SOLUTION BRIEF

Fortinet and Vectra Security Solution

Advanced Monitoring and Threat Detection with Automated Response

Executive Summary

The Vectra and Fortinet security solution delivers complete network visibility, machine-learning (ML) behavioral threat detection, and privilege and identity aware analytics with next-generation firewall (NGFW) capabilities and instant remediation. Organizations can reduce the complexity of managing network and security operations by leveraging FortiSIEM. In addition, FortiSOAR integration provides security orchestration capabilities with automated playbooks and incident triaging, and real-time remediation for organizations to identify, defend, and counter attacks.

The Challenge

With increasingly sophisticated 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 perimeter that has moved to cloud services, a modern security solution needs to monitor privilege and identity to track attacks.

Joint Solution

The Vectra and Fortinet security solution delivers complete network visibility, ML behavioral threat detection, and privilege and identity aware analytics with NGFW capabilities and instant remediation.

The Vectra and Fortinet security solution enables security staff to quickly expose hidden attacker behaviors, pinpoint the specific hosts and accounts at the center of a cyberattack, and block the threat before data is lost. In addition, FortiSIEM allows analysts to hunt for signs of an attack, with the deep context of all relevant data sources. Further, FortiSOAR integrates with Vectra and provides automated playbooks and incident triaging, and real-time remediation for organizations to identify, defend, and counter attacks.

When Vectra detects an attacker and the attacker's behavior progression, it automatically notifies Fortinet to block both source and destination devices via the Fortinet FortiGate NGFW, effectively stopping attacks so that analysts can rapidly investigate and resolve threats.

Joint Solution Benefits

- Automatically detect and stop advanced attackers that have circumvented preventative security solutions in cloud and data center using modern behavioral-based machine-learning detections
- Increase security operations efficiency by feeding triaged Vectra detections to FortiSIEM to allow faster forensic and threat hunting with the correct context and data needed
- Strengthen zero-trust network access by monitoring identity and privileged access transactions to detect privilege abuse and account compromise
- Leverage the award-winning FortiGate enterprise firewall platform to provide unparalleled security protection

Fortinet Fabric-Ready

Fortinet FortiGate NGFWs 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. Fortinet NGFWs meet the performance needs of highly scalable, hybrid IT architectures, enabling organizations to reduce complexity and manage security risks. FortiGate NGFWs are powered by artificial intelligence (AI)-driven FortiGuard Labs and deliver proactive threat protection with high-performance inspection of both clear-text and encrypted traffic to stay ahead of the rapidly expanding threat landscape.

As an integral part of the Fortinet Security Fabric, FortiGate NGFWs can communicate within the comprehensive Fortinet security portfolio as well as third-party security solutions in a multivendor environment. Through awareness of applications, users, and content within network traffic, FortiGate NGFWs offer comprehensive protection against known and unknown threats, such as ransomware, malicious botnets, zero day, and encrypted malware.

The Fortinet security information and event management system, FortiSIEM, reduces the complexity of managing network and security operations to effectively free resources, improve breach detection, and even prevent breaches. Fortinet architecture enables unified data collection and analytics from diverse information sources including logs, performance metrics, security alerts, and configuration changes. FortiSIEM essentially combines the analytics traditionally monitored in separate silos of the security operations center (SOC) and network operations center (NOC) for a more holistic view of the security and availability of the business.

Fortinet FortiSOAR is a holistic security orchestration, automation, and response (SOAR) workbench, designed for SOC teams to efficiently respond to the ever-increasing influx of alerts, repetitive manual processes, and shortage of resources. This patented and customizable security operations platform provides automated playbooks and incident triaging, and real-time remediation for enterprises to identify, defend, and counter attacks.

FortiSOAR third-party connectors and integrations provide access to hundreds of products including desktop security software, directories, network infrastructure, and other third-party security systems maximizing your ROI and providing unparalleled visibility and control across your network through SOAR. FortiSOAR seamlessly integrates with other vendors and technologies, including Vectra, for threat intelligence.

Vectra Technology and Product

The Vectra Cognito® network threat detection and response platform provides the fastest, most efficient way to find and stop attackers that have hidden in your cloud or data center network. Cognito delivers real-time attack visibility and puts attack details at your fingertips to empower immediate action.

Leveraging artificial intelligence, Cognito performs non-stop, automated threat hunting with always-learning behavioral models to quickly and efficiently find hidden and unknown attackers before they do damage.

Cognito also delivers blind-spot-free threat detection coverage by directly analyzing all interactions to gain high-fidelity visibility into the actions of all identities and devices—from cloud and data center workloads to user and IoT devices—leaving attackers with nowhere to hide.

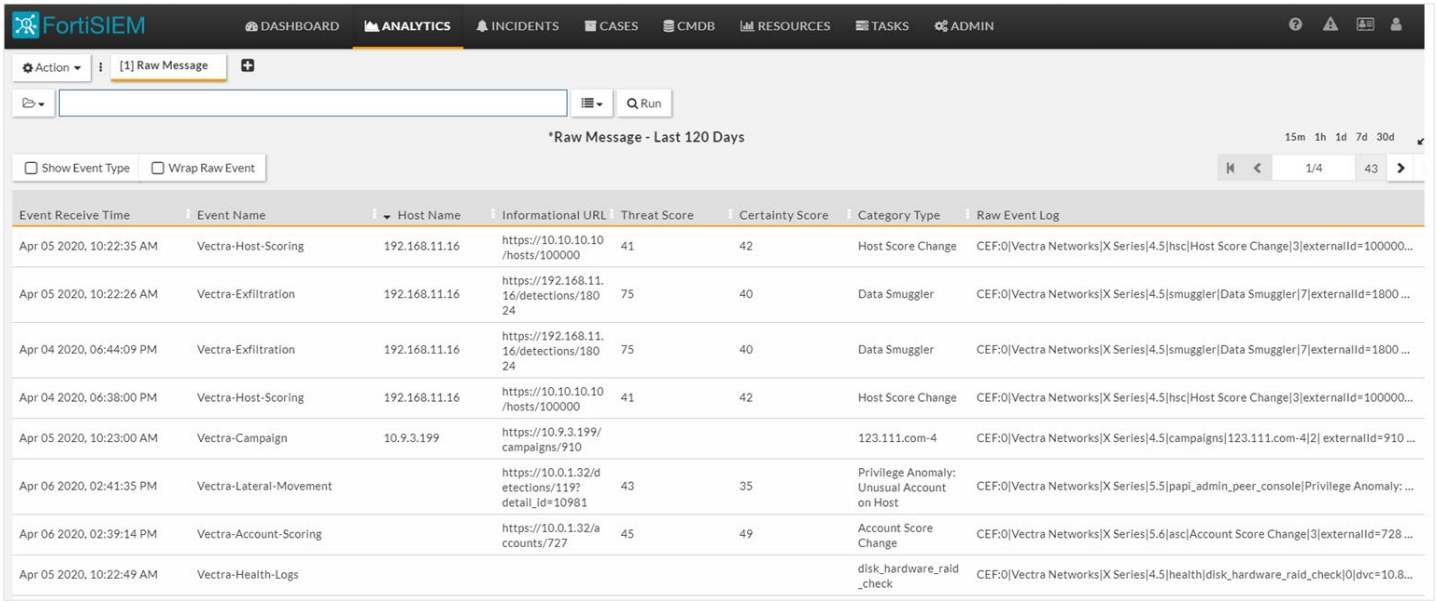

Figure 1: Events from Vectra in FortiSIEM.

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 http://www.fortinet.com.

About Vectra

Vectra® is the leader in network detection and response—from cloud and data center workloads to user and IoT devices. Its Cognito® platform accelerates threat detection and investigation using artificial intelligence to enrich network metadata it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers three 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. For more information, visit vectra.ai.

August 1, 2020 5:12 AM

741713-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\Vectra\sb-FA-fortinet-and-vectra-security-solution-812020\sb-FA-fortinet-and-vectra-security-solution-812020