Joint Solution Brief

Identify Unknown Threats Hidden Inside the Network with E8 Security and Gigamon

The Challenge

Without adequate visibility into traffic streams, security operators spend too much time manually investigating alerts and correlating event logs from multiple, siloed security systems—and not enough time proactively responding to threat indicators.

Integrated Solution

Integrated with the Gigamon GigaSECURE® Security Delivery Platform, the E8 Security Fusion Platform gains the pervasive network visibility needed to help eliminate data silos and generate rich context into suspicious activity for better, faster threat response.

Joint Solution Benefits

- Broad and deep visibility across physical, virtual and cloud network traffic allows the E8 Security Fusion Platform to help identify unknown threats inside the network
- The E8 Security Fusion Platform can leverage the GigaSECURE Security Delivery Platform's automatic traffic load balancing and aggregation functionality to reduce bottlenecking and port oversubscription
- With the GigaSECURE platform's real-time SSL decryption functionality, the E8 Security Fusion Platform gets increased visibility into traffic
- Filtering and distribution of relevant east-west traffic to the E8 Security Fusion Platform accelerates time-to-threat detection

Introduction

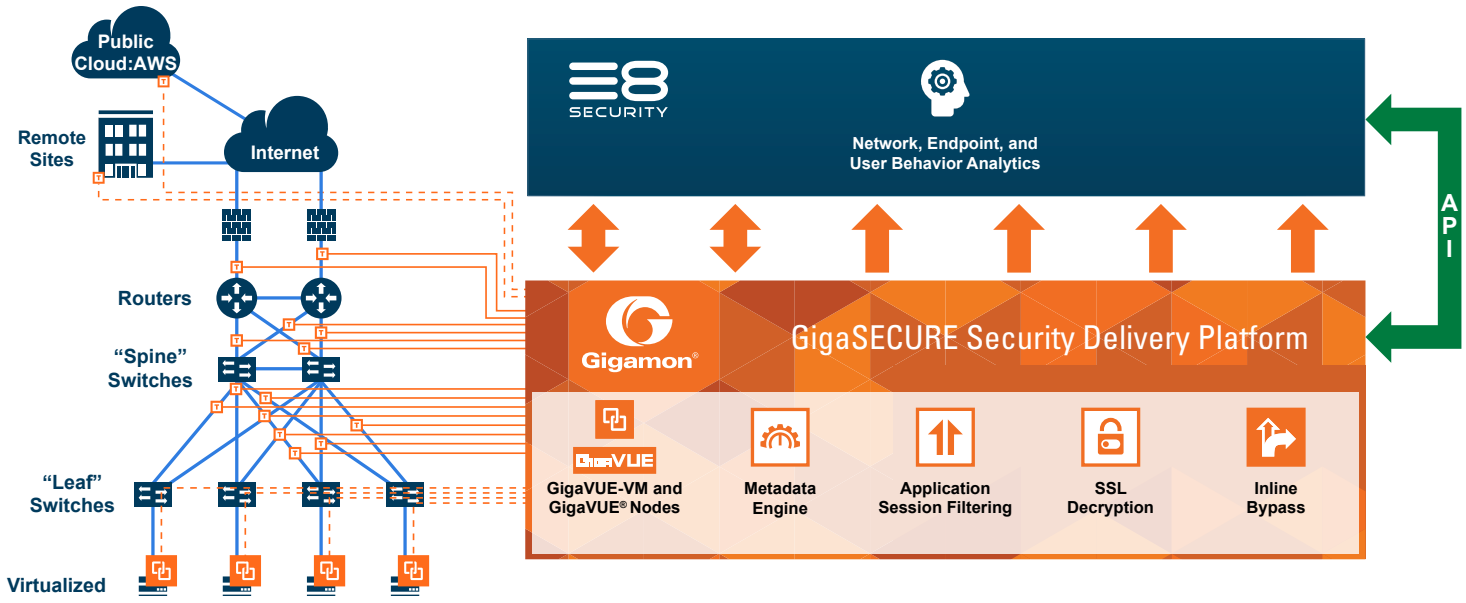
In using manual analysis or legacy systems that rely on rule- and signature-based technology, organizations can only identify known threats and, too often, they struggle to consume the volume and variety of data needed to accurately identify and prioritize unknown threats to effectively remediate them.

E8 Security is transforming traditional security operations with a strategy that combines the power of visibility, machine learning, and behavioral analytics to hasten the identification of unknown threats hidden inside the network. With pervasive visibility and analytics based on user and network activity and endpoint behavior, security teams can now gain context into suspicious activity and expose threat movement inside the network, including command-and-control (C2) communication, lateral movement, credential compromise, and attacker persistence.

The Gigamon and E8 Security Joint Solution

Together with the Gigamon GigaSECURE Security Delivery Platform, the E8 Security Fusion Platform provides insight into the real risk and nature of security threats to help determine the best and fastest course of mitigative action. By automating the analysis of Big Data with machine-learning and multi-dimensional algorithms, the E8 Security Fusion Platform helps eliminate sole reliance on static rules, correlations, and previously-known signatures. It breaks down data silos by integrating user, network, and endpoint data into a single analytical platform and cross-correlates behavior patterns across multiple technologies to help provide the insights needed for a security operations team to be successful.

By establishing a baseline of what is normal in the network, the E8 Security Fusion Platform helps security teams quickly determine if abnormal behavior is indicative of a threat and respond right away. Moreover, it measures an organization's risk for a data breach, identifies the early warnings signs when critical resources are being targeted, and scores threats based on the sequence of anomalous events and customer-specific contextual information to help analysts prioritize alerts and speed response times.



Key GigaSECURE Security Delivery Platform features that augment the value of E8 Security technology include:

Easy access to traffic from physical, virtual and cloud networks: The GigaSECURE platform manages and delivers all network traffic—in the format required—to the E8 Security Fusion Platform. To monitor east-west data center traffic, and public cloud workloads, Gigamon taps virtual traffic and incorporates it into the GigaSECURE platform for delivery to E8 Security, which helps eliminate blind spots and increase the probability of discovering anomalous behavior.

Aggregation to minimize tool port use: Where links have low traffic volumes, GigaSECURE can aggregate these together before sending them to the E8 Security Fusion Platform to minimize the number of ports needed. By tagging the traffic, GigaSECURE enables the identification of the traffic source.

SSL decryption: Real-time SSL decryption integration increases traffic visibility for the E8 Security Behavioral Intelligence Platform, broadening its scope for analysis and inspection of malicious activity.

Masking for security: GigaSECURE is able to mask any sensitive data (e.g., credit card numbers in e-commerce and patient identification in healthcare) within packets before sending them to other tools where operators or other unintended recipients may see them.

De-duplication: Pervasive visibility requires tapping or copying traffic from multiple points in the network, which, in turn, means tools may see the same packet more than once. To avoid unnecessary packet processing overhead on the E8 Security Fusion Platform, GigaSECURE has a highly effective de-duplication engine that removes duplicates before they consume resources and helps balance monitoring coverage.

Learn More

For more information on E8 Security and Gigamon solutions, contact:

E8 SECURITY
e8security.com

Gigamon®
www.gigamon.com

3210-01 12/16