CSPi

CSPi Security Solutions for Secure DevOps & Enhanced Network Security

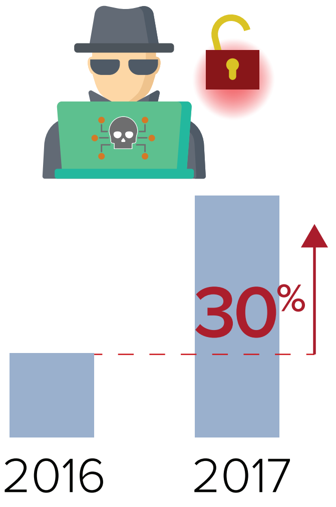
New Security Challenges Call for **New Security Approaches**

Onslaught of Data Breaches Demands Change

Organizations of all sizes and across all industries are the targets of an increasing number of sophisticated cyber attacks. The risk of breach is very real, and gets worse every day.

The industry recognizes that approaches such as threat prevention and breach detection are ineffective. For proof, just consider the recent IRS, Equifax, and Anthem breaches. These organizations' big security investments led them to believe they could detect threats before data loss could occur – until they failed.

How can we improve? Patching vulnerabilities quickly is part of the answer, but is not sufficient. Organizations need better methods and tools to secure their environments and protect their applications and their high-value data no matter where it resides. Placing priority on application defense and a more effective means to leverage their network traffic to see and immediately stop threats puts companies on a success path to eliminating the damage a data breach can cause.



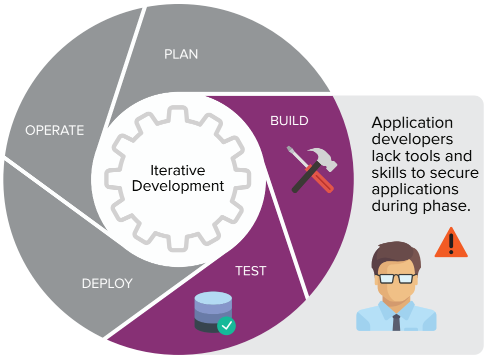
Cyber attacks and breaches continue to grow

Secure DevOps for True Application Security

Any new security solution must allow companies to easily and effectively secure applications created through DevOps or traditional development methodologies. The DevOps model speeds up development through rapid iterative deployment and

1010100101011
1010101010010010110101

improvement – yet the onus is put on the developers to secure the applications and the data they handle or create.


PLAN
OPERATE
BUILD
Iterative Development
TEST
DEPLOY
Application developers lack tools and skills to secure applications during phase.

Security considerations are generally not part of the early stages of DevOps models, which contributes to increased vulnerabilities and new risks.

Yet something is missing. Application developers generally don't have the right skills or tools to add sophisticated security features into the development process. While they may be able to include limited functions into their build process, such as automated vulnerability scans, these efforts simply aren't enough.

Companies must move beyond mere vulnerability detection to achieve secure DevOps. This level of security is important and required, but it is not sufficient to protect applications and the data they produce. This means that companies need a new way to control what can access an application, and then protect data as it is created, transmitted, and stored. Only this level of security will provide the required protection level to defeat attackers internally and externally.

Proper protection comes down to adding two additional functions:

1. Controlling who and what can connect to and application
2. Protecting the application and the data with the appropriate level of protection via encryption techniques

Your Network Can Tell You Everything

Network security isn't new, but it needs to work better for today's challenging environments. Today's threat detection techniques have primarily focused on monitoring the perimeter and end points for issues and threats. Attempts to monitor everything in between, like east-west traffic, has proven to be ineffective, and yet this is where the greatest blind spot lies, inhibiting the ability to properly detect threats and issues once they are inside the organization.

Up until now, organizations haven't been able to fully tap transparently into their network traffic at line rates in order to have the visibility needed to find threats and violations of connection policy. However, new tools now exist that not only provide actionable intelligence about what is happening in the network. These tools can take automated and immediate action to stop connectivity that violates policy or redirect specific traffic flows for deeper inspection as well as send such flows for forensic capture for compliance purposes. Such tools make DLP and IDS/IPS tools more effective by sending them only relevant traffic flows to screen. This allows them to scale and optimizes traffic flows and application response time.

