Cognito automated threat detection and response with the Gigamon Security Delivery Platform

CHALLENGE

Despite a strong perimeter defense with next-generation firewalls, IDS and malware sandboxes, cyber attackers will still get into your network. And without visibility into what's happening inside the network, it's impossible to detect and mitigate these attacks.

SOLUTION

With the GigaSECURE® Security Delivery Platform from Gigamon, the Cognito automated threat detection and response platform provides continuous monitoring of internal network traffic to pinpoint in-progress cyber attacks that evade perimeter defenses.

Cognito automatically detects cyber threats hidden in approved applications and encrypted traffic, correlates those threats to the hosts that are under attack, and delivers unique context about what attackers are doing, enabling security teams to quickly prevent or mitigate loss.

BENEFITS

- Cognito detects in-progress cyber attacks that evade prevention security defenses and spread inside networks – automatically and in real time.
- Offering visibility into physical and virtual traffic across the network, Cognito combines data science, machine learning and behavioral analysis to detect all phases of a cyber attack.
- Gigamon ensures that only the relevant traffic and sessions are sent to Cognito, thereby improving efficacy.
- Gigamon taps virtual traffic and delivers it to Cognito on the physical network – ensuring all traffic is monitored and analyzed together and avoiding blind spots.

Despite strong perimeter defenses using next-generation firewalls, IDS/IPS and malware sandboxes, cyber attackers continue to slip past the signatures and reputation lists used by these prevention systems and spread inside networks. And mobile device users can bypass these controls altogether, literally carrying hidden threats from public Wi-Fi hotspots into the network.

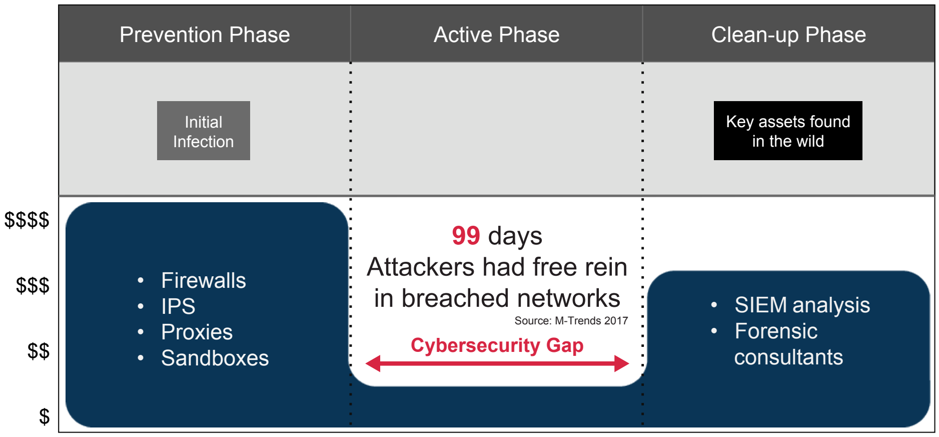
The problem is that signatures and reputation lists only detect *known* threats and must be continually updated. It's easy for attackers to mount an assault using different IP addresses or by adding a few bits to a malware file so it can slip by, unknown and undetected.

Security analysts today are also overwhelmed by a never-ending succession of alerts and logs about potential network cyber attacks. It's not humanly possible to sift through and interpret that much data, identify the most serious threats, and then mitigate attacks before they spread.

