Guardians of the Connected World

Our Solutions

Powered by the Visibility Without Borders Platform

nGenius Enterprise Performance Management

- Mission Critical Apps
- Remote and Hybrid Workforce
- UCaaS and Collaboration
- Hybrid Multi-cloud Migration

Taps and Packet Flow Switches

- In Line Taps
- Packet Flow Switches
- High speed decryption appliances

Omnis Network Security

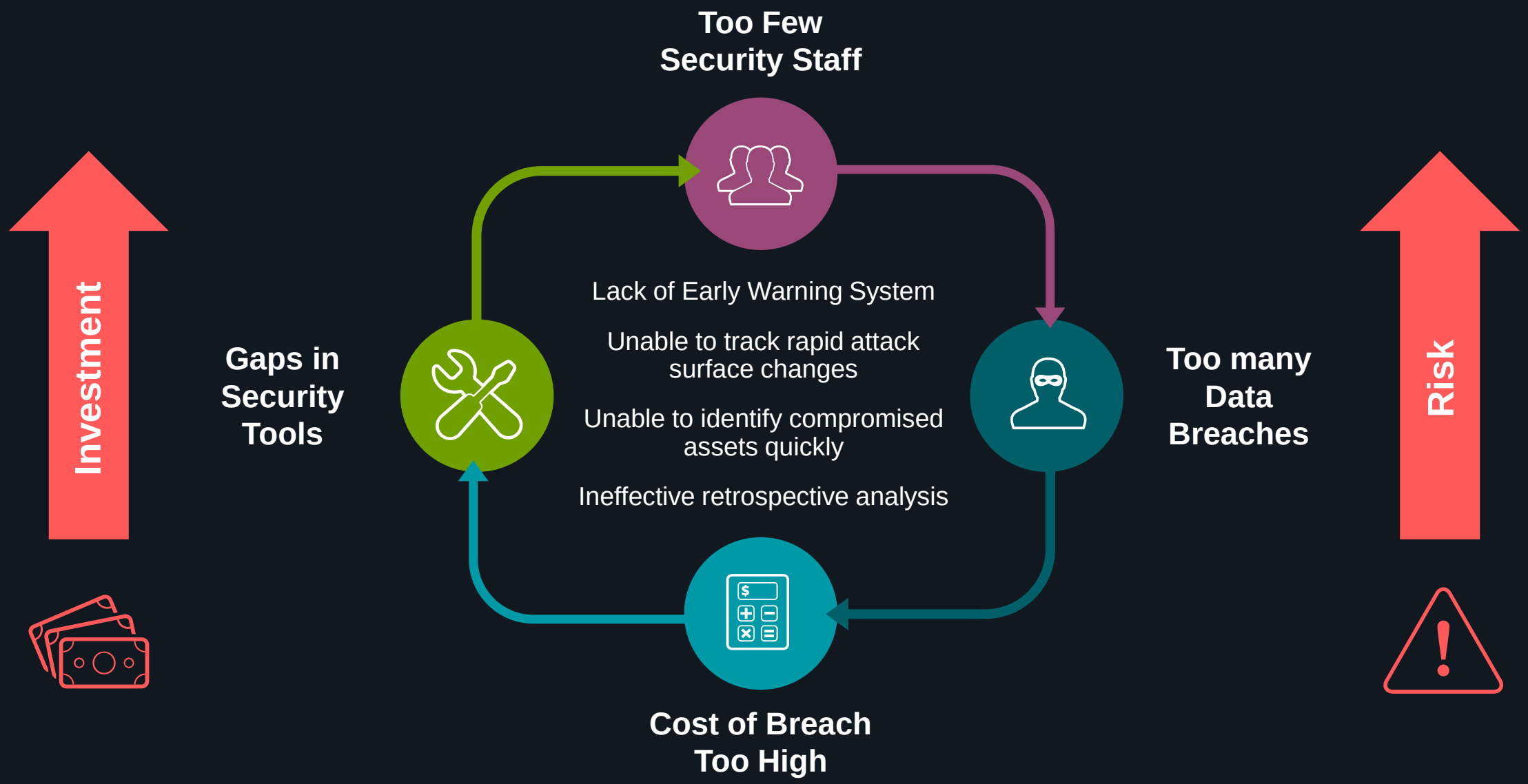
- Comprehensive Network Visibility
- Cyber Threat Detection
- Ecosystem Integration

Arbor DDoS Protection

- Pervasive Network Visibility
- Adaptive DDoS Protection
- Global Threat Intelligence

The real-time network visibility platform for performance, security, and availability, at any scale.

Big Picture Challenges for Cybersecurity…



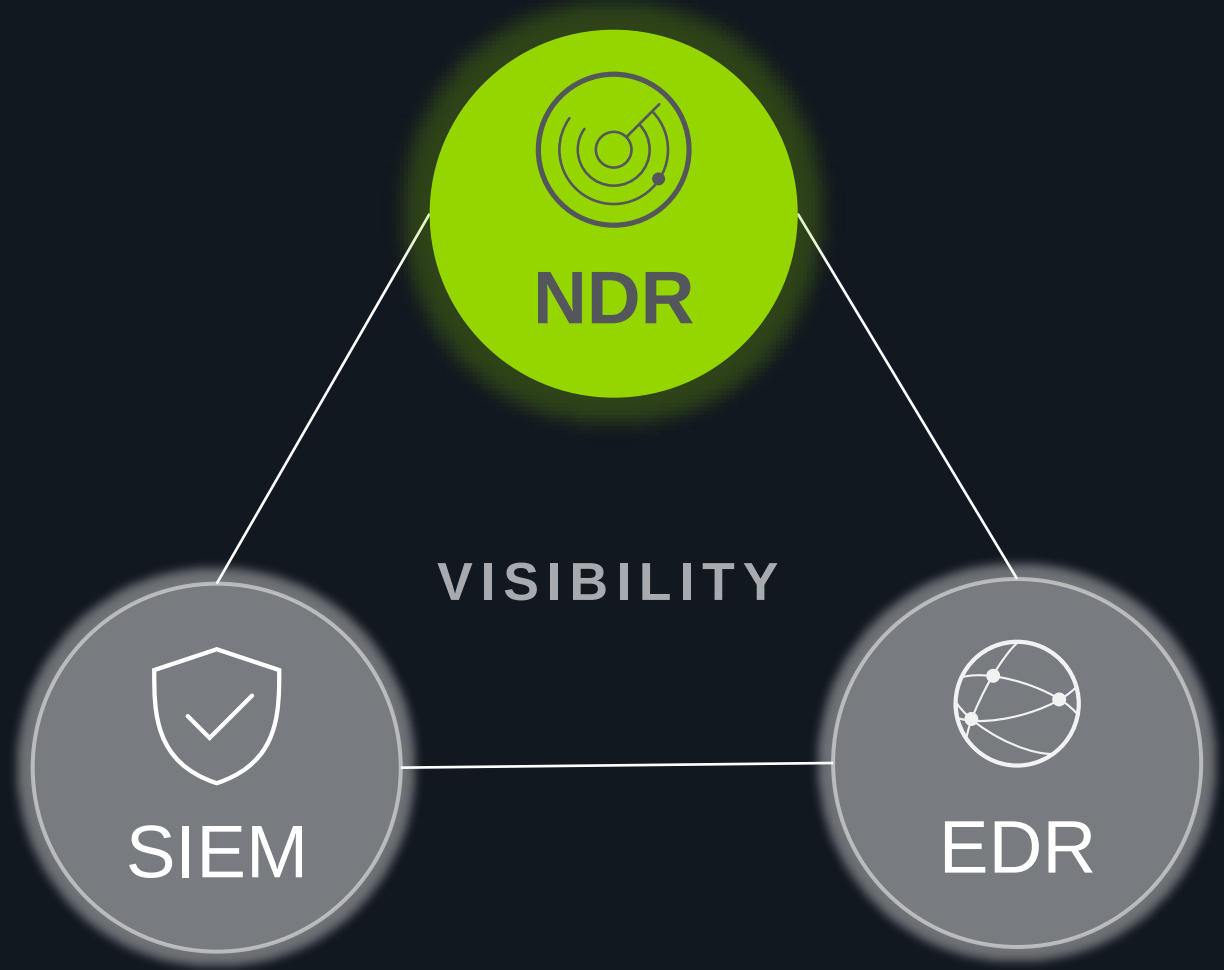
Current State of Security Technology

Hackers Continue to Beat the “Good” Guys While Security Spend Skyrockets

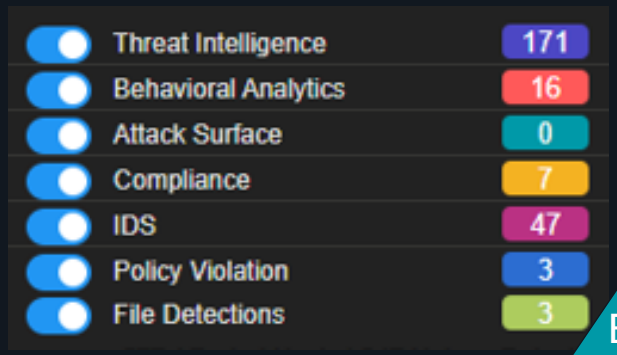
- Security technology today is primarily focused on threat mitigation using tools like NGFW, IDS, NDR, SIEM, EDR etc. These technologies often focus on sophisticated detection algorithms on top of a poor and noisy data set.
- Despite all the spend driven by fear-factors, attacks continue to rise unabated and ransomware breaches are at all-time high. Hackers and malicious elements are always one step ahead.
- To address this, we need a **risk-focused approach** (rather than a threat-focused one) that can reduce the Mean Time to Restore to minutes instead of days or weeks.

The SOC Visibility Triad (Gartner)

- *"You can't protect yourself from what you can't see"*
- Three main sources of SOC visibility: SIEM, EDR, NDR
- Each has its pros and cons, but security teams need all three to detect, investigate and remediate threats.



Multiple Detection Methods (DM)



PLUS -MITRE ATT&CK –at source Configurable & Extensible

Behavior of an individual user or host, or a group of hosts or users, that deviates from the locally norm. MITREE ATT&CK mapping.

Unexpected internal-to-external traffic patterns (Attack Surface Events)

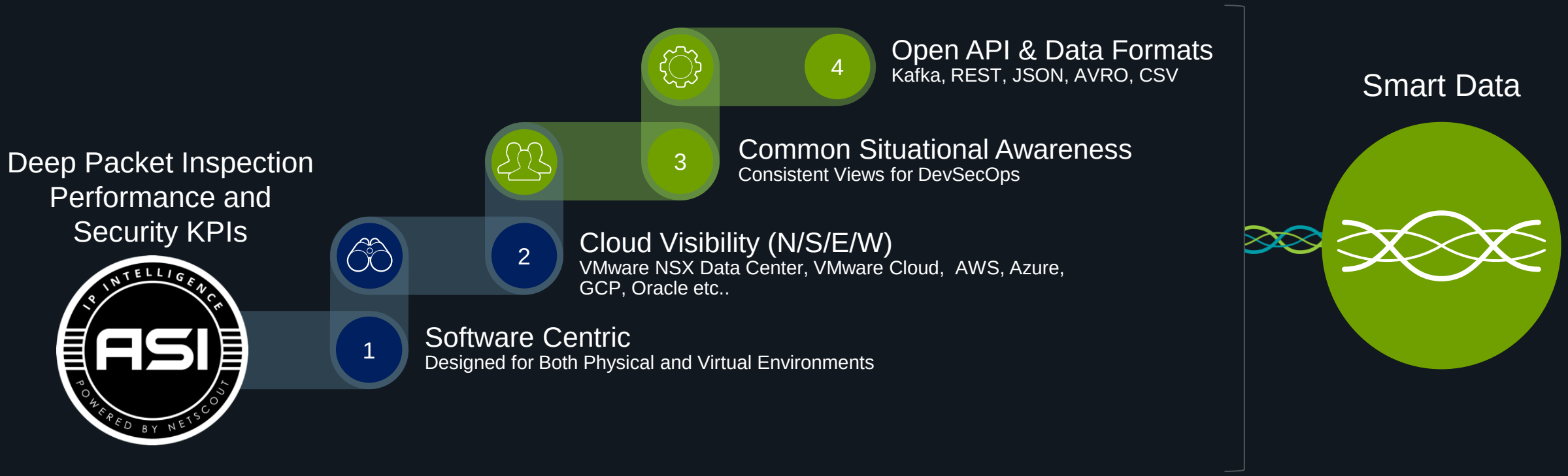
Specific pattern or set of characteristics to identify known malicious activity or threats and files (Suricata-based rules and signatures)

Use of configuration information to detect access violations, validation of compliance and network access policy configuration rules (Uses Host Groups definitions)

Specific pieces of evidence/IoCs (ex. known bad IP, URL, DNS) to indicate a security breach or malicious activity has occurred.

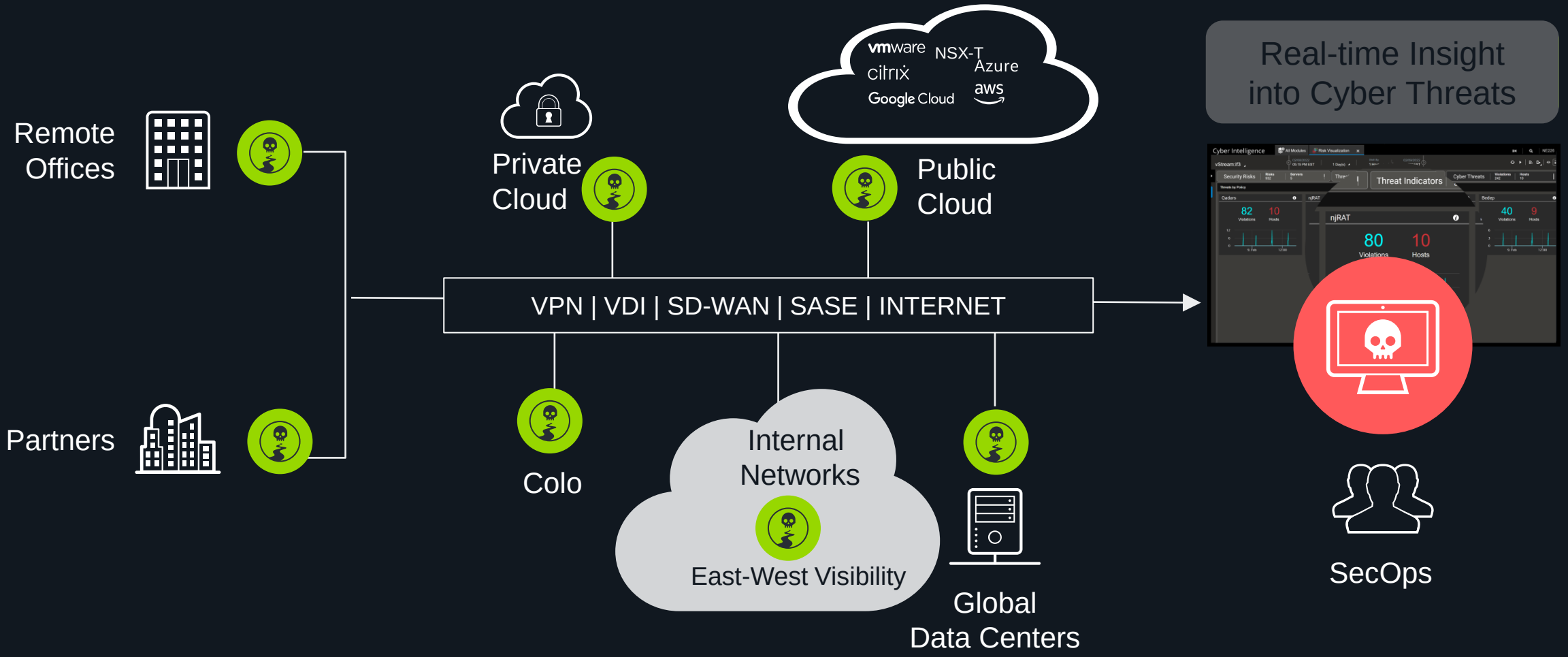
What is Smart Data?

Smart Visibility into Network, Applications, Dependencies, and Security



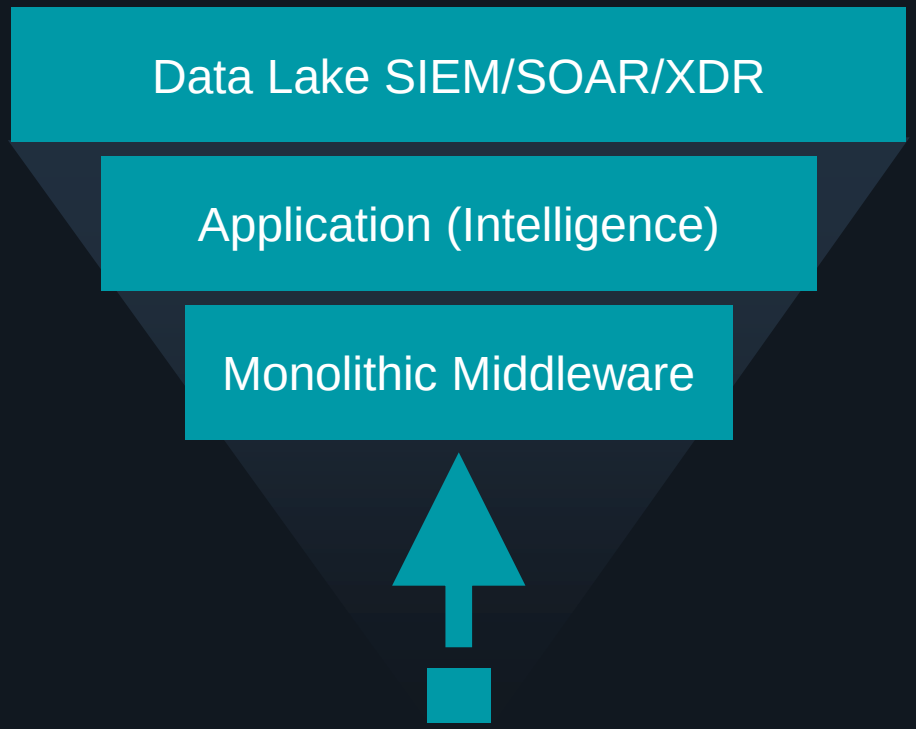
Preferred NDR Deployment

Wherever Workloads and Users are Located



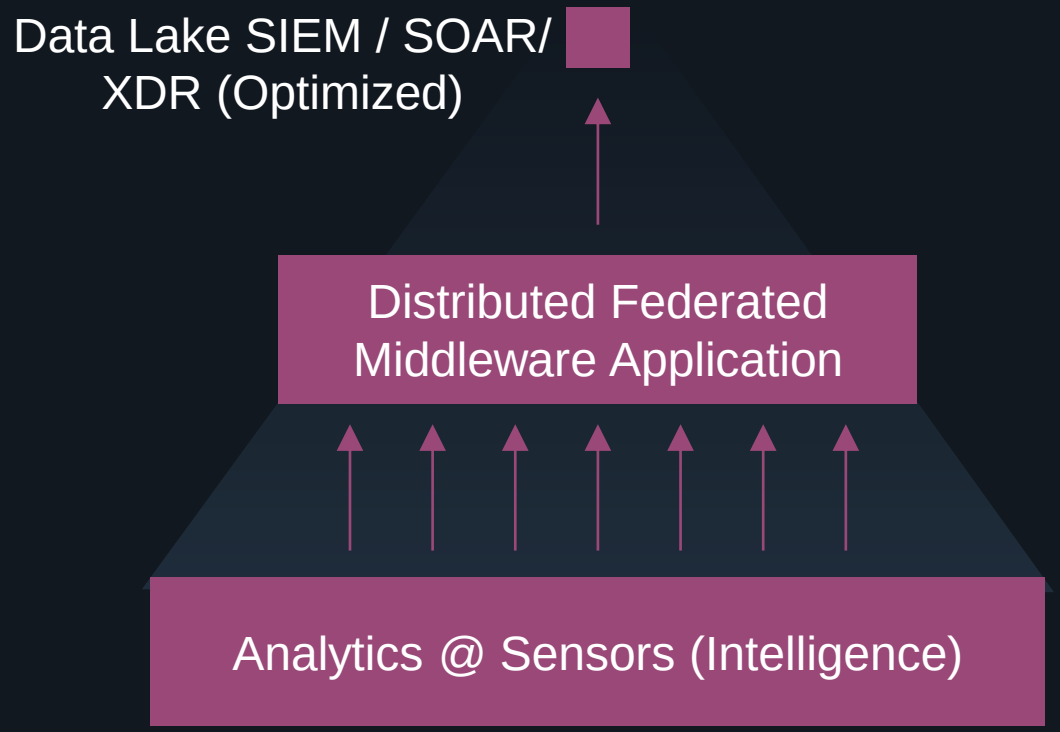
NDR Architecture Redefined

Industry Present Mode of Operation
Centralized



- Intelligence in middleware/ higher layers (higher cost)
- Weak historical depth
- Point Products

NETSCOUT
Disaggregated (Hierarchical)



- Intelligence in distributed sensors provides Visibility without Borders at less cost).
- Confidential, historical data kept local vs in public, multi-tenant, expensive cloud.
- Platform approach (starts with proprietary packet broker, decryption)

IDS detections:

Signature-based Detection

String signatures:

The string signature engines support regular expression pattern matching and alarm functionality.

Connection signatures:

They generate an alarm based on the conformity and validity of the network connections and protocols.

DoS signatures:

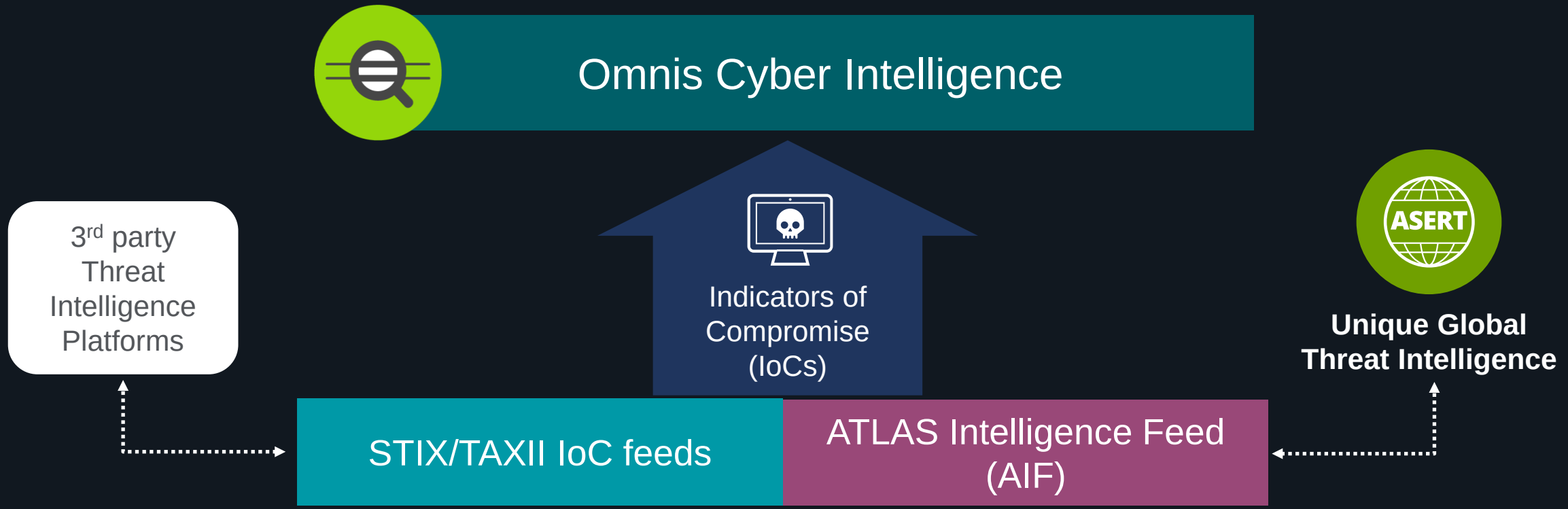
They contain behavior descriptions that are considered characteristics of a DoS attack.

Exploit signatures:

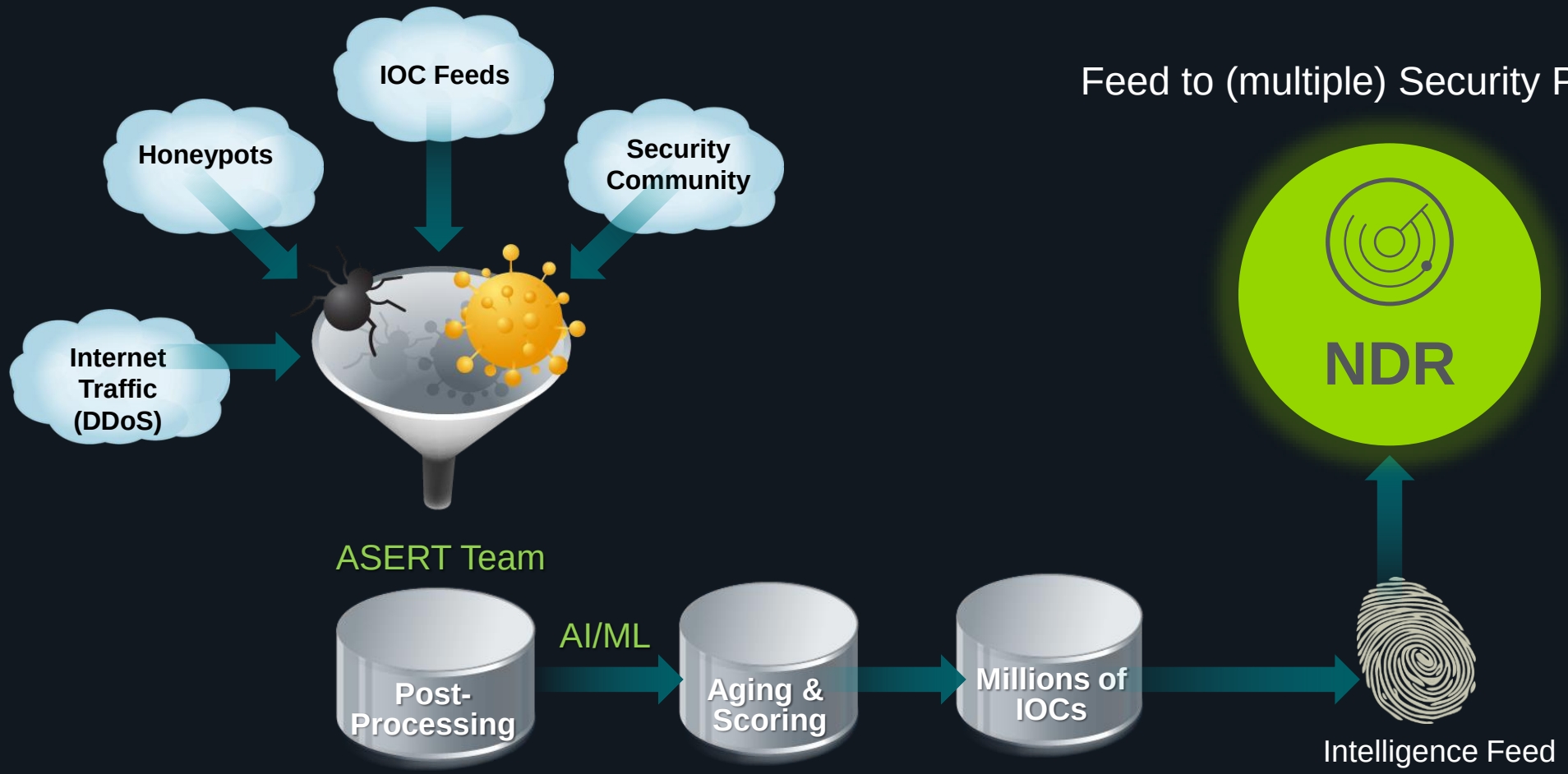
They typically identify a traffic pattern that is unique to a specific exploit; therefore, each exploit variant may require an individual signature. Attackers may be able to bypass detection by slightly modifying the attack payload. One often must produce an exploit signature for each attack tool variant.

Cyber Threats – IoC support

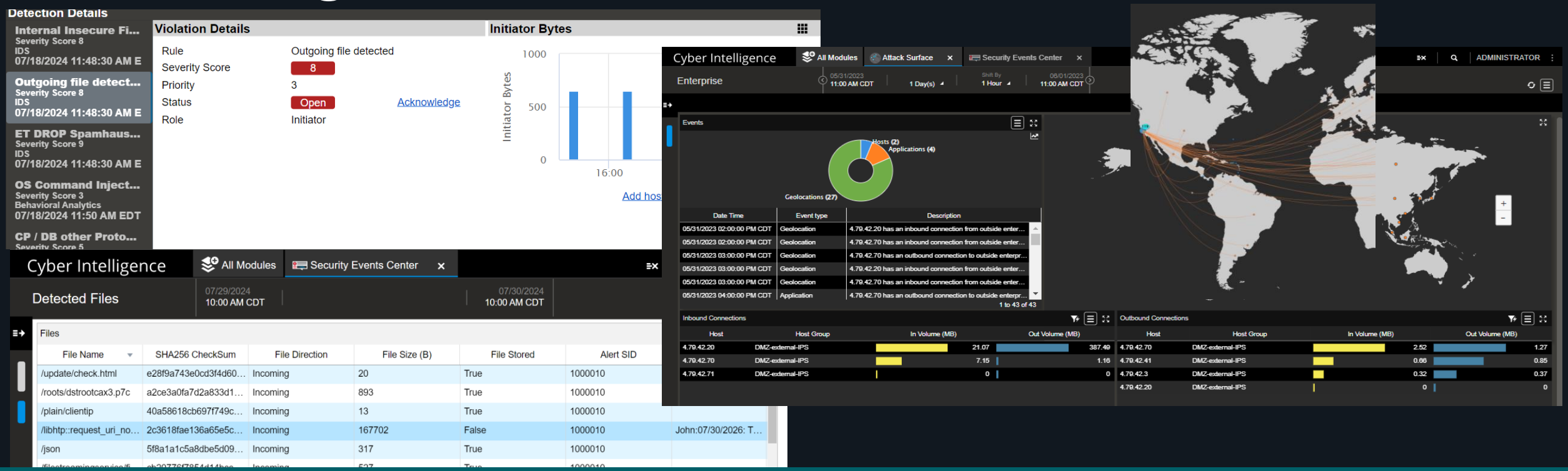
Signature Matching with IoC feeds



A highly curated intelligence feed



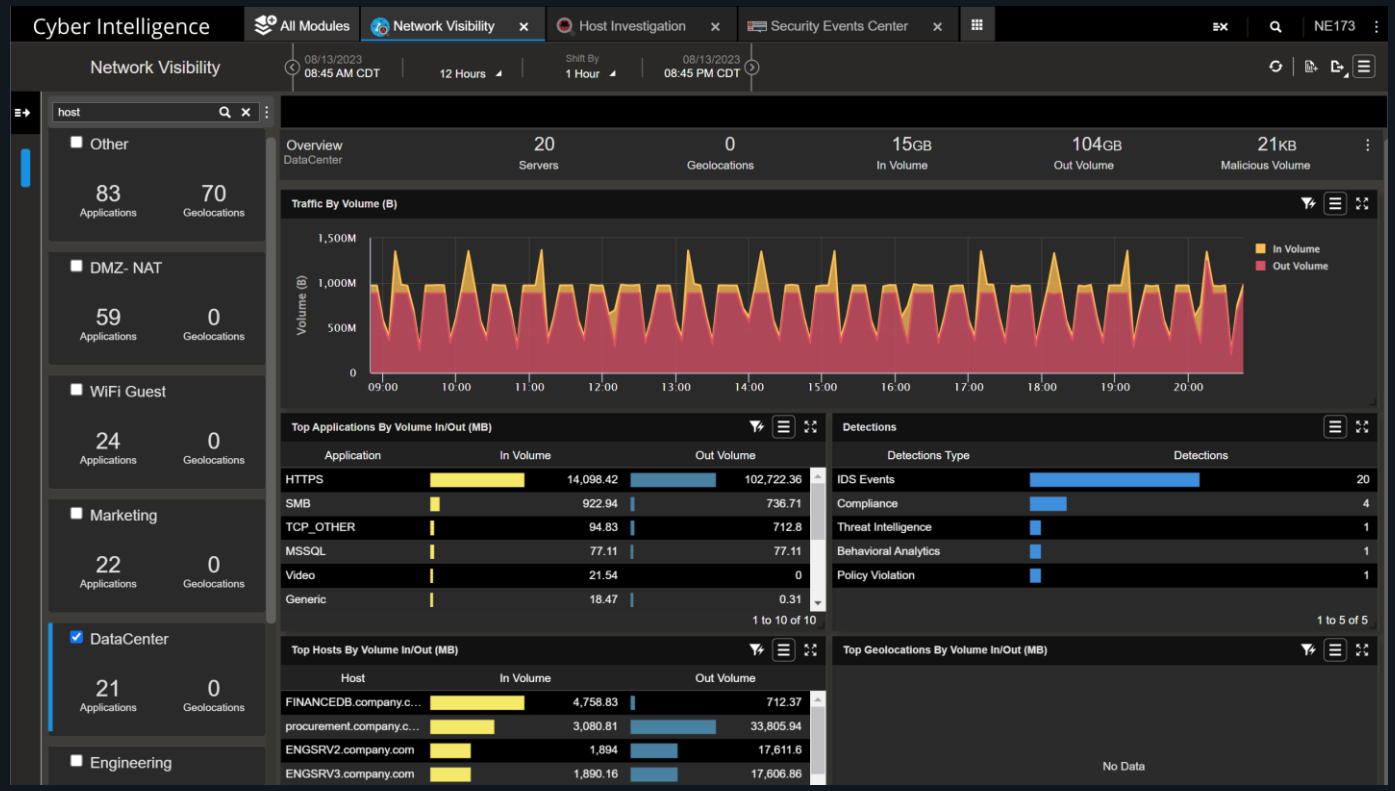
Detecting Initial Phase of an Attack

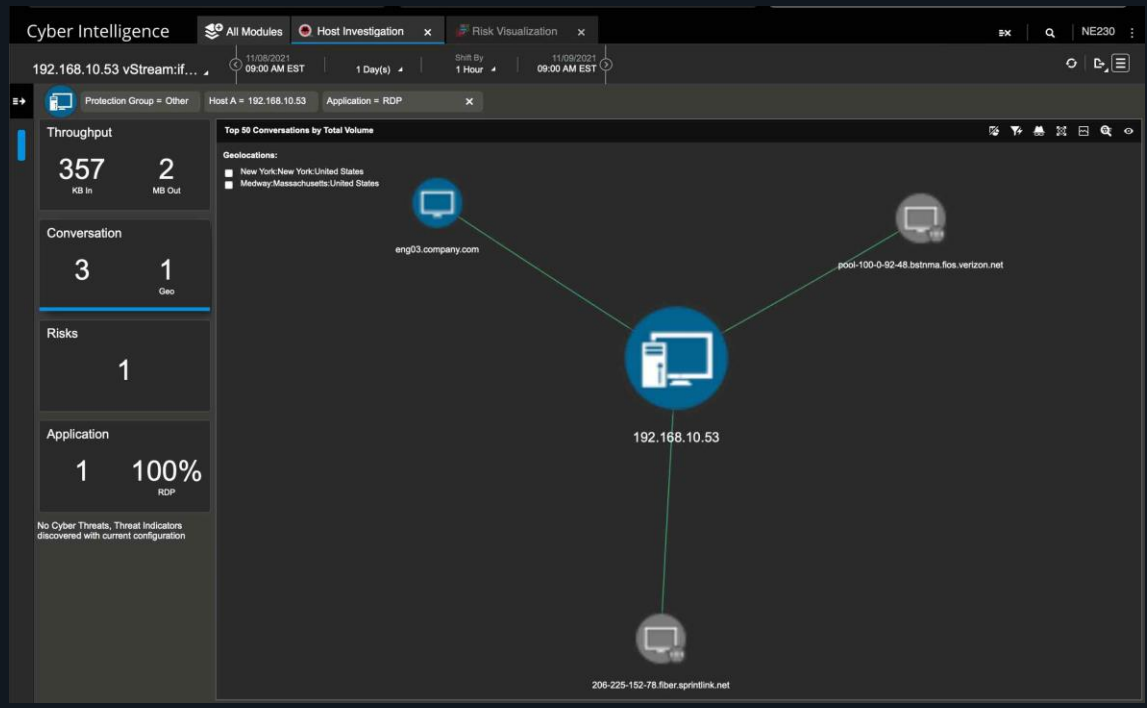


A NDR solution needs to detect more than 50% of previously unknown outbound threats and 95% of otherwise undetected reconnaissance:

- Define Protection Groups to highlight activity in high-risk areas
- Detect scanning and brute force access attempts
- Alert on activity associated with known vulnerabilities

Attack Surface Discovery





A NDR needs the ability to identify vulnerabilities in the infrastructure:

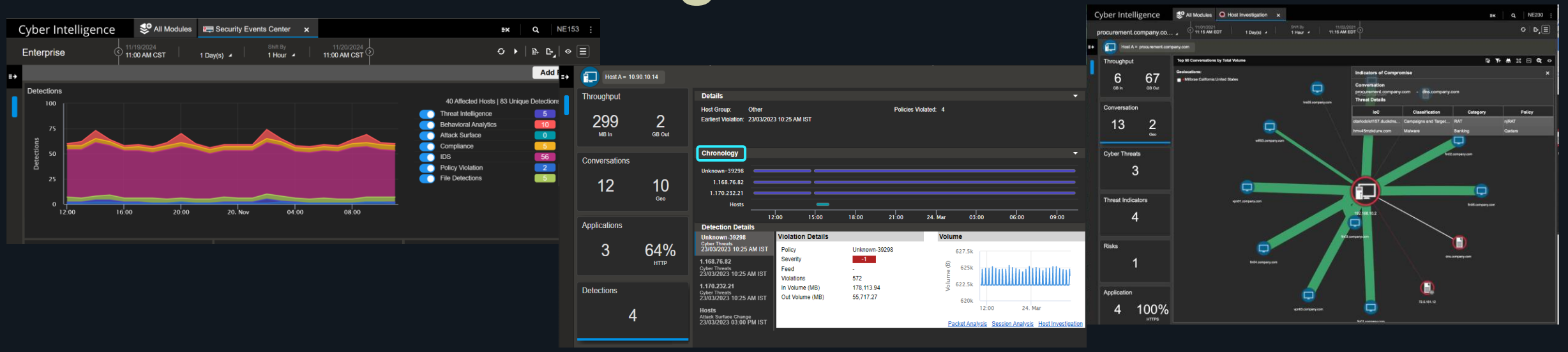
- Discovery of unauthorized servers, firewall rules and access; use of vulnerable protocols
- Detect successful reconnaissance attempts, e.g., TCP connections to open ports
- Identify breaches of security controls, e.g., use of external DNS services
- Poor SSL hygiene, e.g., weak cipher suites and certificates

Contact-Tracing For Incidents

A NDR needs to enables incidence response teams to reduce Mean Time To Knowledge to minutes:

- Collect evidence
- Identify the entry points and attack vectors used by the threat actor
- Determine if lateral movement or data exfiltration occurred
- Focus resources on incident boundary by establishing the extent of a breach or anomaly

Back In Time Investigation



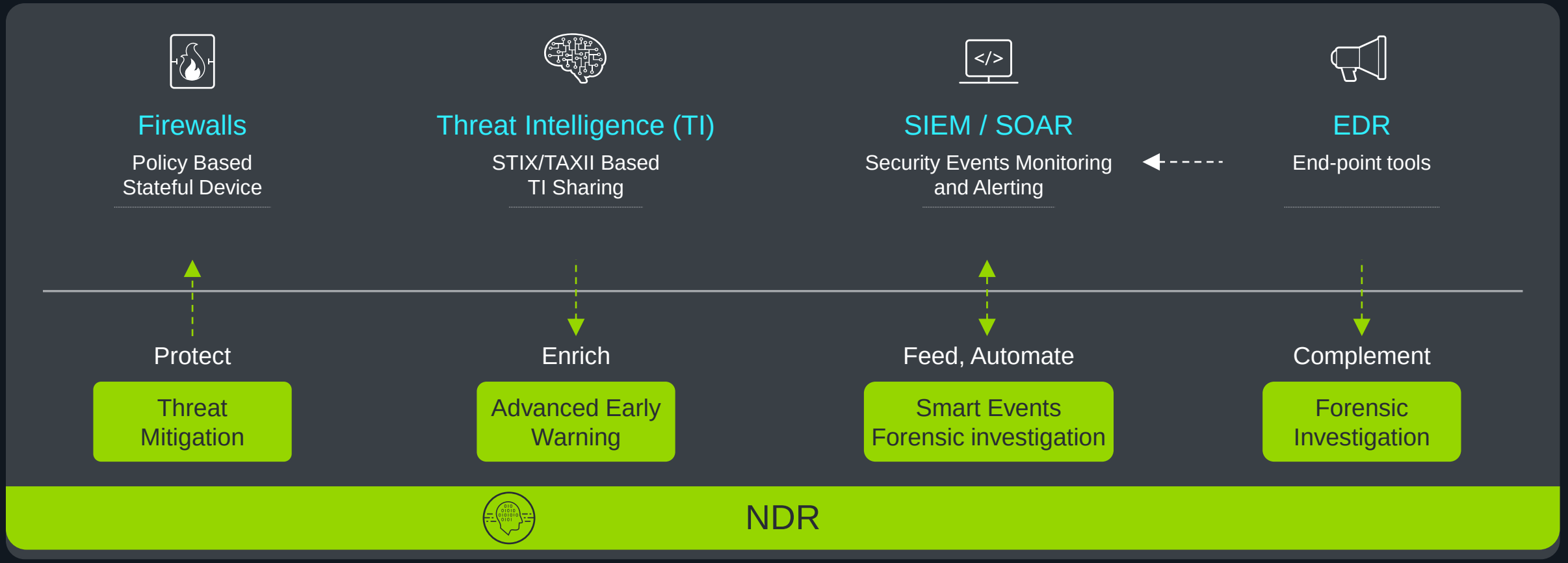
51	1:58:45.798.297.834 PM EDT	0.000.015.395	54	FINANCEDB.company.com	eng02.company.com	TCP: S=51670 D=43479 LEN=0 SEQ=171501477 ACK=34662	ACK
52	1:58:45.798.461.881 PM EDT	0.000.164.047	95	FINANCEDB.company.com	eng02.company.com	FTP: Response 200 Active data connection established.	ACK/PSH
53	1:58:45.798.463.075 PM EDT	0.000.001.194	95	FINANCEDB.company.com	eng02.company.com	TCP: S=21 D=60570 LEN=41 SEQ=3696153880 ACK=394866	ACK/PSH
54	1:58:45.799.123.236 PM EDT	0.000.660.161	79	eng02.company.com	FINANCEDB.company.com	FTP: Request RETR finance_export.csv	ACK/PSH
55	1:58:45.799.963.454 PM EDT	0.000.840.218	108	FINANCEDB.company.com	eng02.company.com	FTP: Response 125 Data connection already open. Transfer sta	ACK/PSH

Mean Time To Knowledge needs to be reduced from weeks or months to minutes:

- Quickly browse backwards through massive amounts of network traffic
- View breaches and anomalies as they happened
- Avoid re-creating problems or waiting for repeat incidents to troubleshoot them
- Apply newly available IoCs *IP addresses* retrospectively

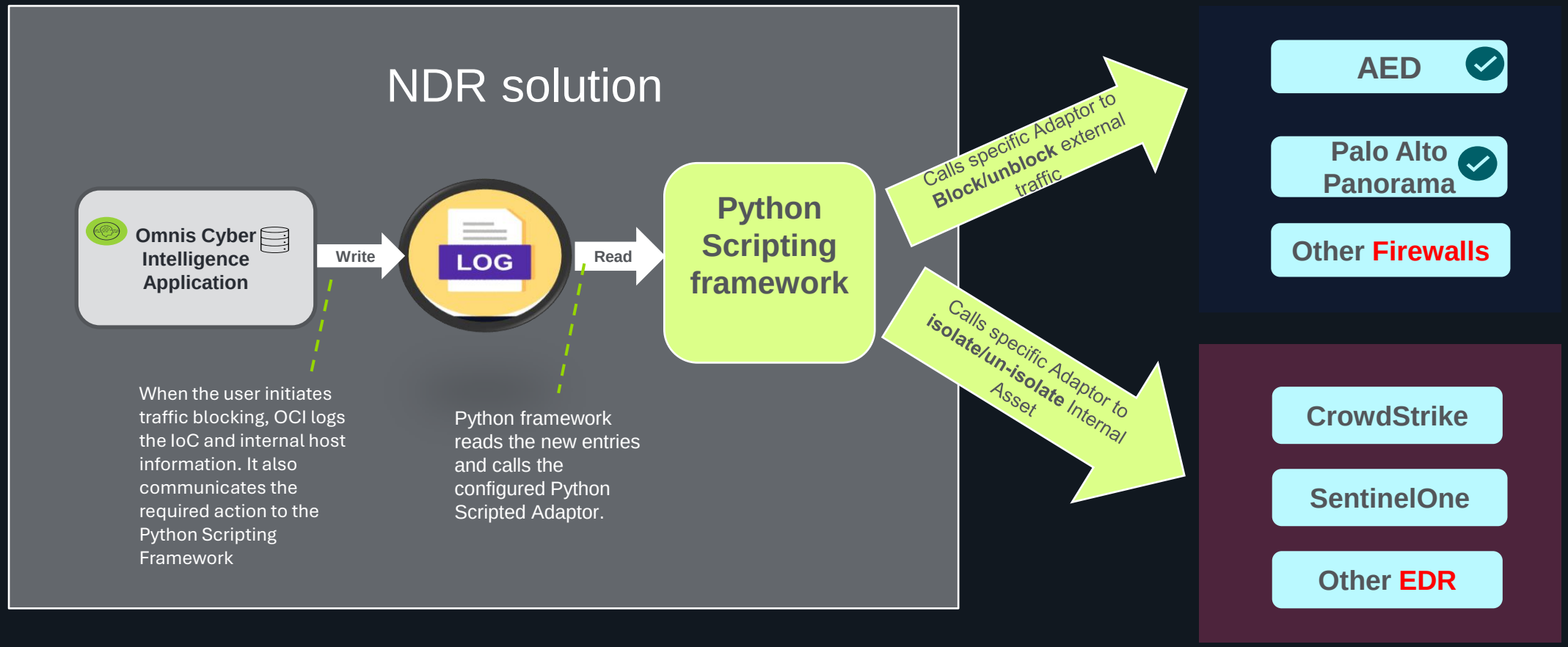
NDR in the Security Ecosystem

Fully Integrated with Security Stack to Maximize ROI



Open Architecture for 3rd Party Integration

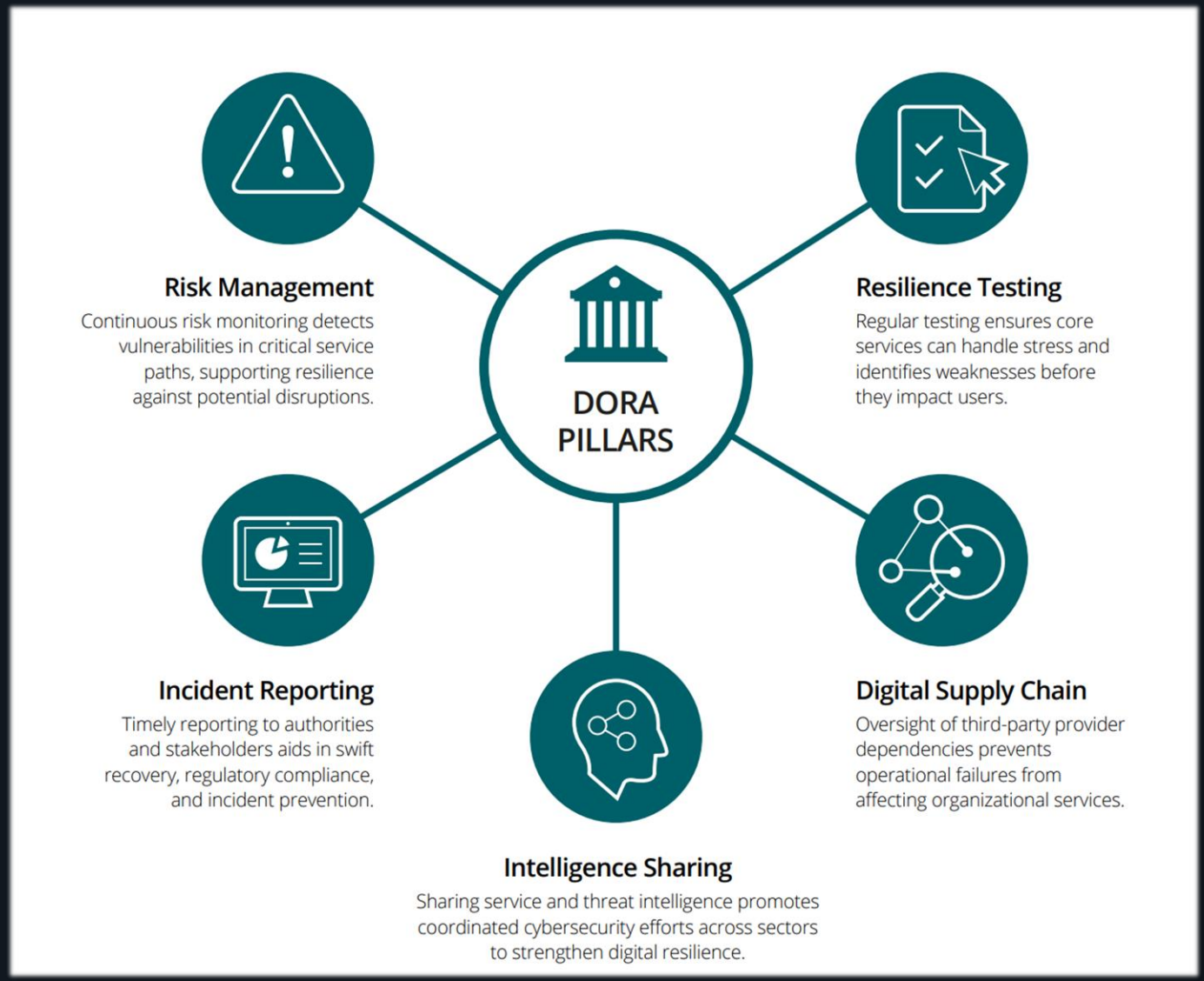
An Open Integration Architecture to integrate with any Firewall (block Traffic) or EDR (quarantine Assets), by calling their exposed API interface.



SIEM integration

Continuous risk monitoring for Compliance and Performance Standards

DORA – NIS-2



NETSCOUT®

Guardians of the Connected World