Scoring**.

In Cumulative Scoring, a single point is assigned to each evaluated feature that is regarded as being fully present, a half point to each feature that is partially present or pending in an upcoming release, and zero points to features that are deemed to be absent. The assigned points are summed and normalized to a value out of 10. For example, if a particular Vendor Landscape evaluates 8 specific features in the Feature Criteria, the summed score out of 8 for each evaluated product would be multiplied by 1.25 to yield a value out of 10.

In Scalar Scoring, a score of 10 is assigned to the lowest cost solution and a score of 1 is assigned to the highest cost solution. All other solutions are assigned a mathematically determined score based on their proximity to/distance from these two endpoints. For example, in an evaluation of three solutions, where the middle cost solution is closer to the low end of the pricing scale it will receive a higher score and where it is closer to the high end of the pricing scale it will receive a lower score; depending on proximity to the high or low price it is entirely possible that it could receive either 10 points (if it is very close to the lowest price) or 1 point (if it is very close to the highest price). Where pricing cannot be determined (vendor does not supply price and public sources do not exist), a score of 0 is automatically assigned.

In Base5 scoring a number of sub-criteria are specified for each criterion (for example Longevity, Market Presence, and Financials are sub-criteria of the Viability criterion) and each one is scored on the following scale:

5 - The product/vendor is exemplary in this area (nothing could be done to improve the status).
4 - The product/vendor is good in this area (small changes could be made that would move things to the next level).
3 - The product/vendor is adequate in this area (small changes would make it good, more significant changes are required to be exemplary).
2 - The product/vendor is poor in this area (this is a notable weakness and significant work is required).
1 - The product/vendor is terrible/fails in this area (this is a glaring oversight and a serious impediment to adoption).

The assigned points are summed and normalized to a value out of 10 as explained in Cumulative Scoring, above.

Scores out of 10, known as Raw scores, are transposed as-is into Info-Tech’s Vendor Landscape Shortlisting Tool which automatically determines Vendor Landscape positioning (see **Vendor Landscape Methodology: Information Presentation - Vendor Landscape**, below), Criteria Score (see **Vendor Landscape Methodology: Information Presentation - Criteria Score**, below) and Value Index (see **Vendor Landscape Methodology: Information Presentation - Value Index**, below).
Vendor Landscape Methodology: Information Presentation – Vendor Landscape

Info-Tech’s Vendor Landscape is a two-by-two matrix that plots solutions based on the combination of Product score and Vendor score. Placement is not determined by absolute score, but by relative score. Relative scores are used to ensure a consistent view of information and to minimise dispersion in developing markets while enhancing dispersion in commodity markets to allow for quick visual analysis by clients.

Relative scores are calculated as follows:

1. Raw scores are transposed into the Info-Tech Vendor Landscape Shortlisting Tool (for information on how Raw scores are determined, see Vendor Landscape Methodology: Scoring, above).
2. Each individual criterion Raw score is multiplied by the pre-assigned weighting factor for the Vendor Landscape in question. Weighting factors are determined prior to the evaluation process to eliminate any possibility of bias. Weighting factors are expressed as a percentage such that the sum of the weighting factors for the Vendor criteria (Viability, Strategy, Reach, Channel) is 100% and the sum of the Product criteria (Features, Usability, Affordability, Architecture) is 100%.
3. A sum-product of the weighted Vendor criteria scores and of the weighted Product criteria scores is calculated to yield an overall Vendor score and an overall Product score.
4. Overall Vendor scores are then normalized to a 20 point scale by calculating the arithmetic mean and standard deviation of the pool of Vendor scores. Vendors for whom their overall Vendor score is higher than the arithmetic mean will receive a normalized Vendor score of 11-20 (exact value determined by how much higher than the arithmetic mean their overall Vendor score is), while vendors for whom their overall Vendor score is lower than the arithmetic mean will receive a normalized Vendor score of between 1 and 10 (exact value determined by how much lower than the arithmetic mean their overall Vendor score is).
5. Overall Product score are normalized to a 20 point scale according to the same process.
6. Normalized scores are plotted on the matrix, with Vendor score being used as the x-axis, and Product score being used as the y-axis.
Vendor Landscape Methodology: Information Presentation – Criteria Scores (Harvey Balls)

Info-Tech’s Criteria Scores are visual representations of the absolute score assigned to each individual criterion as well as of the calculated overall Vendor and Product scores. The visual representation used is Harvey Balls.

Harvey Balls are calculated as follows:

1. Raw scores are transposed into the Info-Tech Vendor Landscape Shortlisting Tool (for information on how Raw scores are determined, see Vendor Landscape Methodology: Scoring, above).
2. Each individual criterion Raw score is multiplied by a pre-assigned weighting factor for the Vendor Landscape in question. Weighting factors are determined prior to the evaluation process, based on the expertise of the Senior or Lead Research Analyst. to eliminate any possibility of bias. Weighting factors are expressed as a percentage such that the sum of the weighting factors for the Vendor criteria (Viability, Strategy, Reach, Channel) is 100% and the sum of the Product criteria (Features, Usability, Affordability, Architecture) is 100%.
3. A sum-product of the weighted Vendor criteria scores and of the weighted Product criteria scores is calculated to yield an overall Vendor score and an overall Product score.
4. Both overall Vendor score/overall Product score as well as individual criterion Raw scores are converted from a scale of 1-10 to Harvey Ball scores on a scale of 0-4 where exceptional performance results in a score of 4 and poor performance results in a score of 0 (zero).
5. Harvey Ball scores are converted to Harvey Balls as follows:
   - A score of 4 becomes a full Harvey Ball.
   - A score of 3 becomes a three-quarter full Harvey Ball.
   - A score of 2 becomes a half full Harvey Ball.
   - A score of 1 becomes a one-quarter full Harvey Ball.
   - A score of 0 (zero) becomes an empty Harvey Ball.
6. Harvey Balls are plotted by solution in a chart where rows represent individual solutions and columns represent overall Vendor/overall Product as well as individual criteria. Solutions are ordered in the chart alphabetically by vendor name.
Vendor Landscape Methodology: Information Presentation – Feature Ranks (Stop Lights)

Info-Tech’s Feature Ranks are visual representations of the presence/availability of individual features that collectively comprise the Features criterion. The visual representation used is Stop Lights.

Stop Lights are determined as follows:

1. A single point is assigned to each evaluated feature that is regarded as being fully present, a half point to each feature that is partially present or pending in an upcoming release, and zero points to features that are deemed to be fully absent.
   - Fully present means all aspects and capabilities of the feature as described are in evidence.
   - Fully absent means no aspects or capabilities of the feature as described are in evidence.
   - Partially present means some, but not all, aspects and capabilities of the feature as described are in evidence OR all aspects and capabilities of the feature as described are in evidence but only for some models in a line.
   - Pending means all aspects and capabilities of the feature as described are anticipated to be in evidence in a future revision of the product and that revision is to be released within the next 12 months.

2. Feature scores are converted to Harvey Balls as follows:
   - Full points become a Green light.
   - Half points become a Yellow light.
   - Zero points become a Red light.

3. Stop Lights are plotted by solution in a chart where rows represent individual solutions and columns represent individual features. Solutions are ordered in the chart alphabetically by vendor name.

For example, a set of applications is being reviewed and a feature of “Integration with Mobile Devices” that is defined as “availability of dedicated mobile device applications for iOS, Android, and BlackBerry devices” is specified. Solution A provides such apps for all listed platforms and scores “Green”, solution B provides apps for iOS and Android only and scores “Yellow”, while solution C provides mobile device functionality through browser extensions, has no dedicated apps, and so scores “Red”.

<table>
<thead>
<tr>
<th>Features</th>
<th>Feature 1</th>
<th>Feature 2</th>
<th>Feature 3</th>
<th>Feature 4</th>
<th>Feature 5</th>
<th>Feature 6</th>
<th>Feature 7</th>
<th>Feature 8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
</tbody>
</table>

Green means a feature is fully present, Red fully absent, Yellow shows partial availability (such as in some models in a line).
Info-Tech’s Value Index is an indexed ranking of solution value per dollar as determined by the Raw scores assigned to each criteria (for information on how Raw scores are determined, see Vendor Landscape Methodology: Scoring, above).

Value scores are calculated as follows:

1. The Affordability criterion is removed from the overall Product score and the remaining Product score criteria (Features, Usability, Architecture) are reweighted so as to retain the same weightings relative to one another while still summing to 100%. For example, if all four Product criteria were assigned base weightings of 25%, for the determination of the Value score Features, Usability, and Architecture would be reweighted to 33.3% each to retain the same relative weightings while still summing to 100%.

2. A sum-product of the weighted Vendor criteria scores and of the reweighted Product criteria scores is calculated to yield an overall Vendor score and a reweighted overall Product score.

