VECTRA SECURITY THAT THINKS® | FORTINET®

SOLUTION BRIEF

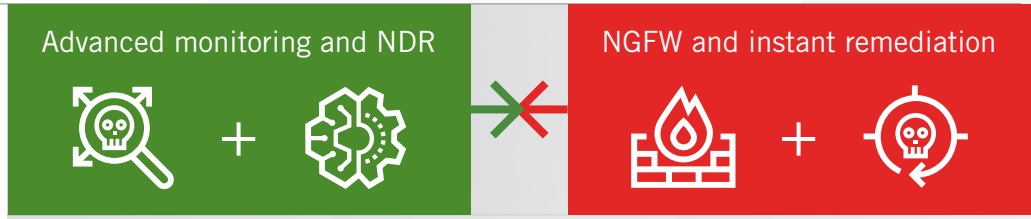
Vectra and Fortinet: Advanced monitoring and NDR with automated response

Advanced threats, security teams need accurate and continuous monitoring for threat activity across all environments, and automated response that quickly stops attackers before they succeed.

With the adoption of zero trust and a security perimeter that has dissipated in cloud services, a modern cybersecurity approach is required for immediate detection and response to threats in cloud, data center, IoT, and enterprise infrastructures.

Together, Vectra® and Fortinet deliver greater infrastructure visibility by combining AI-driven NDR – including privilege and identity aware analytics – with next-generation firewall capabilities and instant remediation.

Vectra and Fortinet enable security teams to quickly expose hidden threat behaviors, pinpoint the specific hosts and accounts at the center of a cyberattack, and block the threat before data is damaged or stolen.



HIGHLIGHTS

- Automatically detect and respond to hidden attacks in cloud, data center, IoT and enterprise networks using behavior-based machine learning detection algorithms.
- Increase efficiency by feeding triaged Cognito platform detections with security-enriched insights to FortiSIEM for faster, more conclusive investigations and threat hunting.
- Strengthen zero-trust network access by monitoring identity and privileged access transactions to detect privilege abuse and account compromise.
- Leverage the award-winning Cognito NDR platform and FortiGate NGFWs to detect, respond and block cyberattacks in cloud, data center, IoT, and enterprise networks.
- Increase SOC team productivity via FortiSOAR security orchestration, automated playbooks and incident triaging.

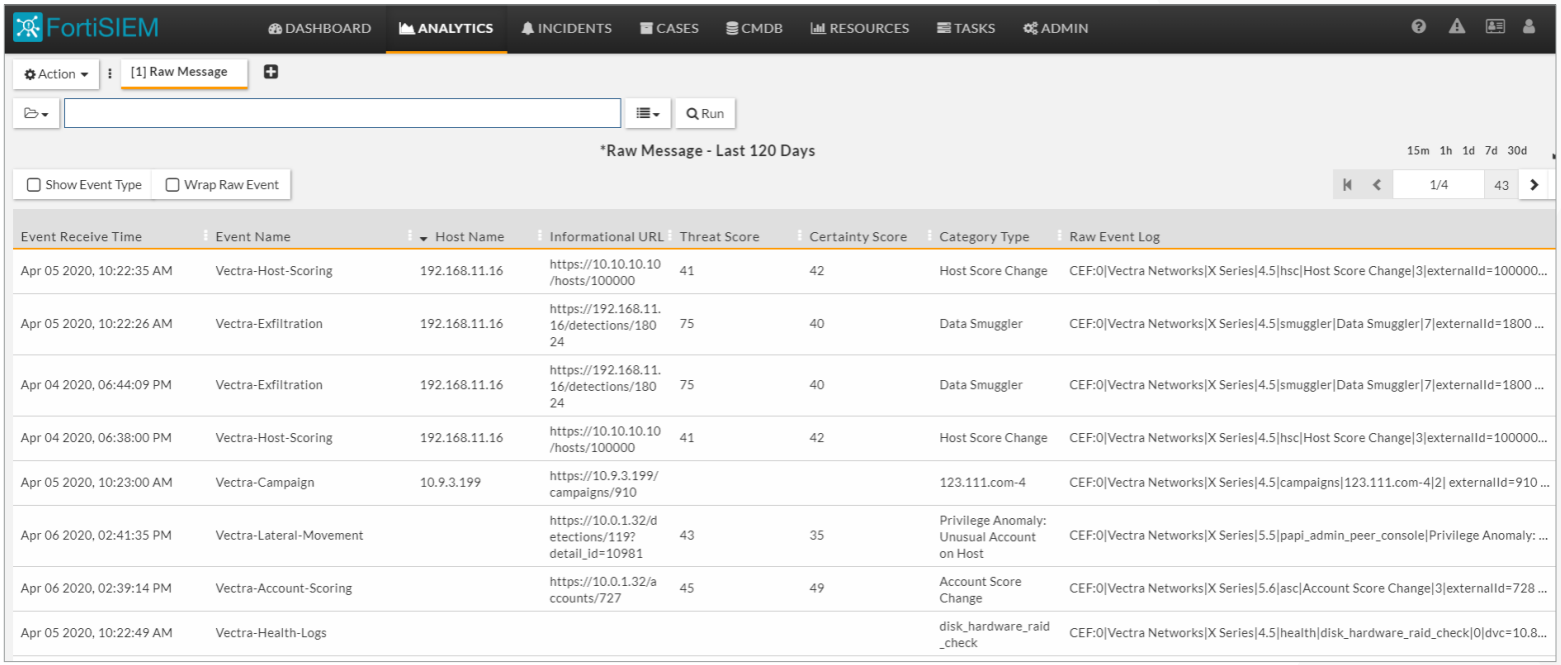
Unrivaled NDR

The Cognito® NDR platform from Vectra uses AI-derived machine learning algorithms to automatically detect, prioritize and respond to in-progress attack behaviors that pose the highest risk – across cloud, data center, IoT, and enterprise networks.

