Joint Solution Brief

See Everything. Identify What Matters Most. Respond Faster.

The Challenge

When new intelligence is released on a previously unknown threat, an organization needs to know if it's been compromised or if it has not. If the network or cloud workloads have been compromised, the organization needs intuitive technology that breaks through the noise to deliver deep network forensics and rapid incident response.

Integrated Solution

ProtectWise provides a new utility model for enterprise security, delivering pervasive visibility, automated threat detection, and unlimited forensic exploration on-demand and entirely from the cloud. Gigamon's GigaSECURE® Security Delivery Platform delivers network traffic, providing a prioritized view of physical, virtual, and cloud network traffic to share with ProtectWise. By integrating with the Gigamon platform, ProtectWise secures workloads in enterprise, cloud or hybrid deployments.

Key Benefits

- Easily collect and visualize NetFlow, metadata, truncated flows and full-fidelity PCAP by protocol and application from physical and virtual links
- Long-term retention for retrospective analysis and correlated event creation
- Continuous, automated threat detection and analysis in real-time and retrospectively
- Community-scaled threat intelligence and analysis
- Rapidly access full PCAP within The ProtectWise Grid™ to conduct deep-dive, comprehensive forensic investigations and reduce attacker dwell time
- De-duplicate traffic and/or decrypt SSL/TLS traffic before sending it to The ProtectWise Grid™
- Slice or mask sensitive data to help facilitate compliance before sending it to The ProtectWise Grid™

Introduction

With an ever-increasing number of breaches and incidents impacting today's networks, instrumenting the environment for visibility is essential, but it's not the end of the story. The security solution also needs to be able to detect and analyze threats—both in real time and retrospectively—without adding unnecessary noise. When new intelligence is released on a threat that was previously unknown, an organization needs to be able to go back and see how it impacted them, and for how long. If the organization has been compromised, it needs to be able to quickly respond, manage alarm events, review situational reports, and investigate network activity and threat observations—all within a system that provides the context of the business to guide its actions.

The Gigamon and ProtectWise Joint Solution

Record Everything

The ProtectWise Grid creates a memory of an organization's network traffic on any network segment, whether owned by it (e.g., internal network) or not (e.g., cloud environment), and uses this information for detection and analysis of both new and previously unknown threats. Because The ProtectWise Grid™ runs entirely from the cloud, this memory can retain full-fidelity network traffic.

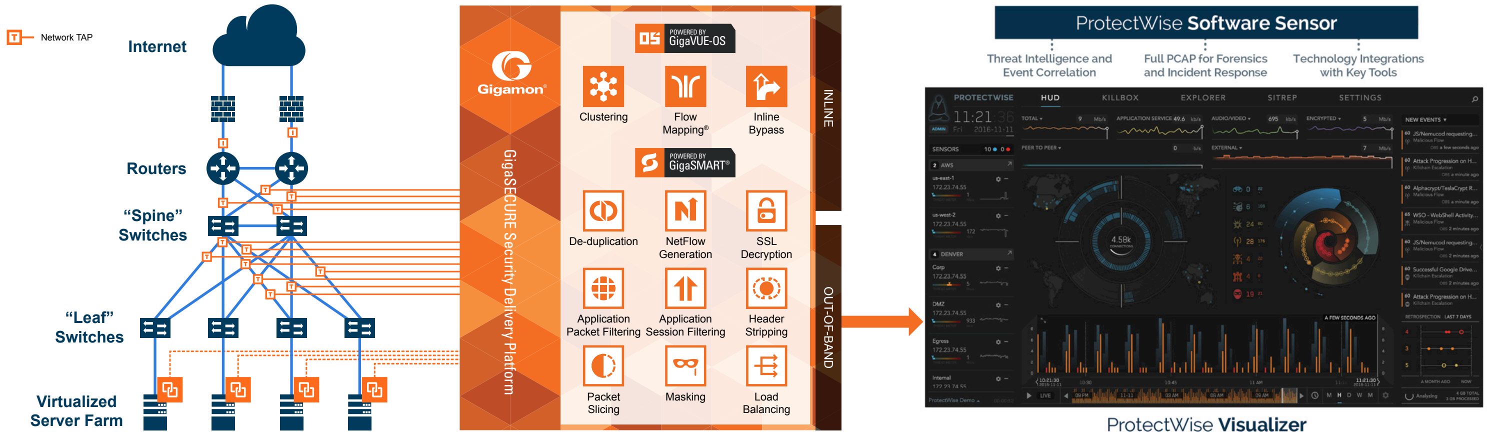
Gigamon's GigaSECURE Security Delivery Platform is ideal for identifying the appropriate traffic flows within the network, de-duplicating, manipulating, and filtering that traffic before delivering it to the ProtectWise Grid. SSL/TLS encrypted traffic can also be decrypted by the GigaSECURE platform before passing it to the ProtectWise Grid to enhance complete visibility.

