SOLUTION BRIEF

Fortinet and CSPi Security Solution

Automated Breach Detection for Improved Incident Response

Challenges

The sheer volume of data to monitor and protect is leaving organizations overwhelmed in their security efforts. The constantly changing network perimeter, highly distributed resources, dynamic movements of data between devices and across environments, and new applications have opened unprecedented access, making it easier for cyber criminals to get to critical data. This also causes an organization's security platform and products to receive a staggering number of alert events, as many as 5,000 a day, that even their highly trained security teams struggle to keep up with.

Manual mining of the data is risky and error-prone and can lead to missing a critical alert. Given that organizations also need to meet tightening data privacy regulations and compliance time constraints, it is critical for them to continuously monitor, analyze, and focus on the right and often highly regulated personally identifiable information (PII) data.

It's clear that breaches are not going to stop and are difficult, if not impossible, to prevent; therefore, organizations today need an effective solution not only for detecting, validating, and determining the scope of a breach but also for automating sharing the intelligence and synchronizing the increasingly automated responses to the threats in real time to ultimately improve their incident response time.

The Joint Solution

The Fortinet Security Fabric is designed around a series of open application programming interfaces (APIs), open authentication technology, and standardized telemetry data

to address these challenges. It enables organizations to integrate existing security technologies via open interfaces to provide end-to-end security without compromise.

FortiGate enterprise firewall and CSPi Myricom nVoy Series are integrated via the Fabric-Ready Program to deliver a comprehensive, highly effective security solution with intelligent cyber threat detection and verification, and detailed, all-encompassing, packet-level data inspection that results in rapid response times and mitigation of threats. The integration allows the nVoy solution to continuously ingest alerts issued by the FortiGate enterprise firewall and automatically compare those against identified critical assets. Since the network traffic between critical assets is recorded, it enables the breach identification and extraction of all event-driven threat conversations, thus enabling the security teams to conduct an extremely focused incident investigation of an organization's most critical, and in some cases highly regulated, data such as PII, financial transactions, or other intellectual property (IP).

Joint Solution Components

- Fortinet FortiGate
- CSPi Myricom nVoy Series

Automated Investigative Response

Automated breach identification, detailed threat conversation extractions, and immediate email notifications for a focused and complete analysis of any breach.

360° Insight

Superior intelligence into breaches involving critical assets. Know which records were exposed and which weren't.

Greater Efficiency

Reduce time—from intrusion to detection to response—to a few hours.

Enhanced Analysis

Pivot around incidents and utilize the information to analyze other critical assets an intruder or malicious insider attempted to access.

Significant ROI

Shorten investigation time to a few hours, compared to a few weeks using traditional manual IR techniques.

FORTINET FABRIC-READY

CSPi Myricom nVoy Series

CSPi Myricom nVoy Series automates two critical elements of the incident investigation process: data breach validation and complete data extraction. When the nVoy Automated Investigative Response (AIR) application is paired with the Myricom nVoy packet recorder, it assesses all alerts issued by a Fortinet intrusion detection system/intrusion prevention system (IDS/IPS) to determine if any are against a user-specified list of critical assets (devices, applications, or a combination). If so, the nVoy AIR application uses the alert event data, including the source and/or target address, along with the recorded time stamps to drive the nVoy Packet Recorder to produce an extraction file of all the conversations between those devices. The nVoy solution eliminates manual intervention and thus drastically reduces the risk of missing an alert, puts resources to better use, and most importantly, saves crucial time during the investigation. An additional benefit is that this process can run 24×365 and generates the data required to remain in compliance with minimal human effort. And the nVoy AIR application will notify the analyst team or the managed service provider when an extract is created so that incident investigation can immediately commence.