By automating manual and mundane Tier-1 and Tier-2 security tasks, the Cognito NDR platform reduces the workload of security analyst, giving them more time to focus on incident investigations and threat hunting.

With Vectra, the power is in the data. The Cognito NDR platform captures metadata at scale from all network traffic and enriches it with security context and deep insights about every attack. This enables security teams to investigate and hunt faster, more conclusively.

The Vectra NDR platform is in 100% service of detecting and responding to attacks inside cloud, data center, IoT, and enterprise. Our job is to find those attacks early and with certainty.



Event Receive Time	Event Name	Host Name	Informational URL	Threat Score	Certainty Score	Category Type	Raw Event Log
Apr 05 2020, 10:22:35 AM	Vectra-Host-Scoring	192.168.11.16	https://10.10.10.10/hosts/100000	41	42	Host Score Change	CEF:0|Vectra Networks|X Series|4.5|hsc|Host Score Change|3|externalId=100000...
Apr 05 2020, 10:22:26 AM	Vectra-Exfiltration	192.168.11.16	https://192.168.11.16/detections/18024	75	40	Data Smuggler	CEF:0|Vectra Networks|X Series|4.5|smuggler|Data Smuggler|7|externalId=1800 ...
Apr 04 2020, 06:44:09 PM	Vectra-Exfiltration	192.168.11.16	https://192.168.11.16/detections/18024	75	40	Data Smuggler	CEF:0|Vectra Networks|X Series|4.5|smuggler|Data Smuggler|7|externalId=1800 ...
Apr 04 2020, 06:38:00 PM	Vectra-Host-Scoring	192.168.11.16	https://10.10.10.10/hosts/100000	41	42	Host Score Change	CEF:0|Vectra Networks|X Series|4.5|hsc|Host Score Change|3|externalId=100000...
Apr 05 2020, 10:23:00 AM	Vectra-Campaign	10.9.3.199	https://10.9.3.199/campaigns/910			123.111.com-4	CEF:0|Vectra Networks|X Series|4.5|campaigns|123.111.com-4|2| externalId=910 ...
Apr 06 2020, 02:41:35 PM	Vectra-Lateral-Movement		https://10.0.1.32/detections/119?detail_id=10981	43	35	Privilege Anomaly: Unusual Account on Host	CEF:0|Vectra Networks|X Series|5.5|papi_admin_peer_console|Privilege Anomaly: ...
Apr 06 2020, 02:39:14 PM	Vectra-Account-Scoring		https://10.0.1.32/accounts/727	45	49	Account Score Change	CEF:0|Vectra Networks|X Series|5.6|asc|Account Score Change|3|externalId=728 ...
Apr 05 2020, 10:22:49 AM	Vectra-Health-Logs					disk_hardware_raid_check	CEF:0|Vectra Networks|X Series|4.5|health|disk_hardware_raid_check|0|dvc=10.8...

Cognito threat detections seen through the FortiSIEM dashboard.

Better together

To accelerate response time, the Cognito NDR platform integrates and shares the same context and insights with third-party security solutions – including FortiSIEM, FortiSOAR, and FortiGate next-generation firewalls (NGFWs) – for end-to-end threat management.

FortiSIEM allows analysts to hunt for signs of an attack, using security insights and context from the Cognito NDR platform. And FortiSOAR integrates with the Cognito to provide automated playbooks, incident triaging and real-time threat remediation.

When Vectra detects attacker behaviors, it automatically notifies Fortinet FortiGate next-generation firewall to block the source and destination devices. This stops attacks and enables security analysts to conduct faster investigations.

Fortified security from Fortinet

FortiGate NGFWs from Fortinet enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection.

Powered by AI-driven FortiGuard Labs, FortiGate NGFWs deliver proactive threat protection with high-performance inspection of both clear-text and encrypted traffic to stay ahead of the rapidly expanding threat landscape. Unified data and analytics are collected from diverse sources, including logs, performance metrics, security alerts, and configuration changes.

The unique architecture of the Fortinet Security Fabric unifies these security technologies across the digital network, including multicloud, endpoints, email and web applications, and network access points, into a single security system integrated through a combination of open standards and a common operating system.

These Fortinet security technologies are then enhanced through the integration of advanced NDR technologies – such as the Cognito NDR platform from Vectra – and a unified correlation, management, orchestration, and analysis system.

About Vectra

Vectra® protects businesses by identifying and stopping cyberattackers before they spread throughout the IT infrastructure – across, cloud, data center, IoT, and enterprise networks. As a leader in network detection and response (NDR), Vectra AI is the premier choice among cybersecurity professionals around the world to automate attacker discovery, prioritize threats and respond with unparalleled speed. Vectra is equally adept at protecting IaaS, PaaS and SaaS deployments, resulting in true enterprise-scale threat coverage. For more information, visit vectra.ai.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks number one in the most security appliances shipped worldwide and more than 450,000 customers trust Fortinet to protect their businesses. Learn more at fortinet.com.

For more information please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai