VECTRA SECURITY THAT THINKS® | PROFITAP

SOLUTION BRIEF

Complete network visibility for real-time detection and response

Intelligent, AI-Driven Threat Detection and Response

The Cognito Network Detection and Response platform uses AI-derived machine learning algorithms to enrich and analyze metadata from network traffic, relevant logs and cloud events. This way, the Cognito NDR pplatform automatically detects, prioritizes and responds to in-progress attack behaviors that pose the highest business risk – inside cloud, data center, IoT, and enterprise networks.

By automating manual and mundane Tier-1 and Tier-2 security tasks, the Cognito NDR platform significantly reduces the workload in security operations centers, giving analysts more time to investigate incidents and hunt for threats. With detailed context about each attack, security teams are empowered to perform more conclusive incident investigations and faster assisted threat hunting. The information you need to stop an attack is always at your fingertips.

Along with technological evolution comes the sophistication of cybercrime, which continuously develops new attacks types, tools and techniques, allowing attackers to mitigate more complex network infrastructure whilst remain untraceable. Therefore, incident detection and response must be a top priority.

CHALLENGE

A threat that goes unseen will go undefeated. Network visibility is crucial to protecting organizations from cyber-attacks. Without full traffic visibility, the security teams are limited in their ability to see the entire attack lifecycle, which in turns limits the understanding and context of what is really happening.

Balancing the need for visibility, detection and response with the cost and complexity of security stack is never easy. As organizations struggling to find solution in preventing cyber-attacks, Profitap and Vectra provide ways to overcome them.

Profitap and Vectra have joined forces to provide enterprises with a comprehensive network visibility for real-time detection and analysis of active cyber attacks.

BENEFITS

Profitap's network visibility solutions combined with the Vectra Cognito NDR platform offers effective way to quickly identify cyber attacks in high availability network, including:

1. Reliable, complete access and visibility across the network.
2. Use real-time traffic capture and customizable filters to forward the most relevant data in real-time while maintaining link layer visibility at times.
3. Detect known and unknown threats in real-time anywhere in the network, including remote locations, network segments and cloud environments.
4. Expose encrypted and hidden attack communications without decrypting traffic.

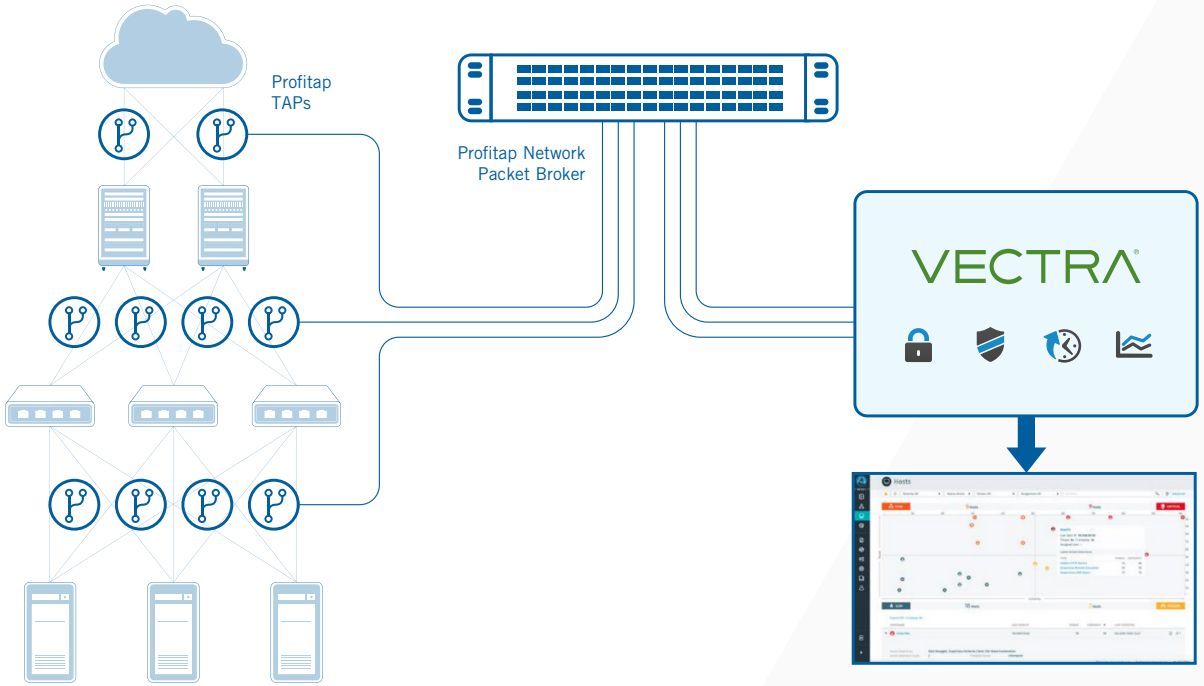
Profitap's network visibility solutions complement Vectra's high-end technology by providing all the data that it needs to make a complete and accurate analysis. Using this data, network engineers can monitor what is happening over the network in real-time, choose what data will be analyzed thus they can better prevent and uncover potential threats crossing the network.

Complete Access and Visibility to the Network

To get full access to what is going on the network lines, a TAP is required. Profitap's innovative Network TAPs offer a reliable access to the right data and insights into the network without introducing points of failure. In addition to providing line rate traffic capture, Profitap's Network TAPs also provide fail-safe access to the network. This ensures uninterrupted network operation in all cases also when the power is lost.

With Profitap's X2-Series Network Packet Brokers, traffic is then filtered and aggregated from all the network access points before being forwarded to Cognito platform for real-time threat analysis. The X2-Series Network Packet Brokers provide intelligent filtering as well as packet deduplication on physical and virtual networks, passing actionable flow data while maintaining the bandwidth usage.

The combined techniques and integration of Vectra and Profitap provide robust security at scale. Data privacy is assured because the Cognito NDR platform only analyzes metadata from packets – not the payload.



About Vectra

Vectra® is a leader in network detection and response – from cloud and data center apps and workloads to user and IoT devices and accounts. Its Cognito® platform accelerates threat detection and investigation using AI to enrich network metadata and cloud logs it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers four applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store and investigate threats in enriched metadata. And Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed. Cognito Detect for Office365 and Azure AD™ finds and stops attacks in enterprise SaaS applications and the Microsoft 365 Ecosystem.

About Profitap

Profitap develops and manufactures a complete range of innovative Network TAPs, Network Packet Brokers and Field Service Troubleshooters for security, forensics, deep packet capture and network performance monitoring sectors. All their network monitoring tools are highly performant and user-friendly, providing complete visibility and access to your network, 24/7. With a non-intrusive and fail-safe design, Profitap network analysis and traffic acquisition solutions send all the data to your security appliances so that your team can easily prevent and analyze cyberthreats.

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai