Security Without Compromise With Integrated Deception-Based Threat Management

Highlights

- Real-time threat detection
- Detailed attack analysis and actionable forensics
- Automated Blocking
- Accelerated incident response
- Unparalleled security protection

Joint Solution Brief

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 real-time. 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.

Joint Solution

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

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 efficient mechanism for detecting advanced threats that have evaded perimeter and endpoint security. Detailed attack analysis and forensics accelerate incident response and provide protection against future cyberattacks.

ThreatMatrix and Fortigate Integration

Figure 1 illustrates how 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 within user networks, data centers, cloud, IoT, SCADA and POS networks. The process is friction-less to deploy and easily scalable with no dependence on known attack patterns or signatures, making it extremely efficient for detecting malware and advanced threats catching all types of threat vectors of both known and unknown attackers.

When the attacker seeks out its target, he 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.

About Attivo Networks®

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

www.attivonetworks.com

About Fortinet

Fortinet (NASDAQ: FTNT) protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company's fast, secure and global cyber security solutions provide broad, high-performance protection against security threats while simplifying the IT infrastructure.

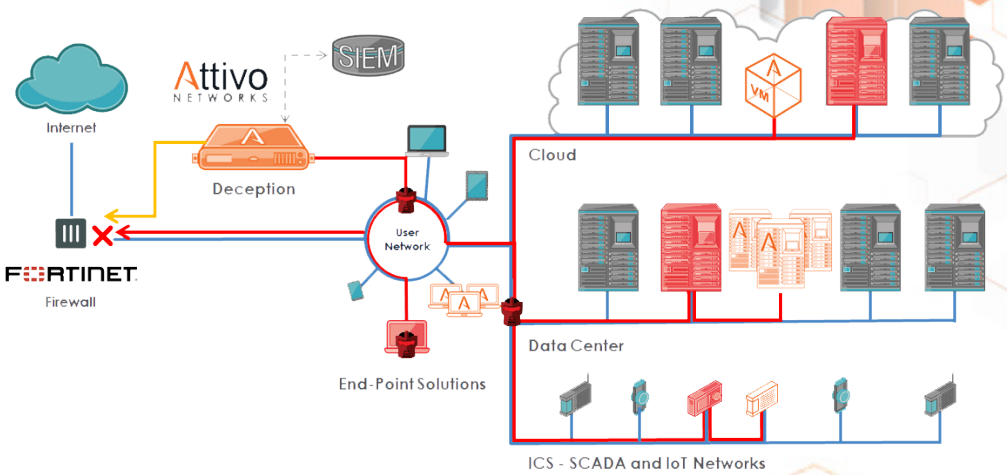
www.fortinet.com

Attivo NETWORKS

FORTINET

Joint Solution Brief

Figure 1: Fortinet and Attivo Networks integrated security solution



Solution Benefits

- Real-time deception-based threat detection. Authentically matches production assets to deceive attackers into revealing themselves.
- Enhanced prevention. Attack analysis is shared through API integration to improve incident response by automatically blocking and quarantining attackers.
- 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.
- Accelerated incident response with automated attack blocking.
- Unparalleled security protection with integration to the Fortinet FortiGate network security platform.
- Leverage global threat intelligence by using the Fortinet FortiGuard Security Subscription Services to enable visibility and control for next generation protection against advanced threats, including zero day attacks.

Summary

The integration of prevention and detection solutions empowers organizations with early detection and analysis of inside-the-network threats, arming them with critical and detailed forensic information required for blocking the attacker and preventing exfiltration of valuable data.

It provides security with a time and staff resource advantage and helps them rise above the noise of potential false-positive alerts, prompting accelerated incident response from partner programs to block and quarantine the infected endpoints and servers before mass damage occurs.

Today's security posture requires organizations to take an assumed breach stance and the joint solution empowers organizations to quickly detect and respond to even the most advanced threat actor.