Introduction

Cybersecurity threats are increasing in sophistication, automation, and diversity. Organizations are seeking an edge in protecting infrastructure, applications and services which are critical priorities for IT organizations today. Addressing these sophisticated threats requires mechanisms and systems to predict, prevent, detect and respond to them in realtime. Embracing an adaptive approach to network security is key, along with automation to enable rapid exchange of threat information between systems, to prevent infections from spreading and compromising key assets.

Fortinet and Attivo Networks have partnered to deliver a security solution with the edge that executives and operations need to address these risks. Attivo Networks’ ThreatMatrix Deception and Response Platform integration with Fortinet’s FortiGate® firewall platform enables customers to benefit from Attivo’s award-winning deception-based threat management capabilities, while simultaneously leveraging the best-validated security protection in the industry provided by Fortinet.

How Does it Work?

The Attivo Networks ThreatMatrix Deception and Response Platform changes the balance of power with sophisticated deception technology that deceives an attacker into revealing themselves. The platform accelerates breach discovery and provides an elegant mechanism to trap the BOTs and APTs that bypass perimeter and endpoint security. Detailed attack analysis and forensics accelerate incident response and provide protection against future cyberattacks.

As illustrated in Figure 1, the ThreatMatrix platform adds deception decoys that appear as production assets, thereby obfuscating the attack surface and turning the entire network into a trap. Deception decoys can be added in the data center, cloud, IoT and SCADA networks. This process is friction-less and easily scales, since it is based on connecting to the trunk port of a switch and then uses unused IP addresses for the decoys. The solution is not reliant on signatures or database lookup, making it extremely efficient for catching all types of threat vectors of both known and unknown attackers.

When the attacker seeks out its target, the attacker is deceived into engaging with a deception server. Once engaged, high-fidelity alerts are raised and automated response actions occur. The combination of early detection, attack analysis and automated response actions provide a highly efficient platform for continuous threat management.

The ThreatMatrix integrates with the Fortinet FortiGate firewall platform by leveraging the Fortinet Security Fabric APIs. Once the ThreatMatrix platform identifies an infected network node, it communicates with the firewall to provide the IP address information via the API for policy enforcement, effectively preventing exfiltration of valuable data.

Key Benefits

- The Attivo ThreatMatrix Platform includes deception decoys and servers that obfuscate the attack surface turning the entire network into a trap
- Upon engagement, the attackers are lured away from production assets and into engaging with the BOTsink server that generates detailed attack forensic reports and alerts FortiGate firewalls
- The FortiGate firewalls automatically block communications from the infected systems
- FortiSandbox, another key component of the Fortinet Security Fabric, adds inspection and advanced ATP capabilities to the solution
Solution Benefits

- **Real-time threat detection.** Deception-based detection authentically matches production assets to deceive attackers into revealing themselves.

- **Detailed attack analysis and actionable forensics.** Collect Tactics, Techniques, and Practices (TTP) of BOTs, APTs, and insider threat actors based on malware attack and phishing email analysis.

- **Accelerate incident response with automated attack blocking.**

- **Enhance prevention** - Attack analysis is shared through API integration to improve incident response by automatically blocking and quarantining attackers.

- **Unparalleled Security Protection** - Leverage the industry’s best validated security protection offered by Fortinet’s FortiGate network security platform to protect against sophisticated cyberthreats.

- **Leverage Global Threat Intelligence** by using Fortinet’s FortiGuard Security Subscription Services to enable visibility and control for next generation protection against advanced threats, including zero day attacks.

About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo Deception Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

Learn more at [www.attivonetworks.com](http://www.attivonetworks.com)