Such a solution empowers security professionals the ability to visualize their network data, at line rate, classify the flows, and take action on these flows as appropriate.

CSPi's Security Solutions:

ARIA Software-Defined Security (SDS) Platform

CSPi's ARIA™ SDS platform takes a radically different approach to enterprise-wide data security with a focus on both enhancing network security application data impenetrability, to fill the gaps in order to stop data loss and misuse. ARIA's fully automated capabilities enable organizations to address secure DevOps challenges and protect critical data, on-premise or in public clouds no matter whether it is in use, in transit, or at rest.

The ARIA platform automatically applies the organization's appropriate contextually aware security policies – where it's needed most: at the servers or in the network. Additionally, the ARIA Orchestrator automatically discovers the ARIA instances and manages the application of the appropriate type and level of security services upon deployment.

The central execution, across an entire organization, using a single pane of glass, ensures the desired access controls, micro-segmentation, encryption service types and levels, and other service techniques are correctly applied – no matter where the applications are running.

Benefits:

- Easy application security
- Impenetrable data protection
- Automatic policy application

Secure DevOps with ARIA

Easy Application Security

Imprenetable Data Protection

Automatic Policy Application

ARIA SDS Applications

It is the use of ARIA SDS applications that bring life to the ARIA platform. These applications can be easily deployed anywhere in the environment – containers, VMs, our own Myricom Secure Intelligent Adapter (SIA) – wherever they are needed, with little effort and next to no specialized knowledge, to fully protect and secure an organizations applications and high-value data no matter where it resides, is used, or accessed.

ARIA Packet Intelligence Application:

- Monitor east-west as well as north-south data to generate analytics and classify traffic without performance impact.
- Mine Netflows and Application IDs – export for visibility.
- Classify traffic and application level flows – allowing better intelligence gathering.
- Take immediate action – preprogramed as per policy, driven automatically via APIs, or directly as instructed by SOC team actions.
- Drop and alert upon specific data flows being sent to/from unapproved destinations.
- Redirect or send copies of select traffic streams for deeper inspection through rules-based detection applications (DLP, IDS/IPS) to detect threats or stop potential leaks of PII/PHI information.
- Directs copies of specific traffic streams for forensic recording.

ARIA Application Defense Application:

- Easy for developers to add and connect its lightweight agents when building their application using standard DevOps practices.
- Automatically discover agents with the ARIA Orchestrator, which programmatically uploads and activates the proper security features.
- Provides instant notification to InfoSec teams when new agents appear and can set or change such polices as the applications come live – without involving developers or operations.

ARIA KMS Application:

- Key management application–serves and manages encryption keys for storage and HCI deployments, including VMware® vSPHERE 6.5, enabling VM and vSAN encryption.
- KMIP 1.4 based – Securely serves keys and certificates to any KMIP-based application, as well as through a simple to use API for all other applications. FIPS 140-2 compliant.
- Enables “bring your own key” for cloud application as well as on-premises deployments. Simple zero-touch deployment, configuration, and management, including high availability options where multiple KMS act as one solution for zero downtime.
- Deployable on the Myricom SIA for high performance/high capacity key serving with full FIPS 140-2 level 3 compliance.

ARIA microHSM Application:

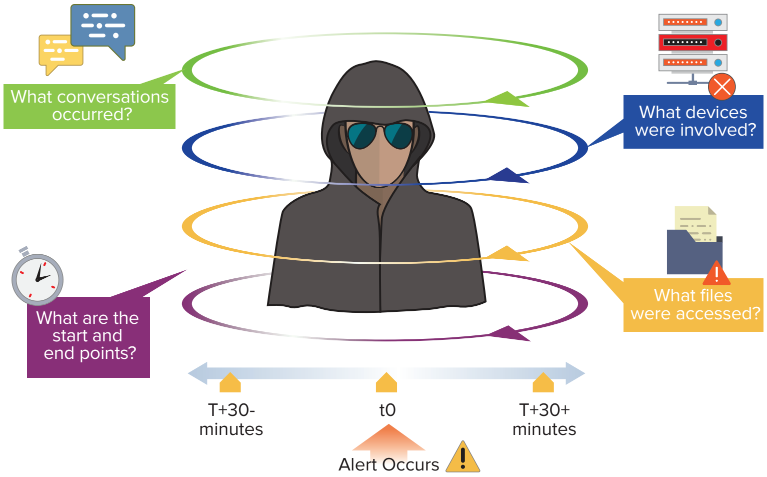
- Fully secured high performance PCIe adapter-based HSM – locally offloads and fully secure key management and encryption functions from the servers Intel x86 cores.
- Generates and caches keys locally in its protected TrustZone. Unlike x86 deployments, its keys are not vulnerable to Meltdown, Spectre, Foreshadow NG,, and whatever comes next.
- Handles over 900,000 crypto operations per second. Capable of uniquely encrypting each application’s traffic separately and/or each transaction separately to meet the latest compliance requirements for PII/PHI.

nVoy Compliance Assurance Solution

CSPi’s nVoy Series works with ARIA to automatically verifies breaches against critical assets and immediately notifies, as well as dispatches a report containing all of the conversations between devices – providing concrete proof required to avoid compliance fines from GDPR, DSS PCI, and 23 NYCRR 500.

Benefits:

- Meet compliance deadlines
- Complete investigations in hours
- Pinpoint PII records that may have been impacted
- Provide the evidence needed for audit and compliance


What conversations occurred?
What devices were involved?
What files were accessed?
What are the start and end points?
T+30- minutes
t0
T+30+ minutes
Alert Occurs

Myricom Network Adapters

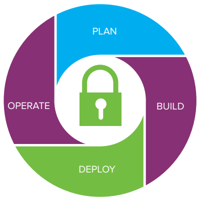
The Myricom lines of network adapters have a long, successful history in network monitoring and intelligence made famous by their success in fighting the war on terror.

- ARC Series of 1/10G adapters with Sniffer10G provide pure-packet processing as well as zero-loss reliability, user-defined functionality, and the ability to improve network security – representing a significant value over competitive products.
- The Secure Intelligent Adapter (SIA) 25/50G works seamlessly with the ARIA platform to offload and accelerate security functions such as key management, data encryption, compression, packet capture, and traffic monitoring and classification.
- Network Probe appliance – Provides bump on the wire deployments of the Myricom line of adapters.

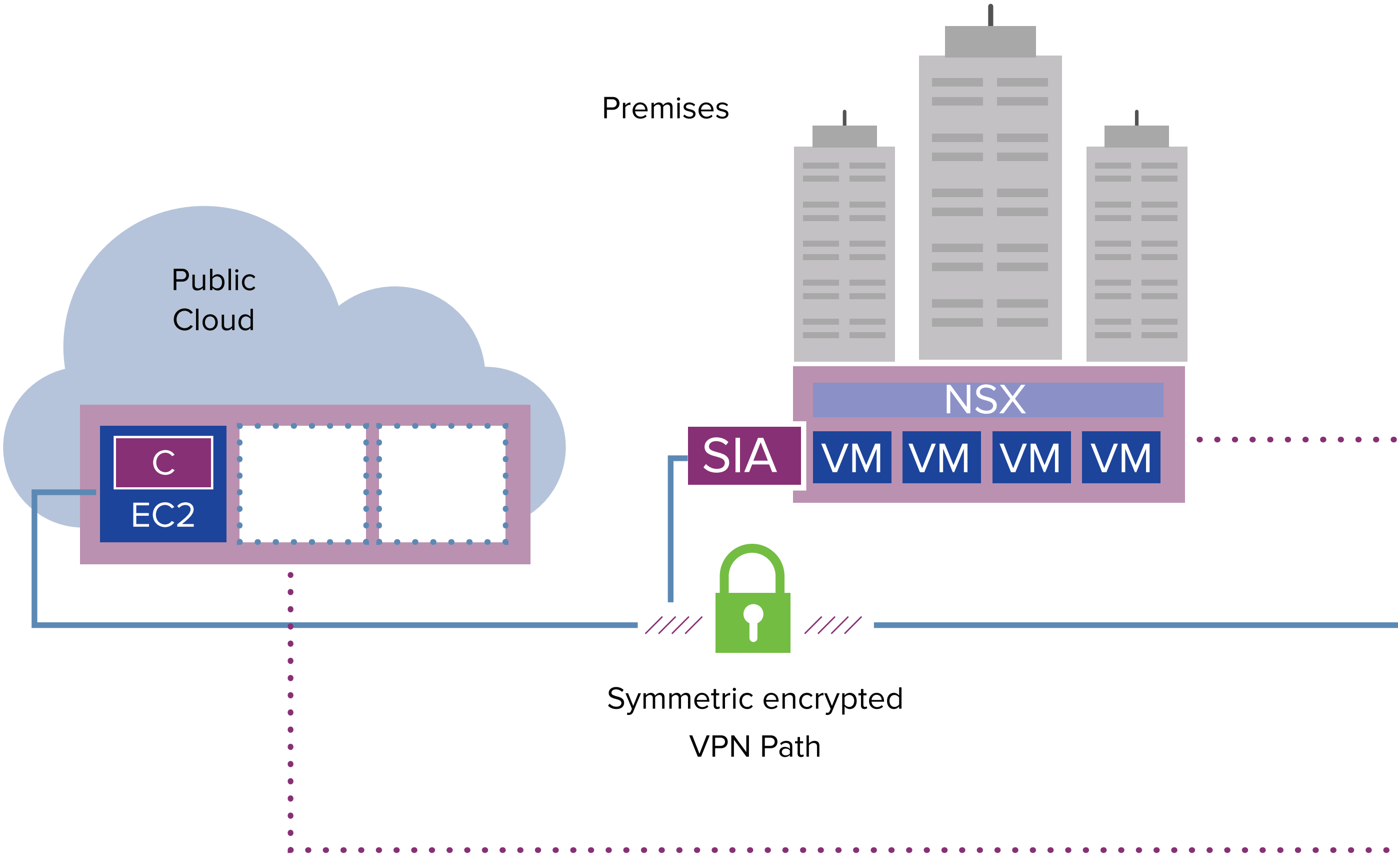
Benefits:

- Dropless packet capture, indexing, and time stamping at line rate
- Offload CPU-intensive security functions
- Reduce costs by eliminating the need for software-based encryption or server upgrades
- Improve security with impenetrable encryption key storage and execution

CSPi



Secure DevOps with **ARIA SDS**



ARIA SDS Applications:

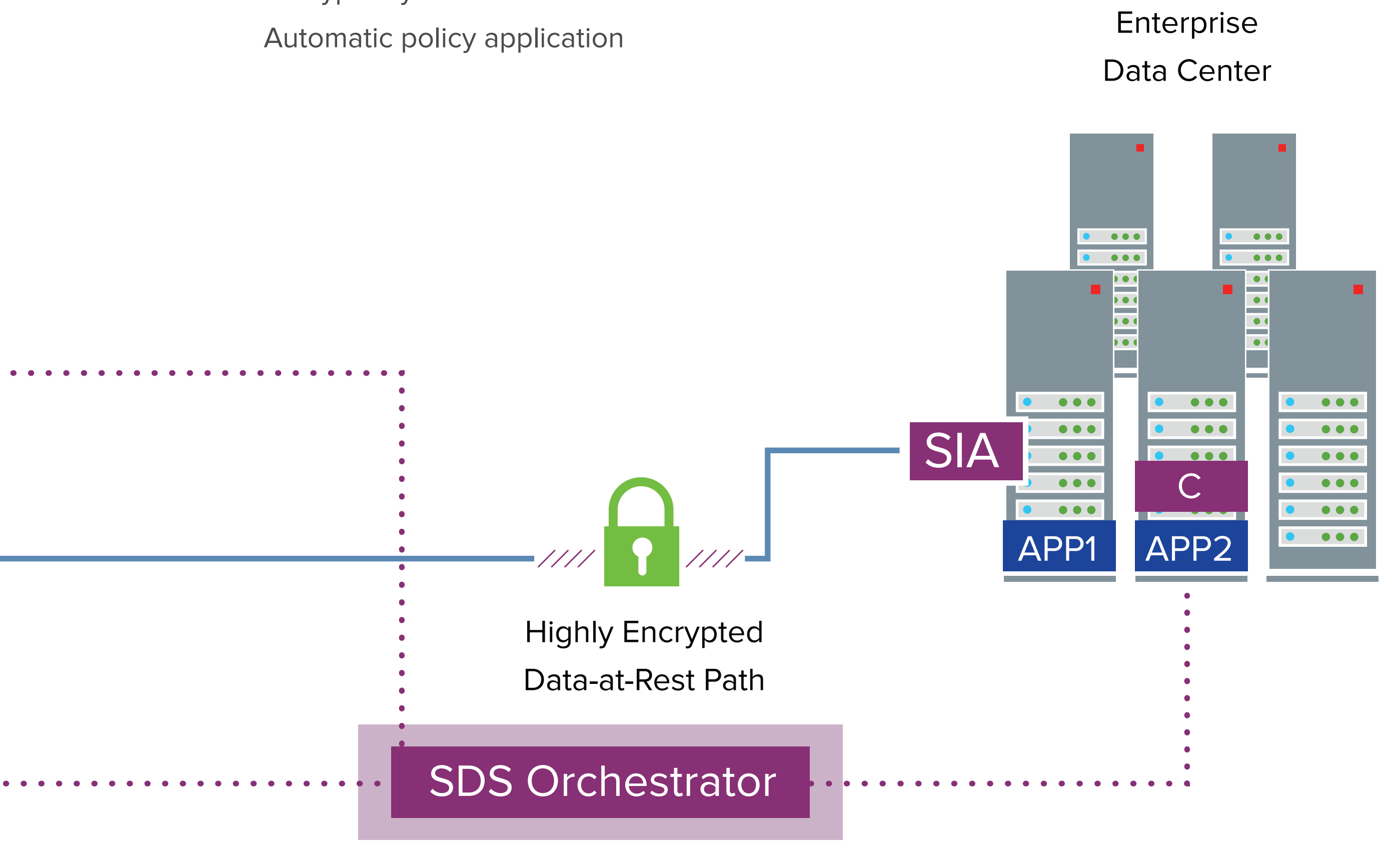
- microHSM
- Key Management Server
- Microsegmemtation

CSPi's ARIA™ SDS platform takes a radically different approach to enterprise-wide data security. The focus is data impenetrability vs data breach prevention. ARIA's fully automated capabilities, enables organizations to address Secure DevOps challenges, and protects critical data on-premise and in the public cloud no matter whether it is in use, in transit or at rest.

Easy App Security

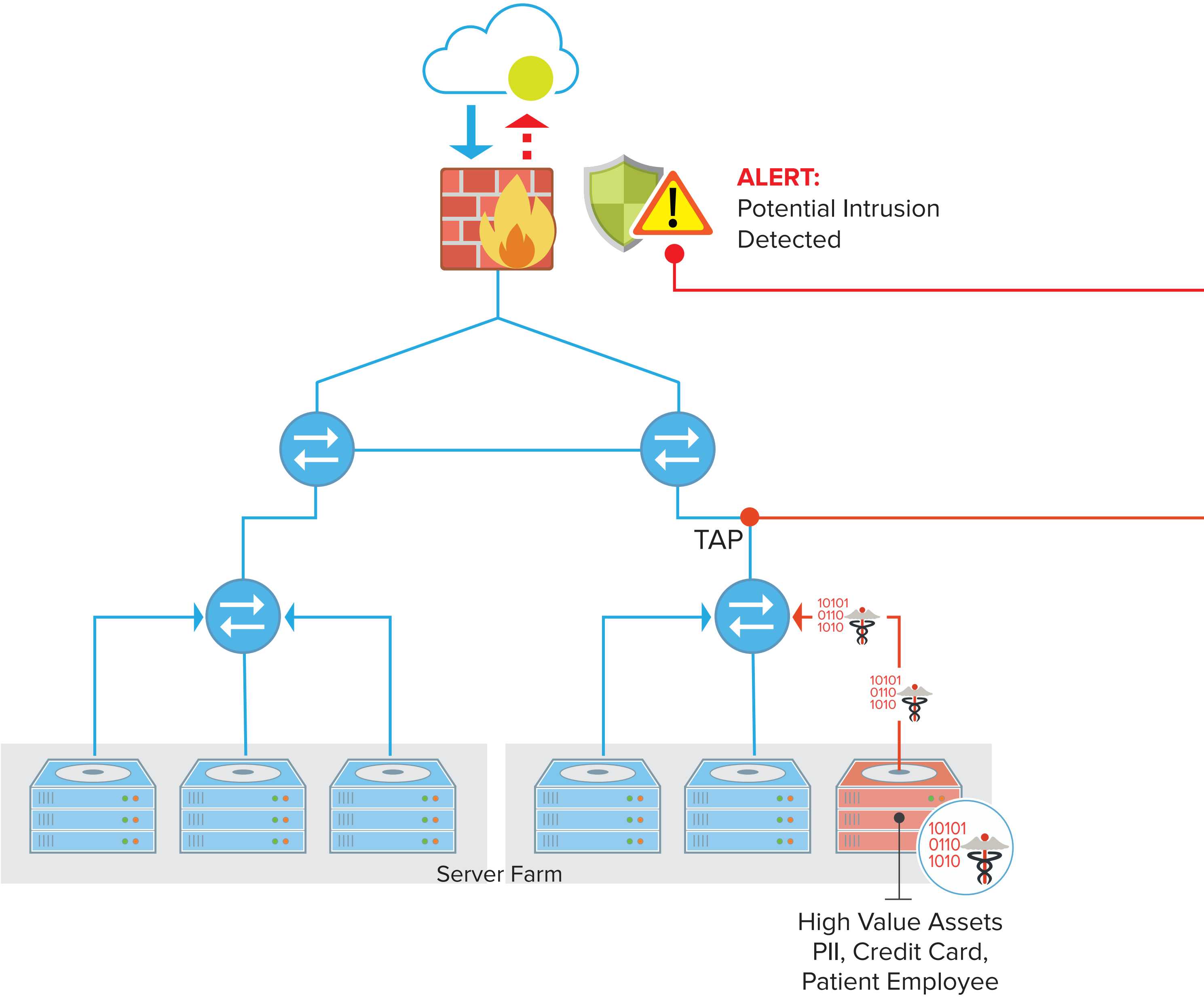
Encrypt any data

Automatic policy application



Winner of Leading Security Awards for Best New Product

Auto Breach ID + Notification with nVoy Series

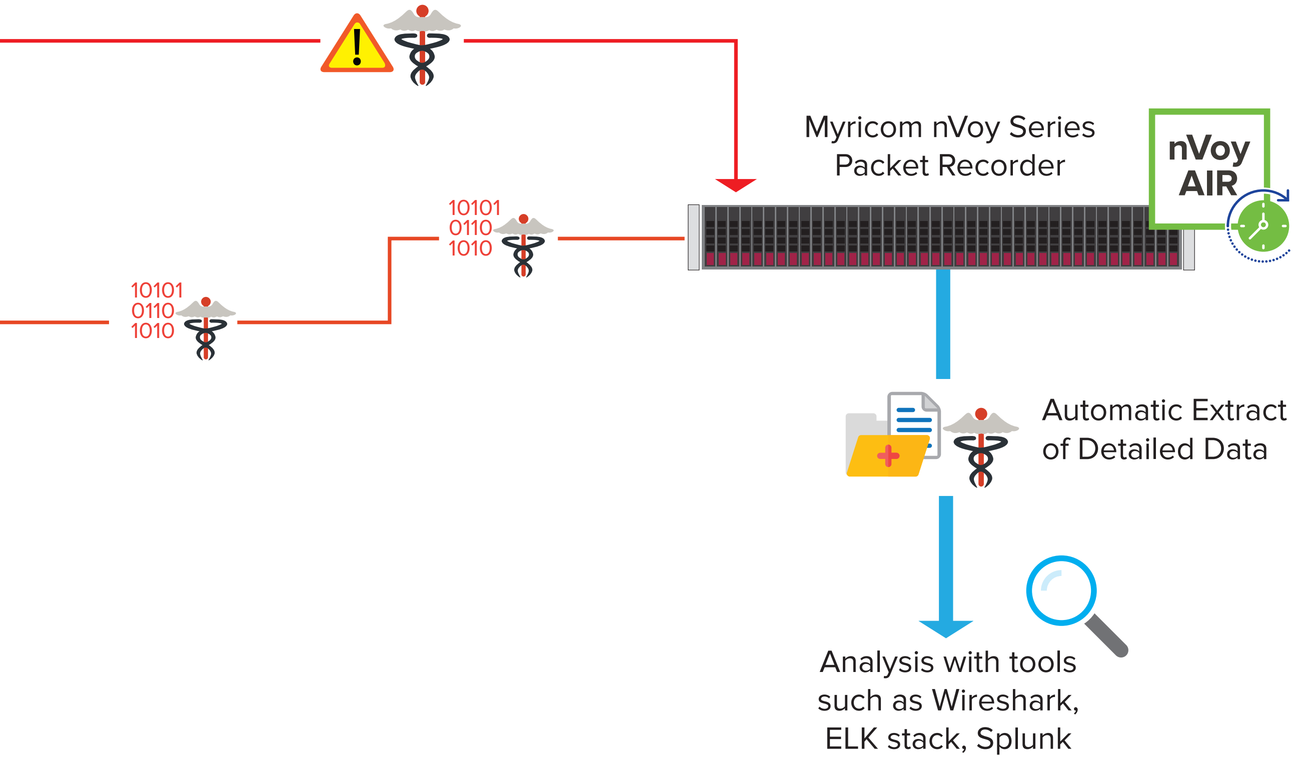


CSPi's Myricom® nVoy Series automatically verifies breaches against critical assets and immediately dispatches a report containing all conversations between devices– providing the concrete proof required to avoid compliance fines including GDPR, DSS PCI and 23 NYCRR 500.

Meet compliance deadlines

Complete investigation in hours

Pinpoint PII records impacted



Myricom nVoy Series Packet Recorder

Automatic Extract of Detailed Data

Analysis with tools such as Wireshark, ELK stack, Splunk

Compatible with firewalls including:

FORTINET paloalto NETWORKS CISCO JUNIPER NETWORKS

Comprehensive security solutions. Complete business results.

Today's companies require efficient and effective security solutions, capable of protecting their most critical data and allowing for the rapid scale, deployment, and management of their business data – no matter where it travels or resides. CSPi's security solutions delivers on this potential, while also giving application developers and InfoSec teams a proven way to achieve Secure DevOps, and improve network security reaping all of their related benefits.

Organizations need a simple, yet cost-effective solution for enterprise-wide security that meets the following goals:

- Has no negative impact on business operations and ideally reduces time to secure application deployment.
- Provides a complete security approach to not only protect east-west and north-south traffic, but also secure all the packet-level data at rest, in motion, and in use.
- Can be easily deployed in any environment, including private networks and data centers, public clouds, or hybrid environments, and dosen't require any significant infrastructure changes.
- Gives developers the tools they need to easily, and quickly secure applications during development without changing the normal development approach, thus ensuring the security of production-level data.
- Allows the operations team, in particular the InfoSec Ops team, to independently set policies as applications appear and to quickly adapt such rules to application deployment and usage.
- Programmatically applies the organization's appropriate security policies to the applications, servers, virtualized machines, cloud instances and containers as they grow and scale.
- Offloads core-intensive security functions to allow for such features to run in legacy server environments without application performance issues.

About CSPi

CSPi (NASDAQ: CSPi) is a global technology innovator driven by a long history of business ingenuity and technical expertise. A market leader since 1968, we are committed to helping our customers meet the demanding performance, availability, and security requirements of their complex network, applications and services that drive success.

CSPi Corporate Headquarters
175 Cabot Street - Suite 210
Lowell, MA 01854
800.325.3110 (US & Canada)

CSPi High Performance Products
800.325.3110 (US & Canada)
us-hpp-sales@cspi.com

CSPi Technology Solutions
800.940.1111
us-ts-sales@cspi.com

www.linkedin.com/company/csp-inc

@ThisIsCSPi

us-hpp-sales@cspi.com

www.cspi.com

All companies and logos mentioned herein may be trademarks and/or registered trademarks of their respective companies.

www.cspi.com