Virsec®

SentryWire
PACKET CAPTURE PLATFORM

Unprecedented Data Breach Prevention and Forensic Analysis with ARMAS™ and SentryWire™

The Challenge

- Zero-day and hard-to-detect memory-based attacks are steadily growing with an average 140 days, of invisibility
- High operational cost of deployment, management, monitoring
- Too little forensic data to piece together all important elements of the attack

Integrated Solution

- Real-time detection of zero-day and memory-corruption cyberattacks
- End-to-end capability spanning to incident forensic analysis with logging and network packet capture analytics.

Key Benefits

- Demonstrated benchmark results; near 100% accurate millisecond detection of data-borne attacks against web apps such as SQL injection or XSS
- Dramatically reduced alerts and more efficient use of analysts
- Precision on where and what formed an attack
- More focused incident response around data transfers or exfiltration attempts

Introduction

File-less, memory-based, and zero-day attacks are rising rapidly against enterprises. These attacks on critical applications and OS processes, as well as Internet-exposed server endpoints, can circumvent all traditional and next-generation endpoint solutions, including file whitelisting. Gartner estimates that over 80% of breaches have application involvement, either at the web layer or against underlying binaries that may be unpatched or use 3rd party components.

Initial infiltration into a network is just the first step in a sophisticated cyberattack. Once the bad actor has breached a network, implanting key loggers, installing backdoors, encrypting files, ex-filtrating business critical data, and migrating to other compute assets are all fair game. After the fact analysis of these attacks is time consuming, difficult, and often yields little information.

The ARMAS™ / SentryWire™ Joint Solution

Short of securely rewriting all of the binary underpinnings of an application from scratch, Virsec ARMAS is the only cyber security solution that imposes deterministic (non-signature-based) runtime control flow integrity on all layers of an application. This powerful new security enforcement approach enables ARMAS to detect and remediate both zero-day attacks and attacks against known vulnerabilities, within milliseconds of an initial attack or attempted infiltration.

This early warning counter measure system not only enables organizations to stop cyberattacks proactively, but now in combination with SentryWire, produces a detailed, near-real time trace of the actual traffic involved in the attack; giving organizations the ability to eliminate business disruption, collect evidentiary quality audit logs, and conduct forensic investigations.

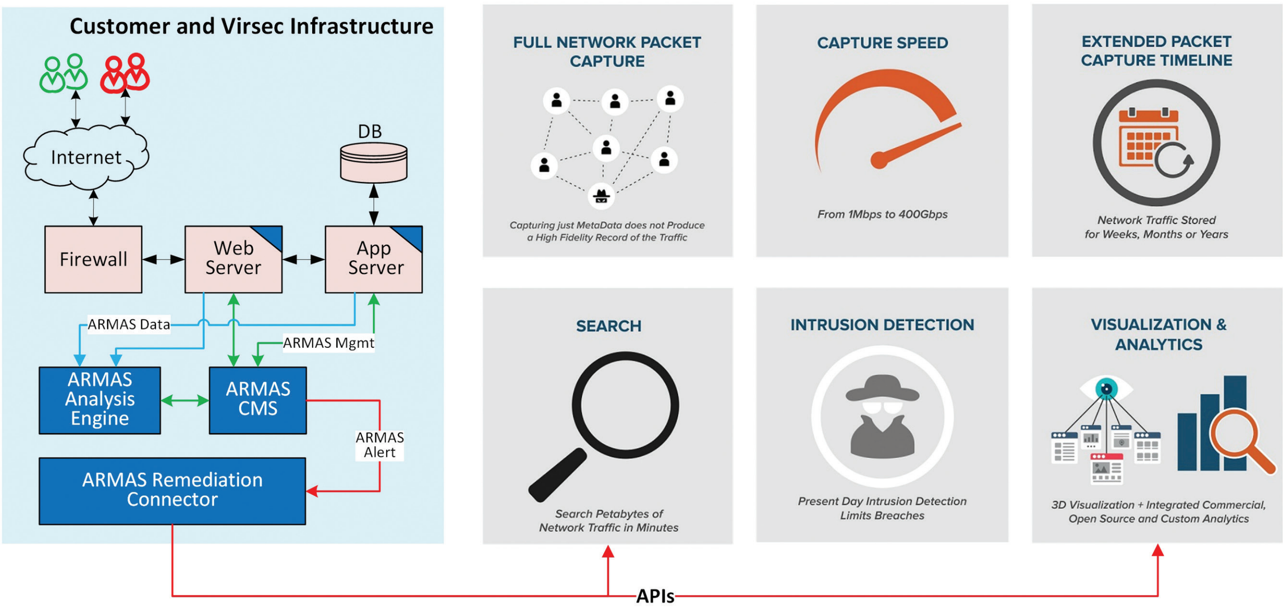
ARMAS™ contributes:

- Detection of Ransomware attacks, such as WannaCry, and any other file-less, memory-corruption attacks which exploit buffer error vulnerabilities in application processes
- Deterministic, near 100% accuracy for identifying and remediating web application attacks against .NET, Java, and other server-side interpreted code language applications
- Millisecond detection and proactive alerting to operations teams via the ARMAS monitoring environment and through SentryWire
- Records phases of a sophisticated cyberattack on server endpoints and their applications; i.e initial infiltration, weaponization actions; i.e dropping files, file system manipulations; i.e file privilege manipulations and/or footprint wiping

SentryWire™ contributes:

- A cost-effective solution for 100% full network packet capture with retention capabilities for months or even years' worth of packets, including traffic between virtual machines in the cloud
- Network Traffic analysis for deeper attack forensics and rollback of transactions against impacted data stores
- Real-time filtering for known IPS signatures and lossless capture rates from 1MB to 100Gbps
- Raw storage compression and compaction on the order of 5 to 30X and at roughly 20% of the cost of other packet capture solutions

Together, the joint solution enables security analysts and incident response personnel to be more effective and efficient in preventing and responding to network and data breach attempts. The combined data, visible under a single pane of glass, enables analysts to zero-in on servers where infiltration attempts are detected, with near certainty. Analysts can then examine network traffic data specific to the attack in highly focused ways within minutes and hours of the network breach, rather than months.


Customer and Virsec Infrastructure
Internet
DB
Firewall
Web Server
App Server
ARMAS Data
ARMAS Mgmt
ARMAS Analysis Engine
ARMAS CMS
ARMAS Alert
ARMAS Remediation Connector
FULL NETWORK PACKET CAPTURE
Capturing just MetaData does not Produce a High Fidelity Record of the Traffic
CAPTURE SPEED
From 1Mbps to 400Gbps
EXTENDED PACKET CAPTURE TIMELINE
Network Traffic Stored for Weeks, Months or Years
SEARCH
Search Petabytes of Network Traffic in Minutes
INTRUSION DETECTION
Present Day Intrusion Detection Limits Breaches
VISUALIZATION & ANALYTICS
3D Visualization + Integrated Commercial, Open Source and Custom Analytics
APIs

About SentryWire

SentryWire, a Division of Alliance Technology Group, is engineered and architected to be the most efficient packet capture solution on the planet. The system supports capture rates up to 100Gbps and retains network traffic for months and even years at 20% the cost of other systems.

Learn more at **www.sentrywire.com**

About Virsec

Virsec is pioneering runtime control flow integrity (Trusted Execution™) for enterprises and enabling unprecedented advanced hacking and data breach prevention on critical applications and server endpoints.

Learn more at **www.virsec.com** or connect with Virsec on **Twitter** and **Facebook**.