3. The overall Vendor score and the reweighted overall Product score are then summed and this sum is multiplied by the Affordability Raw score to yield an interim Value score for each solution.

4. All interim Value scores are then indexed to the highest performing solution by dividing each interim Value score by the highest interim Value score. This results in a Value score of 100 for the top solution and an indexed Value score relative to the 100 for each alternate solution.

5. Solutions are plotted according to Value score, with the highest scorer plotted first, and all remaining scores plotted in descending numerical order.

Where pricing is not provided by the vendor and public sources of information cannot be found, an Affordability Raw score of zero is assigned. Since multiplication by zero results in a product of zero, those solutions for which pricing cannot be determined receive a Value score of zero. Because Info-Tech assigns a score of zero where pricing is not available, it is always in the vendor’s best interest to provide accurate and up to date pricing.
Vendor Landscape Methodology: Information Presentation – Price Evaluation

Info-Tech’s Price Evaluation is a tiered representation of the 3 year Total Cost of Ownership (TCO) of a proposed solution. Info-Tech uses this method of communicating pricing information to provide high-level budgetary guidance to its end-user clients while respecting the privacy of the vendors with whom it works. The solution TCO is calculated and then represented as belonging to one of ten pricing tiers.

Pricing tiers are as follows:
1. Between $1 and $2,500.
2. Between $2,500 and $5,000.
3. Between $5,000 and $10,000.
4. Between $10,000 and $25,000.
5. Between $25,000 and $50,000.
6. Between $50,000 and $100,000.
7. Between $100,000 and $250,000.
8. Between $250,000 and $500,000.
9. Between $500,000 and $1,000,000.
10. Greater than $1,000,000.

Where pricing is not provided, Info-Tech makes use of publicly available sources of information to determine a price. Because these sources are not official price lists, the possibility exists that they may be inaccurate or outdated, and so the source of the pricing information is provided. Because Info-Tech publishes pricing information regardless of vendor participation, it is always in the vendor’s best interest to supply accurate and up to date information.

Info-Tech’s Price Evaluations are based on pre-defined pricing scenarios (see Product Pricing Scenario, below) to ensure as accurate a comparison as possible between evaluated solutions. Pricing scenarios describe a sample business and solicit guidance as to the appropriate product/service mix required to deliver the specified functionality, the list price for those tools/services, as well as three full years of maintenance and support.

Price Evaluation

Call-out bubbles indicate within which price tier the 3 year TCO for the solution falls, provides the brackets of that price tier, and links to the graphical representation.

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000

The scale along the bottom indicates that the graphic as a whole represents a price scale with a range of $1 to $1M+, while the notation indicates whether the pricing was supplied by the vendor or derived from public sources.

Pricing solicited from public sources
Vendor Landscape Methodology: Information Presentation – Scenarios

Info-Tech’s Scenarios highlight specific use cases for the evaluated solution to provide as complete (when taken in conjunction with the individual written review, Vendor Landscape, Criteria Scores, Feature Ranks and Value Index) a basis for comparison by end user clients as possible.

Scenarios are designed to reflect tiered capability in a particular set of circumstances. Determination of the Scenarios in question is at the discretion of the analyst team assigned to the research project. Where possible Scenarios are designed to be mutually exclusive and collectively exhaustive, or at the very least hierarchical such that the tiers within the Scenario represent a progressively greater or broader capability.

Scenario ranking is determined as follows:

1. The analyst team determines an appropriate use case.
   
   For example:
   
   • Clients that have a multinational presence and require vendors to provide 4 hour on-site support.

2. The analyst team establishes the various tiers of capability.
   
   For example:
   
   • Presence in Americas.
   • Presence in EMEA.
   • Presence in APAC.

3. The analyst team reviews all evaluated solutions and determines which ones meet which tiers of capability.
   
   For example:
   
   • Presence in Americas – Vendor A, Vendor C, Vendor E
   • Presence in EMEA – Vendor A, Vendor B, Vendor C
   • Presence in APAC – Vendor B, Vendor D, Vendor E

4. Solutions are plotted on a grid alphabetically by vendor by tier. Where one vendor is deemed to be stronger in a tier than other vendors in the same tier, they may be plotted non-alphabetically.
   
   For example:
   
   • Vendor C is able to provide 4 hour on-site support to 12 countries in EMEA while Vendor s A and B are only able to provide 4 hour on-site support to 8 countries in EMEA; Vendor C would be plotted first, followed by Vendor A, then Vendor B.
Vendor Landscape Methodology: Information Presentation – Vendor Awards

At the conclusion of all analyses, Info-Tech presents awards to exceptional solutions in three distinct categories. Award presentation is discretionary; not all awards are extended subsequent to each Vendor landscape and it is entirely possible, though unlikely, that no awards are presented.

Awards categories are as follows:

- **Champion Awards** are presented to those solutions, and only those solutions, that land in the Champion zone of the Info-Tech Vendor Landscape (see Vendor Landscape Methodology: Information Presentation - Vendor Landscape, above). If no solutions land in the champion zone, no Champion Awards are presented. Similarly, if multiple solutions land in the champion zone, multiple Champion Awards are presented.

- **Trend Setter Awards** are presented to those solutions, and only those solutions, that are deemed to include the most original/inventive product/service, or the most original/inventive feature/capability of a product/service. If no solution is deemed to be markedly or sufficiently original/inventive, either as a product/service on the whole or by feature/capability specifically, no Trend Setter Award is presented. Only one Trend Setter Award is available for each Vendor Landscape.

- **Best Overall Value Awards** are presented to those solutions, and only those solutions, that are ranked highest on the Info-Tech Value Index (see Vendor Landscape Methodology: Information Presentation – Value Index, above). If insufficient pricing information is made available for the evaluated solutions such that a Value Index cannot be calculated, no Best Overall Value Award will be presented. Only one Best Overall Value Award is available for each Vendor Landscape.
Vendor Landscape Methodology: Fact Check & Publication

Info-Tech takes the factual accuracy of its Vendor Landscapes, and indeed of all of its published content, very seriously. To ensure the utmost accuracy in its Vendor Landscapes, we invite all vendors of evaluated solutions (whether the vendor elected to provide a survey and/or participate in a briefing or not) to participate in a process of Fact Check.

Once the research project is complete and the materials are deemed to be in a publication ready state, excerpts of the material specific to each vendor’s solution are provided to the vendor. Info-Tech only provides material specific to the individual vendor’s solution for review encompassing the following:

- All written review materials of the vendor and the vendor’s product that comprise the evaluated solution.
- Info-Tech’s Criteria Scores / Harvey Balls detailing the individual and overall Vendor / Product scores assigned.
- Info-Tech’s Feature Rank / Stop Lights detailing the individual feature scores of the evaluated product.
- Info-Tech’s Value Index ranking for the evaluated solution.
- Info-Tech’s Scenario ranking for all considered scenarios for the evaluated solution.

Info-Tech does not provide the following:

- Info-Tech’s Vendor Landscape placement of the evaluated solution.
- Info-Tech’s Value Score for the evaluated solution.
- End-user feedback gathered during the research project.
- Info-Tech’s overall recommendation in regard to the evaluated solution.

Info-Tech provides a one-week window for each vendor to provide written feedback. Feedback must be corroborated (be provided with supporting evidence) and where it does, feedback that addresses factual errors or omissions is adopted fully while feedback that addresses opinions is taken under consideration. The assigned analyst team makes all appropriate edits and supplies an edited copy of the materials to the vendor within one week for final review.

Should a vendor still have concerns or objections at that time, they are invited to a conversation, initially via email but as required and deemed appropriate by Info-Tech subsequently via telephone, to ensure common understanding of the concerns. Where concerns relate to ongoing factual errors or omissions they are corrected under the supervision of Info-Tech’s Vendor Relations personnel. Where concerns relate to ongoing differences of opinion they are again taken under consideration with neither explicit not implicit indication of adoption.

Publication of materials is scheduled to occur within the six weeks immediately following the completion of the research project, but does not occur until the Fact Check process has come to conclusion and under no circumstances are “pre-publication” copies of any materials made available to any client.
Product Pricing Scenario

A mid-level retailer with corporate offices on the US west coast, east coast, and Ireland is looking to implement a SIEM solution. The company employs 2200 people. The firm is interested in reducing the effort associated with monitoring, alerting, and responding to security events at the Endpoint, Network, and Datacenter levels. The firm also has 100 retail outlets scattered throughout the US and Europe however all stores are franchised and so out of scope.

The corporate office breakdown is as follows:

US West Coast (Head Office)
Employing 1600 people (70% of total staff), the west coast office holds Sales, Finance, Strategy, Marketing, Buyers, and the majority of IT. The IT staff here consists of 45 employees, 3 of which are dedicated security professionals consisting of 1 Security Manager and 2 Security Analysts.

