Joint Solution Brief

Protecting the Modern Data Center with GuardiCore and GigaSECURE

The Challenge

Visibility into east-west data center traffic is not only difficult, but it has created a gaping, deleterious security blind spot that hackers use to their advantage.

Integrated Solution

Integrated with the Gigamon GigaSECURE® Security Delivery Platform, the GuardiCore Centra Security Platform is a single, scalable solution that covers five critical capabilities for effective data center security: visibility, segmentation, breach detection, automated analysis and response.

Joint Solution Benefits

- Broad and deep visibility across both physical and virtual network traffic flows augments GuardiCore's ability to detect and respond to advanced threats in real time
- GigaSECURE Security Delivery Platform's automatic traffic load distribution and aggregation functionality optimizes traffic for GuardiCore
- GigaSECURE de-duplicates traffic gathered from multiple collection points and distributes east-west traffic to GuardiCore to help accelerate breach detection and response
- With the GigaSECURE Security Delivery Platform's real-time SSL decryption functionality, GuardiCore gets increased visibility into traffic flows without performance degradation

Introduction

Data centers, which house critical corporate data and business processes, have proven to be lucrative targets for cyber attackers. They've also proven to be easy to penetrate at the perimeter. Once inside a data center, however, intruders are not so easy to detect. In fact, it can take organizations months—even years—to discover a breach, detect its source, and begin to remediate and assess what happened.

The key to finding them—and finding them much faster—is pervasive visibility across physical, virtual, and hybrid environments.

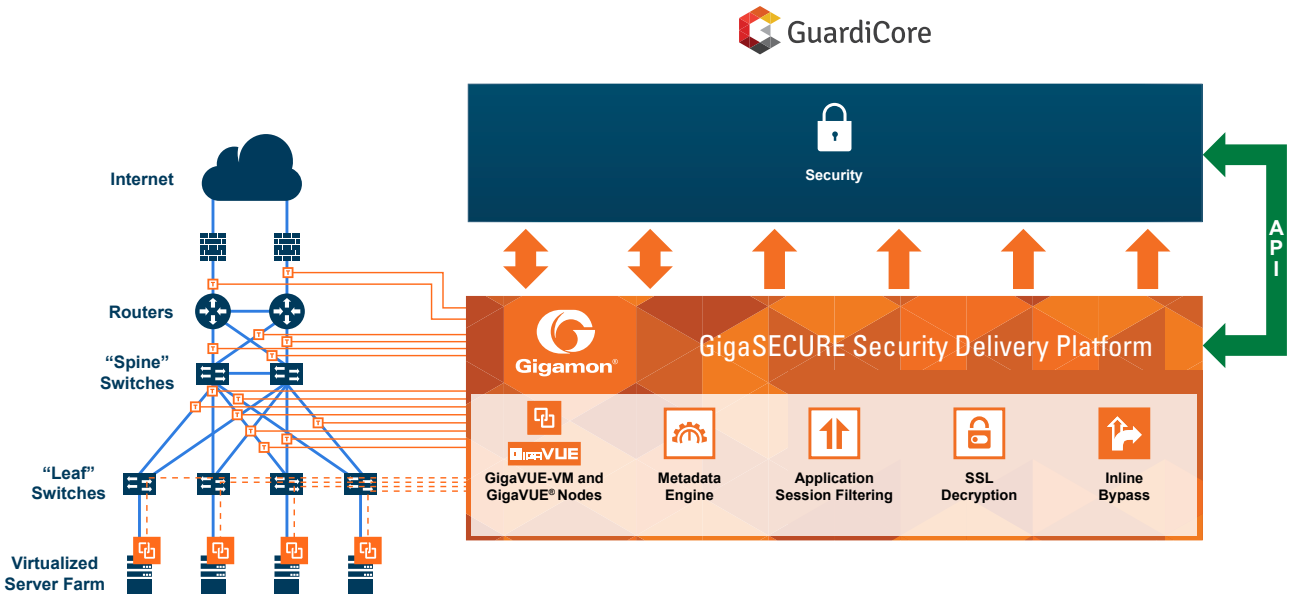
Together with the Gigamon GigaSECURE Security Delivery Platform, GuardiCore helps provides the visibility necessary to spot breaches that other security measures have missed. In particular, it delivers visibility into east-west traffic—too often a substantial security blind spot—to help organizations respond to active breaches in a fraction of the time traditional technologies take, while also eliminating the analysis paralysis associated with log data overload and false positives.

The Gigamon and GuardiCore Joint Solution

GuardiCore employs a unique combination of threat deception, process-level visibility, semantics-based analysis and automated responses to engage, investigate and then thwart confirmed attacks with a high-level of accuracy.

Built on high-interaction, dynamic-deception technology, the GuardiCore Centra Security Platform can quickly identify active breaches with extremely low false-positive rates. It's lightweight, distributed architecture scales to cover data center traffic without impacting performance and can support workloads running on bare metal as well as within virtualized environments, containers, or private and public clouds.

When combined with the Gigamon GigaSECURE Security Delivery Platform, GuardiCore is able to leverage the GigaSECURE platform's automatic traffic load balancing and aggregation real-time SSL decryption functionality, and gain increased visibility into east-west traffic flows without performance degradation for quicker and more efficient breach detection and response. With this new and heightened level of visibility into data center traffic, users can make well-informed policy decisions for micro-segmentation, reduce dwell time during active breaches, and respond to incidents before they result in data theft or other damage.



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

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

Filtering traffic to only send relevant traffic: The GigaSECURE Security Delivery Platform can be configured to send only relevant traffic or sessions to GuardiCore to help ensure that it only analyzes traffic that provides security value.

Aggregation to minimize tool port use: Where links have low traffic volumes, the GigaSECURE platform can aggregate these together before sending them to the GuardiCore Centra Security Platform to minimize the number of ports needed. By tagging the traffic, the GigaSECURE Security Delivery Platform helps to identify the traffic source.

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

Masking for security: The GigaSECURE Security Delivery Platform 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 GuardiCore, the GigaSECURE platform 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 GuardiCore and Gigamon® solutions, contact:

GuardiCore
www.guardicore.com

Gigamon®
www.gigamon.com

3211-01 10/16