FROST & SULLIVAN

BLUE COAT

2016 Global
Network Security Forensics
Market Leadership Award
Contents

Background and Company Performance ................................................................. 3

   Industry Challenges ......................................................................................... 3

   Conclusion Market Leadership of Blue Coat Systems ....................................... 4

   Conclusion ....................................................................................................... 9

Significance of Market Leadership ....................................................................... 10

Understanding Market Leadership ..................................................................... 10

Key Performance Criteria ................................................................................... 11

The Intersection between 360-Degree Research and Best Practices Awards .......... 12


About Frost & Sullivan ....................................................................................... 14
Background and Company Performance

Industry Challenges

Network security forensics is a simultaneously misunderstood and under-appreciated technology. The vendors that offer network security forensics would prefer to frontload their messaging that their platforms offer “continuous forensics.” Continuous forensics would be the idea that endpoint visibility, behavioral analytics, and established rules and performance parameters occur on the same platform. In theory, any type of anomaly on an enterprise network could be detected and malicious attacks thwarted in real time; a lofty goal given the current cyber environment.

However, the role of network security forensics is not secondary to continuous forensics. Therefore, the challenge for network forensic security vendors is two-fold: the vendors must prove their platforms are providing protection, and they need to initiate a comprehensive investigation with maximum visibility if something does go awry. The messages are not in conflict because malicious adversaries are sophisticated and cunning. Sources of security breaches are numerous including malware, compromised credentials, insider attacks, physical theft, and software updates in operating systems, applications, or server configurations. Network security teams\(^1\) must accept that they will have to do everything in their power to prevent a cyber attack, and once thwarted, they will have to work very diligently to understand what happens if a breach does occur.

Thankfully, the practices needed to protect the network and the procedures that are used in a post-breach investigation are similar if not the same. Key to continuous network monitoring is the ability for a network security team to look at security incidents in real-time, or at least near real-time. Security tools are designed to give a network security team notice of anomalies that are indicative of malicious behavior; such anomalies can be any number of events including the discovery of an unknown or blacklisted binary, suspicious end user activity, unexpected activities within files, or a change in network performance.

The most important feature of security incident or post-breach forensic investigations is the ability to provide contextual understanding to metadata. When an alarm is sounded, a whole range of possibilities are in play from false alarms and benign security breaches to breaches that can be easily remediated or full-blown “katy-bar-the-door” events when exfiltration is happening.

\(^1\) Network security team is used broadly in this report. It could be taken to mean a singular IT/security administrator, an on-premises security team, a security operations center (SOC), or a manager professional security service.
The context morphs data into intelligence. “Context” results from the correlation of end users/endpoints, flow data, traffic patterns, applications, and files. Metadata is the foundation upon which context is created. Applied analytics can include the value of a file, or the credentials of an end user, and the severity of a threat (risk management) to provide additional context. The quality of continuous monitoring and of network security forensics is the ability to correlate as much data as possible, and the ability to present the information quickly and purposefully.

Network security forensics have two key distinguishing characteristics: the investigation is going to be (1) post-breach and going to be (2) manual. Instead of looking at metadata in such a way as to dismiss or further investigate a threat, the post-breach investigation is more granular because a breach is occurring and must be mitigated. The emphasis of the investigation moves from malware and anomaly detection to analytics, flow data, and packet inspection. The Blue Coat Security Analytics platform operates exceptionally on both levels; however, in this analysis Frost & Sullivan is focusing more acutely on Blue Coat’s market leading 'post breach' capabilities.

**Network Security Forensics Market Leadership**

Network security forensics products have technology roots from:

- Traditional network security forensics and packet capture
- Network recorders
- Application performance monitoring and application aware network performance monitoring (APM and AANPM)
- Security information and event management (SIEM)
- Continuous monitoring

However, network security forensics is a delicate term because many security platforms will claim to have forensic capabilities. These characteristics distinguish a network security forensics tool (making these different than simply endpoint protection tools, SIEM, antivirus, or other threat detection platforms).

1. **Tooling** - Network forensic tools are designed to help a security analyst investigate a post-breach incident manually.

2. **Session replay** - If a breach occurs, a forensic analysis must be able to reconstruct the event. The degree of fidelity matters.

3. **Packet capture** - A network security forensics investigation must include, at a minimum, packet header data. Full packet capture provides the most visibility and truest fidelity, although, in many cases, storage limitations may make the request
for the full packet recall challenging.

4. **Log metadata required** - Types of log metadata include syslog, internal mapping, Dynamic Host Configuration Protocol (DHCP), the Display Log (DSPLOG) which shows a system’s history log, destination IP address, and packet header information. Network behavioural anomaly detection (NBAD) is a highly useful and highly prevalent capability.

5. **Time stamping capabilities** - Events have to have a logical time sequence. This seemingly obvious, but benign technical capability is difficult to achieve over multiple locations or within a cloud environment.

6. **Remediation** - A forensics investigation must be conducted in such a way that the conclusion of an investigation leads to what must be done to remediate the incident.

In a recent study conducted by Frost & Sullivan\(^2\), the 2015 global network security forensics market was estimated to have achieved $1.12 billion in licensing and appliances. Blue Coat’s offering not only excelled in the requirements for inclusion in this market, it was also the global revenue leader in this $1.12 billion market.

**Growth Strategy Excellence**

In May 2013, Blue Coat Systems acquired Solera Networks. At the time of purchase, Frost & Sullivan believes the Solera Networks DeepSee platform was the most widely used network security forensics platform\(^3\). The DeepSee dashboard provided visibility into IP/endpoints, country origin, social personas, file names and activity, Web servers contacted, and other customizable options. DeepSee was capable of full packet capture and full replay fidelity at up to 10 Gbps.

Blue Coat Systems has several cyber defense technologies in addition to incident response and network forensics including advanced Web security, encrypted traffic management, advanced threat protection, and network performance optimization.

---


\(^3\) The 2015 network security forensics report is the first issued by Frost & Sullivan. We have every reason to believe that the DeepSee platform was the most commonly used network forensics platform in 2013, but did not calculation 2013 market shares.
BlueCoat Security Analytics includes incident detection, network performance, sandbox integration, deep packet inspection, and network security forensics on the same platform. The integration of technologies help incident response teams establish a “system of record” using full traffic capture and replay capabilities to improve the efficiency of incident resolution and forensics. Additionally, Blue Coat Intelligence Services (discussed shortly) improves the quality and depth of the metadata Blue Coat Security Analytics draws from in a network security forensics investigation.

Product Differentiation

Within the network security community, a philosophical divide exists between approaches that use packet headers or full packet capture tools for storage and later recall in network forensic investigations. The use of packet headers, sacrificing parts of the packet, can reduce storage by as much as 80%. Blue Coat Security Analytics seeks to empower security professionals with full packet capture, indexing and analyzing packets to offer maximum resolution in a forensics investigation.

The combination of these packet handling techniques separates Blue Coat Security Analytics from other traditional network security forensics and packet capture vendors.

- Blue Coat Security Analytics records and replays all packets and flows at up to 10 Gbps on a single appliance.

- As network traffic enters the network, deep packet inspection (DPI) technology can classify more than 2,400 applications and index thousands of metadata attributes (server IPs, social personas, artifacts, etc.).
• Importantly, SSL packet decryption is initiated in real-time based upon policies. Because a network security team chooses to use a full packet capture platform, the team has visibility of all L2–L7 traffic.

• Without full packets, the argument can be made that “evidence” is not fully preserved.

Full packet capture has two other added virtues. The specific code of a malicious binary is likely to be hidden deeper in the packet. Most of the information that is contained in the packet headers is needed to route the packet over the Internet and to pass traffic through Web servers. The packet headers are like surfers on a wave; the malicious binaries are likely to dwell underneath the surface. Additionally, Blue Coat Security Analytics can be integrated with next generation firewalls (NGFW), intrusion protection systems (IPS), SIEM, endpoint detection and response (EDR) and sandboxing solutions to provide packet level detail of incoming traffic. The byte level granularity of packet data provides complete context and enriches other security platforms. Also worth noting is packet level recording and indexing provides a forensic chain of exactly what happened before, during and after a security incident.

Brand Strength

On two different fronts, brand strength helps Blue Coat win and maintain business in network forensics. As mentioned earlier, the original DeepSee platform set an industry standard for the combination of high-speed packet capture, metadata collection, and deep packet inspection. Blue Coat Systems established its own strong independent reputation in Web security, global threat intelligence, and in data-loss prevention (DLP). Blue Coat Security Analytics is the culmination of the legacy DeepSee platform, real-time threat intelligence, and advanced forensic analytics. With the recent acquisition of Elastica, Blue Coat also compliments Security Analytics by providing cloud application security and visibility, aiding investigations that may span from the network to cloud applications.

Technology Leverage

Blue Coat Security Analytics uses multiple sources to determine the severity of a potential threat:

• **Blue Coat Intelligence Services** - Intelligence Services is used to provide real-time malware detection across web, mail and file protocols, incorporating URL and file reputation. These intelligence Services automatically query the the Blue Coat Global Intelligence Network (GIN) for updated threat information.

