Solution Brief

# Symantec Technology Integration Partner: E8 Security

## Business Challenge

Gartner reports that the data analyzed by enterprise security organizations is doubling every year and that 40% of enterprises will be using data sets of at least 10 terabytes by 2016.[1] This deluge of data prevents security teams from finding meaningful insights in the data, creating an "insight gap." The insight gap is caused primarily by two challenges. First, by enterprises' reliance on manually configured rules and previously known signatures, which can only identify known patterns, limiting the effectiveness of legacy security tools. Second, by the failure of legacy event monitoring systems to provide the scale and analytical intelligence needed to detect and prioritize threats.

For analysts to progress from insight to effective action and make smart and timely decisions requires prioritization of high-risk anomalies, context about threats, and an understanding of their impact. The current methodology by which analysts extract information from multiple systems and manually derive context to understand the impact can result in significant delays and erroneous decisions, or an "action gap."

## Symantec and E8 Security: Closing the Insight and Action Gaps

Symantec and E8 Security deliver an integrated, end-to-end platform that provides critical capabilities for security operations, including proactive detection, analysis and remediation of threats. E8 Security applies machine learning and multi-dimensional modeling, which examines user and device behaviors to process large volumes of siloed security data, learn behaviors and relationships, and automatically identify anomalous activities. Advanced threat models expose threat activities, such as command and control (C2) communications, lateral movement and credential compromises.

These sophisticated analytics enable machines and humans to optimize their threat identification abilities. By combining the scale of big data, the power of behavioral analytics and incorporating human knowledge, E8 Security's solution provides insight into the real risk and nature of security threats within the business environment – closing both the insight and action gaps.

**Partner:** E8 Security

**Partner Product:** E8 Security Behavioral Intelligence Platform

**Symantec Product:** Blue Coat ProxySG

## How It Works

Visibility into suspicious behaviors is critical to enabling enterprises to contend with sophisticated and persistent cyber attacks. Because the majority of enterprise network traffic is web related, the network, and in particular the secure proxy, is the main control point in effective enterprise security. Blue Coat ProxySG


[1] MacDonald, N. Information Security Is Becoming a Big Data Analytics Problem. March 2012.

acts as a control point to block traffic to malicious destinations identified by the E8 Security platform – automating the detection and containment of newly discovered threat activity.

In addition, the integration of log data from ProxySG with E8 Security's behavioral intelligence platform is what gives E8 Security customers visibility into anomalous activity, including early indicators of compromise (IOCs) such as malware callbacks or compromised credentials. Analysts are presented with a unified view of suspicious user or endpoint activities across all users and devices, as well as detailed insight into how these suspicious users and devices have been communicating across the network. E8 Security's intuitive user interface, allows analysts to quickly and easily drill down into the relevant network traffic or other raw data associated with these suspicious users or endpoints.

## Benefits

- **Identify threats:** By analyzing large volumes of Symantec web proxy logs, network data, user activity and device behaviors, E8 Security's signature-less platform detects threats that bypass other controls. E8 Security's platform applies multi-dimensional models to the data to discover behaviors that are different from the "normal behavior pattern" and pinpoint malicious activity within the network.

- **Make threat remediation faster and more effective:** The solution combines E8 Security-generated behavioral anomalies with ProxySG's secure, real-time threat detection and policy enforcement capabilities to enable analysts to make smart decisions and take faster action.

- **Enable data exploration and retrospective analysis:** E8 Security supports ProxySG's real-time analytics with a big data platform for long-term data retention and historical data analysis. This allows analysts to correlate and explore suspicious activities over extended periods of time. Analysts can retain and analyze historical activity of each entity or group of entities to gain situational awareness and comprehensive understanding of advanced threat activity across the enterprise.

## About E8 Security

E8 Security is transforming the effectiveness of enterprise security teams by extracting actionable intelligence from burgeoning security data. With a scalable machine learning based behavioral analytics platform, E8 Security empowers organizations to find and prioritize previously unknown threats, provide insight for faster resolution and improve the efficacy of existing security infrastructure. The company's breakthrough cyber analytics platform delivers immediate value by reducing business risk, increasing operational efficiency and improving return on existing security investments.

## 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.

Copyright © 2017 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.
# SYMC_sb_TechPartner_ProxySG_E8Security_EN_v1a