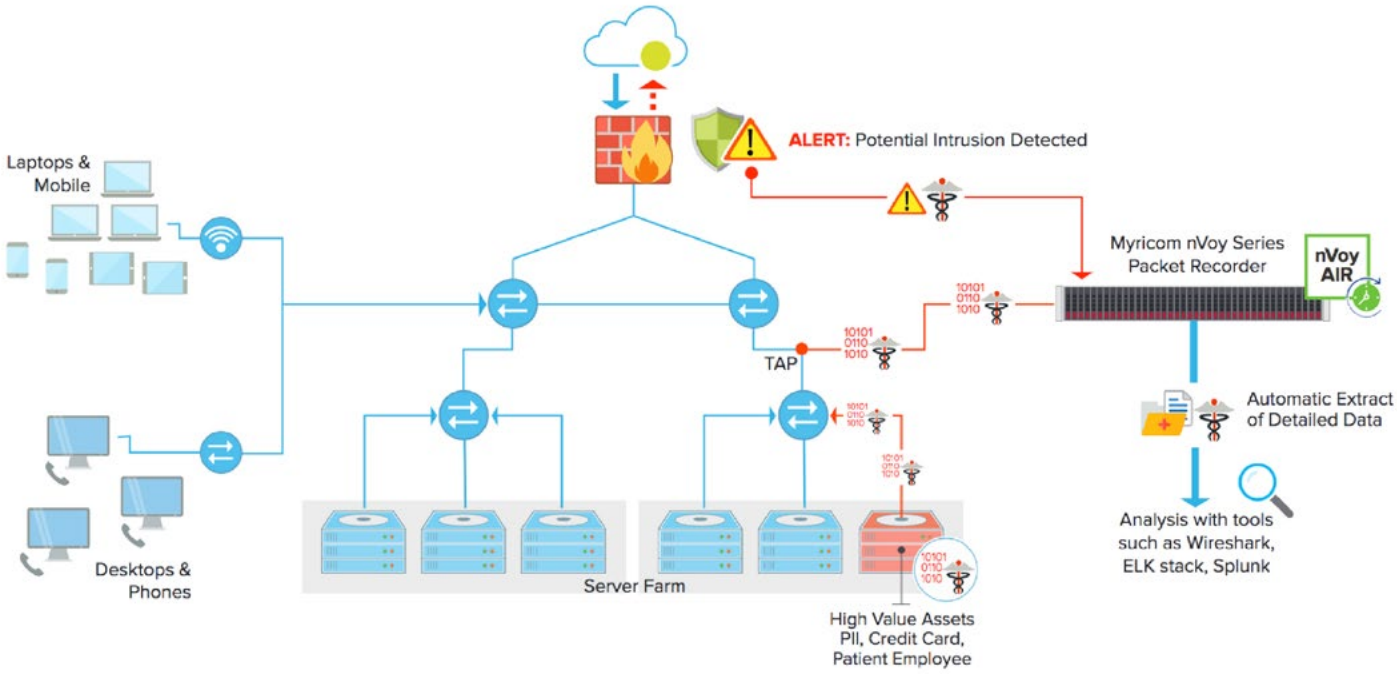

Figure 1: Myricom nVoy AIR watching critical assets and ready to respond to intrusion events.

FortiGate Enterprise Firewall

The Fortinet FortiGate network security platform provides high- performance, layered security services and granular visibility for end-to-end protection across the entire enterprise network. Innovative security processor (SPU) technology delivers high-performance application layer security services (next-generation firewall [NGFW], secure sockets layer [SSL] inspection, and threat protection), coupled with the industry's fastest SSL inspection engine, to help protect against malware

hiding in SSL/transport layer security (TLS) encrypted traffic. The platform also leverages global threat intelligence to protect individual customers, by using Fortinet FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

The Fortinet enterprise firewall solution delivers end-to-end network security with one platform, one network security operating system, and unified policy management with a single pane of glass—for the industry's best protection against the most advanced security threats and targeted attacks.

About CSPi

CSPi delivers a portfolio of cyber security solutions and services focused on rapid data breach response, enterprise-wide breach prevention and critical asset protection. Our solutions dramatically reduces incident response time by leveraging intrusion alerts from firewall or IDS/IPS tools to automate two critical components of the breach investigative process: breach verification and complete forensic data extraction. Security teams are able to quickly and cost-effectively determine the scope of a potential breach while meeting strict PII data privacy compliance requirements. Learn more at: www.cspi.com/nvoy.

August 27, 2021 4:37 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 2:sb-fortinet-cspi:sb-fortinet-cspi_2021

429109-A-0-EN