• **Bidirectional Communications with other security platforms** - Blue Coat Security Analytics enriches and indexes metadata with information from threat security grids, AV engines, other security platforms, and third-party reputation providers in its threat scoring.
• **Isolation of Malware** – Through integration with Blue Coat Malware Analysis, unknown files can be analyzed and detonated in a sandbox to establish risk and assign threat scores within seconds. Threat verdicts of 1-10 are assigned to analyzed files and URLs.

Ultimately, the confluence of packet inspection, intelligence services, and metadata enrichment allows investigators to find the “root cause” of a security incident as it is happening (hopefully) or in a forensic investigation.

**Customer Ownership Experience**

The most common deployment of Blue Coat Security Analytics is as hardware appliances installed on an 'on-premises' network. The hardware appliances are available in 2Gbps or 10Gbps line-rate packet capture capacities. However, other Security Analytics component options include VMware virtual appliance, software and direct attached or SAN storage modules that can scale to petabytes of storage for extended capture windows. For remote locations, virtual sensors can be deployed with the caveat that virtual sensors incur some latencies at 1Gbps or greater.

The Security Analytics Central Manager is used to aggregate multiple appliances, sensors and virtual machines. Communication between appliances and sensors is initiated through secure socket layer (SSL) tunnels for simplified management and investigation. When deployed as software on certified hardware, Security Analytics is a soft appliance and the performance should be the same as a dedicated Blue Coat appliance.

The Security Analytics Central manager is also the platform's logical engine for system-wide forensics investigations. Directed and aggregated searches originate from the Central Manager to the distributed capture appliances. Asset groups can be manually assigned, created by the Central Manager, or Active Directories can be ported to determine access groups. Role-based access control can be used to determine how user access rules are applied.
Conclusion

Blue Coat Systems is the revenue market leader in Network Security Forensics based on Frost & Sullivan estimates. When Blue Coat Systems acquired Solera Networks, the vision was that the respective expertise (Blue Coat with analytics and threat intelligence and Solera DeepSee for packet inspection and network visibility) would mesh to create a powerful incident detection and network security forensics platform. The Security Analytics platform development has not only fulfilled that vision but also has gone beyond simple synergy with an integrated platform that provides packet analysis, metadata collection, comprehensive threat detection and unknown file inspection.

Thanks to its strong overall performance, Frost & Sullivan estimates that Blue Coat Systems has achieved 14% market share, establishing itself as the market leader in today’s $1 billion-plus Network Security Forensics market. Therefore, Frost & Sullivan recognizes Blue Coat Systems with the 2016 Network Security Forensics Market Leadership Award.
Significance of Market Leadership

Ultimately, growth in any organization depends upon customers purchasing from your company, and then making the decision to return time and again. Loyal customers become brand advocates; brand advocates recruit new customers; the company grows; and then it attains market leadership. To achieve and maintain market leadership, an organization must strive to be best-in-class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.

Understanding Market Leadership

As discussed on the previous page, driving demand, strengthening the brand, and competitive differentiation all play a critical role in a company’s path to market leadership. This three-fold focus, however, is only the beginning of the journey and must be complemented by an equally rigorous focus on the customer experience. Best-practice organizations therefore commit to the customer at each stage of the buying cycle and continue to nurture the relationship once the customer has made a purchase. In this way, they build a loyal, ever-growing customer base and methodically add to their market share over time.
Key Performance Criteria

For the Market Leadership Award, Frost & Sullivan analysts focused on specific criteria to determine the areas of performance excellence that led to the company’s leadership position. The criteria that were considered include (although not limited to) the following:

<table>
<thead>
<tr>
<th>Criterion</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Growth Strategy Excellence</td>
<td>Demonstrated ability to consistently identify, prioritize, and pursue emerging growth opportunities</td>
</tr>
<tr>
<td>Implementation Excellence</td>
<td>Processes support the efficient and consistent implementation of tactics designed to support the strategy</td>
</tr>
<tr>
<td>Product Differentiation</td>
<td>The product or service has carved out a market niche, whether based on price, quality, uniqueness of offering (or some combination of the three) that another company cannot easily duplicate</td>
</tr>
<tr>
<td>Product Quality</td>
<td>The product or service receives high marks for performance, functionality and reliability at every stage of the life cycle</td>
</tr>
<tr>
<td>Brand Strength</td>
<td>The possession of a brand that is respected, recognized, and remembered</td>
</tr>
<tr>
<td>Technology Leverage</td>
<td>Demonstrated commitment to incorporating leading edge technologies into product offerings, for greater product performance and value</td>
</tr>
<tr>
<td>Price/Performance Value</td>
<td>Products or services offer the best value for the price, compared to similar offerings in the market</td>
</tr>
<tr>
<td>Customer Purchase Experience</td>
<td>Customers feel like they are buying the most optimal solution that addresses both their unique needs and their unique constraints</td>
</tr>
<tr>
<td>Customer Ownership Experience</td>
<td>Customers are proud to own the company’s product or service, and have a positive experience throughout the life of the product or service</td>
</tr>
<tr>
<td>Customer Service Experience</td>
<td>Customer service is accessible, fast, stress-free, and of high quality</td>
</tr>
</tbody>
</table>
The Intersection between 360-Degree Research and Best Practices Awards

Frost & Sullivan’s 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree-view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan’s research methodologies. Too often, companies make important growth decisions based on a narrow understanding of their environment, leading to errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry players and for identifying those performing at best-in-class levels.
Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Frost & Sullivan Awards follow a 10-step process to evaluate award candidates and assess their fit with select best practice criteria. The reputation and integrity of the Awards are based on close adherence to this process.

<table>
<thead>
<tr>
<th>STEP</th>
<th>OBJECTIVE</th>
<th>KEY ACTIVITIES</th>
<th>OUTPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Monitor, target, and screen</td>
<td>Identify award recipient candidates from around the globe</td>
<td>• Conduct in-depth industry research • Identify emerging sectors • Scan multiple geographies</td>
<td>Pipeline of candidates who potentially meet all best-practice criteria</td>
</tr>
<tr>
<td>2 Perform 360-degree research</td>
<td>Perform comprehensive, 360-degree research on all candidates in the pipeline</td>
<td>• Interview thought leaders and industry practitioners • Assess candidates’ fit with best-practice criteria • Rank all candidates</td>
<td>Matrix positioning all candidates’ performance relative to one another</td>
</tr>
<tr>
<td>3 Invite thought leadership in best practices</td>
<td>Perform in-depth examination of all candidates</td>
<td>• Confirm best-practice criteria • Examine eligibility of all candidates • Identify any information gaps</td>
<td>Detailed profiles of all ranked candidates</td>
</tr>
<tr>
<td>4 Initiate research director review</td>
<td>Conduct an unbiased evaluation of all candidate profiles</td>
<td>• Brainstorm ranking options • Invite multiple perspectives on candidates’ performance • Update candidate profiles</td>
<td>Final prioritization of all eligible candidates and companion best-practice positioning paper</td>
</tr>
<tr>
<td>5 Assemble panel of industry experts</td>
<td>Present findings to an expert panel of industry thought leaders</td>
<td>• Share findings • Strengthen cases for candidate eligibility • Prioritize candidates</td>
<td>Refined list of prioritized award candidates</td>
</tr>
<tr>
<td>6 Conduct global industry review</td>
<td>Build consensus on award candidates’ eligibility</td>
<td>• Hold global team meeting to review all candidates • Pressure-test fit with criteria • Confirm inclusion of all eligible candidates</td>
<td>Final list of eligible award candidates, representing success stories worldwide</td>
</tr>
<tr>
<td>7 Perform quality check</td>
<td>Develop official award consideration materials</td>
<td>• Perform final performance benchmarking activities • Write nominations • Perform quality review</td>
<td>High-quality, accurate, and creative presentation of nominees’ successes</td>
</tr>
<tr>
<td>8 Reconnect with panel of industry experts</td>
<td>Finalize the selection of the best-practice award recipient</td>
<td>• Review analysis with panel • Build consensus • Select winner</td>
<td>Decision on which company performs best against all best-practice criteria</td>
</tr>
<tr>
<td>9 Communicate recognition</td>
<td>Inform award recipient of award recognition</td>
<td>• Present award to the CEO • Inspire the organization for continued success • Celebrate the recipient’s performance</td>
<td>Announcement of award and plan for how recipient can use the award to enhance the brand</td>
</tr>
<tr>
<td>10 Take strategic action</td>
<td>Upon licensing, company may share award news with stakeholders and customers</td>
<td>• Coordinate media outreach • Design a marketing plan • Assess award’s role in future strategic planning</td>
<td>Widespread awareness of recipient’s award status among investors, media personnel, and employees</td>
</tr>
</tbody>
</table>
About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best in class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages almost 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 31 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.