US East Coast (Satellite)
Employing 200 people (10% of total staff), the east coast office holds solely Sales and Marketing department.

Ireland (Satellite)
Employing 400 people (20% of total staff), the Ireland office employs Buyers and Manufacturing and also a DR facility. Manufacturing consists of 300 employees. The company’s remaining 5 IT staff are located here though none have dedicated security responsibilities.

The expected solution capabilities are as follows:

- The organization described in the pricing scenario is interested primarily in reducing the cost of demonstrating compliance with financial and privacy-related regulations, enhancing visibility of typical external and internal threats, and simplifying the forensic effort associated with event/incident response. Advanced persistent threats are a lesser, tangential concern.
- The anticipated volume & complexity of ad hoc queries against logged and correlated event data is fairly small, driven primarily by incident response efforts and gaps (if any exist) in canned compliance reports.
- The SIEM product is expected to be used regularly by 4 IT staff (the Security Manager and 2 Analysts at the head office, as well as one of the IT staff at the Ireland satellite office), with additional dashboard-/report-level access for 4 users (2 in compliance/audit and 2 in IT management/executive).
Product Pricing Scenario, continued

In terms of the IT infrastructure of the organization, consider the following:

General Infrastructure
- Internal network is one gigabit throughout.
- Redundant core routers at all 3 facilities.
- Distribution switches: 80 at Head Office, 10 at East Coast, 20 in Ireland.
- Primarily Microsoft – 70% Virtualized.
- 4 Domain servers (2 at Head Office, 1 at each of the other offices).
- HA production virtual server cluster at Head Office + separate dev and QA virtual servers in Ireland (also used for DR purposes).
- Oracle DB on HP-UX dual servers (non-virtual) at the US West Coast office, and a single instance in Ireland.
- Exchange 2010 (2 servers).
- SharePoint 2010 (single server).
- 700 laptops running Windows 7; 1200 desktops also running Windows 7.
- Blackberry is the standard corporate mobile device (with a single BES server), but iOS and Android phones and tablets are allowed to connect via a guest wireless network.
- Running a virtualized VOIP system as opposed a traditional PBX.

Security Infrastructure
- Gateway firewalls at each site.
- Endpoint & Gateway anti-malware.
- Endpoint encryption is implemented on all laptops.
- No IDPS or content filtering.

Data Sources/Volume
- 125 log sources in the US, 27 in Ireland (+some room for growth = 150/50)
- <5K eps
- EU Data Security requirement.
Industry

9. Wholesale/Retail: 7%
8. Government: 12%
7. Trans/Utilities/Comms: 21%
6. Healthcare: 14%
5. Financial Services: 12%
4. Education: 17%
3. Manufacturing: 10%
1. Business Services: 7%

N = 42
Revenue

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1B+</td>
<td>8%</td>
</tr>
<tr>
<td>$500M–1B</td>
<td>6%</td>
</tr>
<tr>
<td>$100M–500M</td>
<td>17%</td>
</tr>
<tr>
<td>$50M–100M</td>
<td>8%</td>
</tr>
<tr>
<td>$25–50M</td>
<td>23%</td>
</tr>
<tr>
<td>$10–25M</td>
<td>8%</td>
</tr>
<tr>
<td>$5–10M</td>
<td>4%</td>
</tr>
<tr>
<td>$1–5M</td>
<td>8%</td>
</tr>
<tr>
<td>$0–1M</td>
<td>17%</td>
</tr>
</tbody>
</table>
## FTEs

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. 5001+</td>
<td>19%</td>
</tr>
<tr>
<td>7. 2501-5000</td>
<td>6%</td>
</tr>
<tr>
<td>6. 1001-2500</td>
<td>10%</td>
</tr>
<tr>
<td>5. 501-1000</td>
<td>15%</td>
</tr>
<tr>
<td>4. 251-500</td>
<td>15%</td>
</tr>
<tr>
<td>3. 101-250</td>
<td>15%</td>
</tr>
<tr>
<td>2. 51-100</td>
<td>12%</td>
</tr>
<tr>
<td>1. 1-50</td>
<td>8%</td>
</tr>
</tbody>
</table>

*N = 48*
IT Employees

- 11,5001+: 8%
- 10,2501-5000: 2%
- 9,1001-2500: 2%
- 8,501-1000: 4%
- 7,251-500: 6%
- 6,101-250: 4%
- 5,51-100: 10%
- 4,26-50: 10%
- 3,11-25: 12%
- 2,6-10: 10%
- 1,1-5: 29%

N = 48