SOLUTION BRIEF

Fortinet and DefendEdge Security Solution

Broad, Integrated, and Automated Solution for Artificial Intelligence-based Insider Threat Detection and Response

Executive Summary

Fortinet and DefendEdge have partnered to deliver an industry-leading solution by integrating the Fortinet Security Fabric and SiON to provide enterprises proactive rule-based and machine learning in employee anomaly threat detection and response.

Challenges

The attack surface is continuing to expand, and while many security teams are focused primarily on preventing malicious outsiders from exploiting new attack venues, the Verizon 2018 Data Breach Investigations Report found that close to 30 percent of confirmed breaches today involve insiders. However, today's increasingly complex networks, compounded by the proliferation of data, devices, applications, and users accessing networked resources, make it difficult for security teams to detect and prevent insider threats, regardless of whether those breaches are malicious or the result of negligence.

As advanced threats rapidly evolve, CISOs need to implement security controls that protect their company's data, intellectual property, and reputation both inside and out. And they need to do this while simultaneously satisfying industry compliance requirements.

Joint Solution

DefendEdge and Fortinet have established a technology partnership to arm organizations with actionable analytics on employee activities and help make decisions on real-time threats. SiON's proprietary machine-learning platform eliminates false positives in threat hunting and allows cybersecurity teams to focus on confirmed threat indicators.

Solution Components

DefendEdge SiON

DefendEdge's SiON solution is an enterprise platform that integrates and analyzes multiple enterprise data sources and provides the ability to execute workflows defined by the organization based on end-user behavior.

FortiGate Next-Generation Firewall

FortiGate next-generation firewalls (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.

FortiClient Enterprise Management Server

As an integrated agent, FortiClient shares endpoint telemetry with the Security Fabric and delivers broad endpoint visibility, compliance control, and vulnerability management. It provides advanced endpoint protection with pattern-based anti-malware, behavior-based

Solution Components

- Fortinet Security Fabric—Fortinet FortiGate Next-Generation Firewall, FortiClient Enterprise Management Server, FortiSandbox
- DefendEdge SiON

Joint Solution Benefits

- Monitor, identify, and respond to user activity
- Deploy rapid security controls to specific end-users
- Correlate FortiGate to DefendEdge's SiON Employee Threat Profile
- Eliminate false-positive detection rates across all end-user, network-based activity
- Full onboarding, job transfer, and termination access control

FORTINET Fabric-Ready

exploit protection, web filtering, and an application firewall. FortiClient natively integrates with FortiSandbox to detect zero-day threats and custom malware. FortiClient also provides secure remote access with built-in virtual private network (VPN), single sign-on, and two-factor authentication for added security.

FortiSandbox

Top-rated artificial intelligence (AI)-powered FortiSandbox is part of the Fortinet breach protection solution that integrates with the Fortinet Security Fabric platform to address the rapidly evolving and more targeted threats including ransomware, cryptomalware, and others across a broad digital attack surface. Specifically, it delivers real-time actionable intelligence through the automation of zero-day, advanced malware detection and response.

DefendEdge's SiON platform pulls log data from the Fortinet Security Fabric into the platform and leverages enterprise-level authoritative upstream systems and applications and user identity to correlate and analyze data, identify anomalous end-user behavior, and execute automated procedures. Based on the client's end-state architecture, the platform can be hosted on-premises or in the cloud. Integration to target systems is seamless and done through an application programming interface (API), flat files, or other connection-oriented methods. SiON offers several role-based access profiles for executives, directors, and security analysts with multiple report options for auditors and compliance officers.

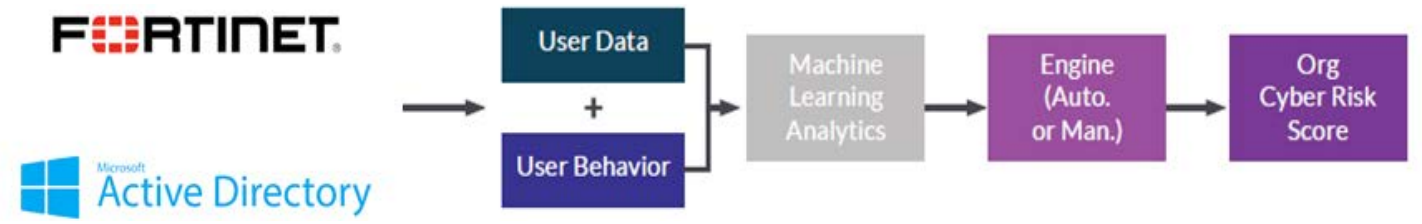

Figure 1: Fortinet Security Fabric and DefendEdge SiON.

Use Cases

Use Case #1

SiON helps solve data exfiltration when an employee has privileged access to sensitive information and attempts to download the data to a thumb drive. SiON alerts the organization that data is being exfiltrated and isolates all end-user activity through the FortiGate and FortiEMS.

Use Case #2

SiON and FortiGate integration helps provide the ability to monitor end-user behavior and login times, geolocations, and data sessions. SiON can take action to terminate anomalous behavior and initiate a password revocation for a suspected compromised user's Active Directory LDAP account.

About DefendEdge

DefendEdge, a Cyber Security company focused on building solutions that will protect your data, infrastructure, reputation, and customers against cybercrime. Our proprietary platform SiON is designed to be the most accurate and effective artificial intelligence platform in human behavior to help clients predict, detect, identify, and respond to human identity access threats in corporate networks.

July 7, 2020 5:22 AM

719134-0-0-EN

D:\Fortinet\Solution Briefs\Grey Solution Brief\DefendEdge\sb-fortinet-and-defendedge-security-solution-772020