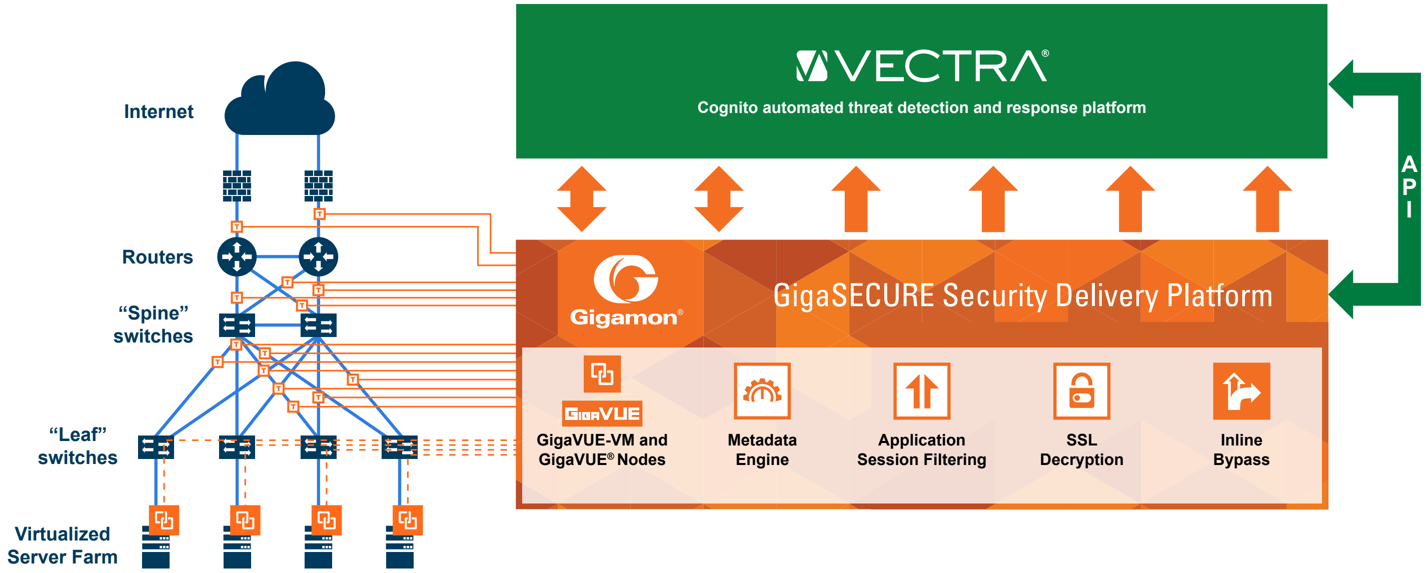
In addition, security teams often don't know what to look for or where. Many organizations use log managers and SIEMs that rely on feeds from security systems that fail to detect threats in the first place. And they are often required to painstakingly reconstruct each cyber breach in order to understand the extent of damage.

Despite all the prevention security tools at your disposal, there remains a dangerous cybersecurity gap between the time attackers infiltrate and spread inside a network and the moment organizations discover they've become victims of a data breach.

The cybersecurity gap



Source: M-Trends 2017


Internet
Routers
"Spine" switches
"Leaf" switches
Virtualized Server Farm
T
VECTRA
Cognito automated threat detection and response platform
API
Gigamon
GigaSECURE Security Delivery Platform
GigaVUE
GigaVUE-VM and GigaVUE® Nodes
Metadata Engine
Application Session Filtering
SSL Decryption
Inline Bypass

The Vectra and Gigamon joint solution

The Cognito™ automated threat detection and response platform from Vectra®, augmented with the GigaSECURE Security Delivery Platform from Gigamon, continuously monitors internal network traffic to pinpoint in-progress cyber attacks in real time.

Gigamon provides intelligent filtering on physical and virtual networks and passes that traffic to Cognito for real-time threat analysis. Multiple Gigamon tap points deployed at the edge and core provide Cognito with intelligent traffic filtering at all key points in network.

In addition to automatically correlating detected threats against hosts that are under attack, Cognito provides unique context about what attackers are doing so organizations can quickly prevent or mitigate loss. Attacks that pose the highest risk are prioritized so IT security teams can focus their attention on the detections that matter most.

Cognito leverages a unique combination of data science, machine learning and behavioral analysis to detect all phases of an attack – command and control, botnet monetization, internal reconnaissance, lateral movement and data exfiltration.

Over time, Cognito understands the naturally occurring communities in the network and continuously listens, thinks and learns to adapt to the ever-changing threat landscape. Cognito gives IT security teams the speed and agility to stopping threats that present the biggest danger.

Cognito and the GigaSECURE platform

The GigaSECURE Security Delivery Platform delivers a wide range of critical features to Cognito deployments, including:

- Easy access to traffic from physical and virtual networks: The GigaSECURE platform manages and delivers all network traffic to Cognito efficiently and in the correct format. To monitor east-west data center traffic, Gigamon taps virtual traffic and incorporates it into the GigaSECURE platform for delivery to Cognito on the physical network. This ensures that all traffic is monitored and analyzed together and eliminates blind spots.
- Filtering traffic to only send relevant traffic: The GigaSECURE platform can be configured to send only relevant traffic or sessions to the Cognito solution. This ensures that Cognito only analyzes traffic that provides security value.
- Aggregation minimizes tool ports: The GigaSECURE platform aggregates links with low traffic-volumes before sending them to Cognito, reducing the number of ports that are used. Traffic tagging ensures that the traffic source is always identified.

Together, Vectra and Gigamon close the dangerous cybersecurity gap between perimeter defenses and post-breach analysis by improving network visibility and detecting the fundamental actions and behaviors that attackers perform when they spy, spread and steal inside networks.

Gigamon®
www.gigamon.com

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai