VECTRA®

Is next-generation IPS masking an old problem?

Intrusion detection systems (IDS) like Cisco Firepower (formerly Sourcefire), Trend Micro Deep Discovery, and McAfee Network Threat Behavior Analysis are all traditional technologies with deep roots in signature-based detection and protection.

These solutions are not true competitors of the Cognito® network detection and response platform from Vectra®, but have recently began marketing themselves as such. Here's why these IPS technologies fall short compared to Cognito.

No behavior detection

Signature-based detections and simple heuristics only detect specific, known attack patterns. Most attacks today – even the opportunistic ones – are at least minimally modified to suit the attacker's needs to be as effective as possible. This is something that we have noted in our Spotlight Report on Ransomware.

Gone are the old days of spray and pray. Attackers have turned to targeted attacks for increased probability of payout. Relying on IDS to defend your network is like running a free trial version of Kaspersky antivirus from the early 2000s, and then being surprised when you get infected in 2019.

Designed for legacy security models

As more organizations move towards a zero-trust model, antiquated systems that focus on guarding the outer on-premises perimeter have become obsolete. This limits the traffic IDS sees to only what passes through the firewall.

Consequently, if attackers compromise the internal network, they are free to move laterally without IDS being any wiser. In fact, the only noticeable difference IDS will show is the significant performance dip of firewalls now having to run heuristics on packets that pass through them.

Furthermore, today's enterprises may generate as much traffic in the cloud as within the on-premises network. As IDS focuses on traffic entering the network, attackers entering through a compromised cloud service account go completely unnoticed.

The Cognito platform can be deployed across all parts of the network, including multicloud environments, to give security analysts a complete view of all company assets, regardless of where they reside.

In addition, the Cognito platform strengthens zero-trust initiatives with Privileged Access Analytics (PAA). PAA allows you to infer account usage on your network and detects internal threat actors who use compromised credentials to further an attack.

Prepare for an onslaught of anomaly alerts

As an anomaly-based detection system, IDS can't identify the highest-risk threats and will overwhelm your security team with a deluge of alerts. These alerts must be manually and individually triaged, increasing your security operations workload. Already-overtasked security teams do not want shoulder this additional burden.

On the other hand, when pitted against humans rather than simulated attacks, Cognito algorithmic models outshine simple signature or heuristics-based detections. In fact, the Cognito platform supports over 85% of the MITRE ATT&CK framework. Its superior detection capabilities quickly become apparent during the proof-of-concept.

In addition, Cognito reduces security operations workload by 34X. It automatically triages alerts into incidents, prioritizes host devices that pose the highest risk, and extracts security-enriched metadata from all network traffic for investigations and forensics.

Single-vendor lock-in is anti-best-of-breed

IDS is typically positioned as part of a broader platform, making it incomplete by itself. It requires further investments in firewalls, URL filtering, application visibility tools, advanced attack detection, and the like. And to get an integrated experience, you must purchase everything from the same vendor.

The Cognito platform, on the other hand, easily integrates with your existing enterprise security stack via APIs. Our ecosystem of technology partners includes the industry leaders in endpoint detection and response, next-generation firewalls, SIEMs, security orchestration, and network access control. Cognito integrations support best-in-class security strategies and drive continued value by protecting existing investments.

The future of IDS

The Cognito platform from Vectra gives you a multitude of advantages over next-generation IDS:

- Detects modern, real-world attacks based on supervised and unsupervised machine learning algorithms.
- Provides complete visibility across your network from enterprise to cloud – not just the data that flows through a firewall.
- Reduces your security operations workload by 34X. Cognito triages attacker detections into prioritized incidents for the fastest, conclusive response.
- True platform performance integrates with other solutions in your security stack.

VECTRA®
Security that thinks®

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