Solution Brief

Symantec Technology Integration Partner: Plixer

Business Challenge

Malware infections have evolved to become a mission critical incident, where loss of data can impact an organization's reputation and business operations. While the typical malware incident response may have been simply reinstalling the operating system in the past, today's incidents require an investigation into what happened, how it happened and what data was stolen to ensure it doesn't happen again. The network, and in particular, the secure proxy, remain the main control points in effective data security and provide the starting point for information around user activity. Significant additional benefit comes from combining the intelligence and actionable data, gathered from routers, switches and servers, with the proxy data on end user devices and their behaviors. The result is extremely useful for both the security operations and incident response teams.

As enterprise network administrators deal with BYOD, shadow IT and the Internet of Things, the need for data theft detection and incident response is crucial. Symantec's portfolio of products integrates with other incident response and behavioral analysis technologies such as Scrutinizer, allowing security professionals to see what is happening in the network in real time or through historical analytics repositories. This "anywhere, anytime" visibility is vital to identifying critical attack indicators and performing impact analysis as attackers move within an organization's network.

Solution: Symantec's Secure Web Gateway and Plixer's Scrutinizer

The combination of Symantec's Secure Web Gateway together with the Plixer's Scrutinizer Incident Response System provides security teams with deeper traffic insight at the edge of the network where end users ingress and egress the network. The Secure Web Gateway collects and logs the details, essentially the "meta data" on every connection request. Scrutinizer then correlates the meta data with the flows collected by every router, switch and server on the network. This integration enhances legacy NetFlow v5 and v9 exports by providing detailed correlated log data, including username, URL, categorization, risk rating and other relevant information on the nature of each connection.

The integrated solution provides a single interface for viewing heterogeneous flow exports from different vendors, and enriches their exported data and logs by correlating and combining the flows with the meta data collected by the Secure Web Gateway. Pivoting from one vendor's interface to another is no longer necessary. This joint solution simplifies the user interface learning curve and ensures that IT team members gain full visibility into the details surrounding each malware incident.

By working with Plixer, Symantec can:

- Ensure that customer meet their compliance needs related to historical storage of events
- Extend the customers investment in legacy flow exporting hardware
- Improve insight into connection performance issues from desktops and wireless devices
- Monitor behaviors over time and detects slow data leaks
- Increase the insight into each malware incident

plixer

Partner: Plixer International, Inc.

Partner Product: Scrutinizer Incident Response System

Symantec Product: Blue Coat ProxySG

Symantec

The Symantec Security Platform is an integral component to an organization's incident response plan.

How it Works

Bluecoat's Secure Web Gateway generates detailed logs containing the specific information around each web request that can be correlated with the flows that could be ingressing anywhere on the network. These logs are collected in the Scrutinizer system. When an incident is investigated, any router, switch or server exporting flows that is chosen to investigate the malware can display additional context obtained from the Bluecoat Secure Web Gateway, including user, authentication, URL, SSL certificate, website categorization, risk level, and other relevant information needed for an investigation.

The diagram below demonstrates how the Symantec and Plixer work together to enhance the contextual details of legacy flows when investigating the traffic patterns of an infection.

The Symantec Secure Web Gateway sits between your users and their interactions with the Internet to identify malicious payloads and to control sensitive content. The Secure Web Gateway consolidates a broad feature-set to authenticate users, filter web traffic, identify cloud application usage, provide data loss prevention, deliver threat prevention, and ensure visibility into encrypted traffic. It also provides coaching and feedback to the user to ensure a strong and secure user experience when interacting with the Internet. Further it can provide consolidated policy management and reporting when deployed in-concert with Symantec's cloud-delivered Secure Web Gateway as a hybrid delivery model.

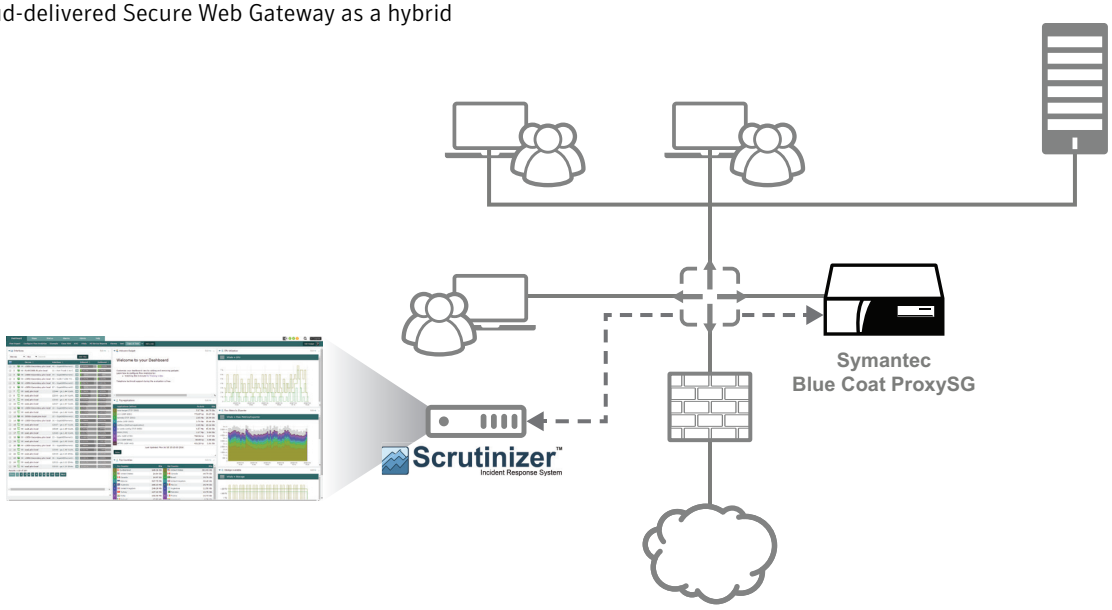
By using Symantec's proxy architecture, organizations get the highest level of web security possible, and an ideal environment for integration with the latest technologies like the Plixer Scrutinizer. The Secure Web Gateway works seamlessly with best-of-breed technologies, empowering your organization to get a full understanding and view of malware incidents being researched by your IT team.

Finally, to prevent any newly discovered malware from entering the network again, Symantec's solution automatically updates its Global Intelligence Network in real time, and if the file hash or URL is ever seen again, ProxySG with Content Analysis will simply block it at the network level before it even enters your organization's environment.

Benefits

The combined Symantec's Secure Web Gateway and Plixer's Scrutinizer Incident Response System:

- Deeper and richer insight into the traffic patterns of low and slow data leaks
- Improve the contextual details provided by legacy exports
- Ensure a company is complaint with industry regulation



About Plixer

Plixer is a leading security analytics and flow forensics provider focused on engineering the incident response system for uncovering unwanted communication behaviors. Rather than depending on packet signatures, their strategy uncovers stealthy communications by leveraging NetFlow, IPFIX, sFlow, and other derivatives. The company was built by network and system engineers who understand the need for scalable distributed collection solutions that meet the dynamic demands of security and network professionals. Customers include Walmart, CNN, The Coca-Cola Company, Lockheed Martin, IBM, AT&T, Raytheon and Xerox. To learn more, please visit www.plixer.com.

For More Information

Learn more about Symantec Technology Integration Partners on our website.

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

SYMC_sb_TechPartner_ProxySG_Plixer_EN_v1a