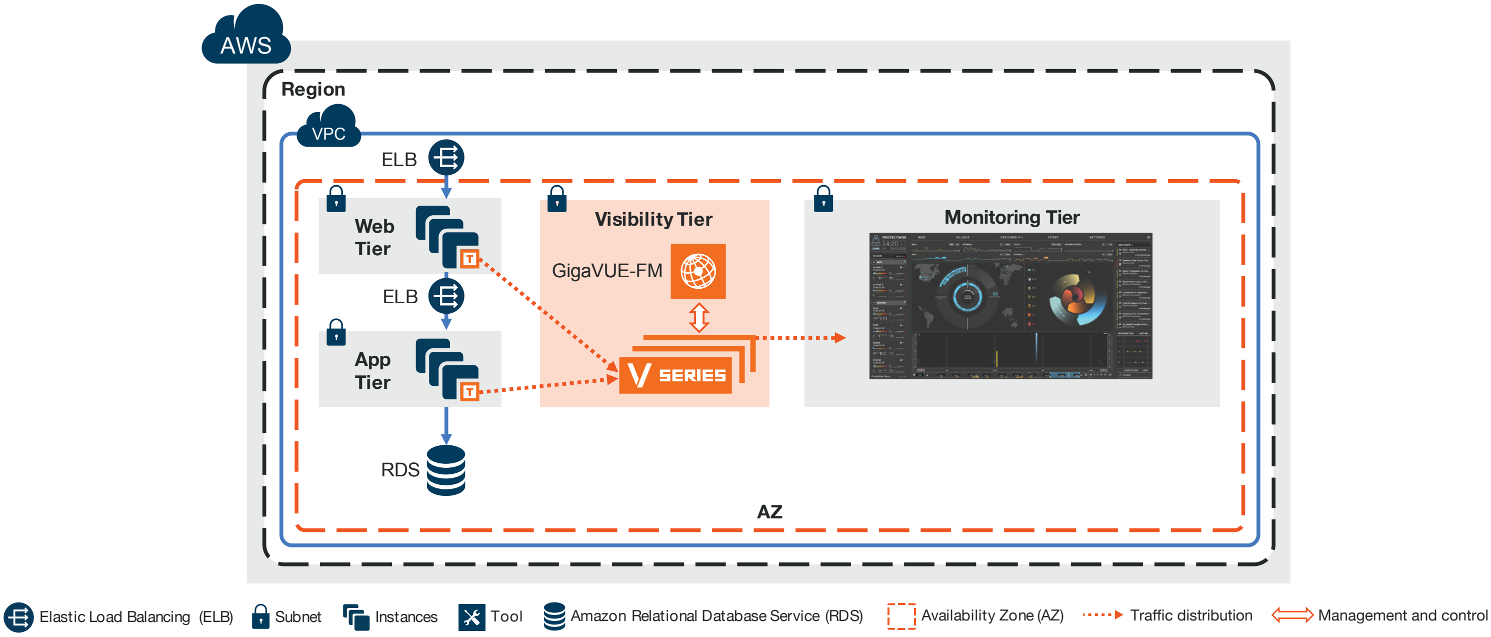
See Everything

Using network traffic from enterprise, cloud, or hybrid deployments, the ProtectWise Grid analyzes NetFlow, metadata, truncated flows or full-fidelity PCAP by protocol and application and offers an unlimited forensic recording window. This allows measurement of the full impact of newly-discovered attacks going back into weeks, months, or even years of past data.

The ProtectWise Grid leverages cloud economies of scale to provide powerful threat detection capabilities that are not possible using standalone appliances. These include continuous, cross-customer correlation of threat intelligence and the industry's only automated retrospection.

The ProtectWise Grid correlates intelligence from proprietary research, machine learning, flow-based traffic algorithms, and multiple third-party intelligence feeds. Collective correlation of security events across customers creates a feedback loop that de-noises the security environment. It's a shared brain that constantly learns, adapts, reduces false positives, and can eliminate alarm fatigue.





ProtectWise integrates with a variety of security products including firewalls, gateways, endpoints, and SIEM to add context and streamline incident response.

Immersive Security

The innovative ProtectWise Visualizer provides analysts with an immersive security experience to cut through the noise and hunt for threats across enterprise, cloud, and hybrid deployments. Get an at-a-glance view of the entire network, see events by kill-chain stage across past and current timelines, and more. Easily pivot into a deeper forensic workbench that includes deep packet exploration, replaying policies for applications and protocols, PCAP download for more advanced threat hunting.

Learn More

For more information about ProtectWise and Gigamon solution, contact:

PROTECTWISE™
www.protectwise.com

Gigamon®
www.gigamon.com