PARTNER BRIEF

ATTIVO NETWORKS AND FORTINET - SECURITY WITHOUT COMPROMISE WITH INTEGRATED THREAT MANAGEMENT

Cybersecurity threats are increasing in sophistication and diversity. Organizations seek 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 essential, along with automating the rapid exchange of threat information between systems, to prevent infections from spreading and compromising critical assets.

HIGHLIGHTS

- Real-time Threat Detection
- Detailed Attack Analysis and Actionable Forensics
- Automated Blocking
- Accelerated Incident Response
- Unparalleled Security Protection

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 ThreatDefend® platform integration with the Fortinet FortiGate® firewall platform enables customers to benefit from Attivo's award-winning threat detection capabilities, while simultaneously leveraging security protection provided by Fortinet.

The Attivo Networks ThreatDefend platform changes the balance of power with sophisticated deception and concealment technologies that tricks attackers 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 protect against future attacks.

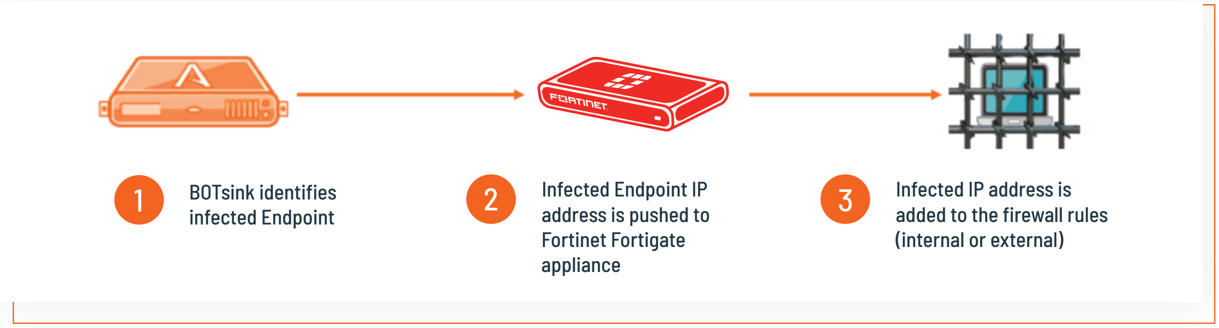
ATTIVO THREATDEFEND PLATFORM AND FORTIGATE INTEGRATION

Figure 1 illustrates how the ThreatDefend platform creates a detection fabric of network, endpoint, and Active Directory deceptions with decoys that mimic production assets and data, thereby obscuring the attack surface and turning the entire network into a trap. Decoys can deploy within user networks, data centers, or specialty networks such as IoT, SCADA, and POS. The frictionless deployment easily scales to on-premises, cloud, and remote work sites. Detections do not depend on known attack patterns or signatures, making it extremely efficient for detecting advanced threats, ransomware, and other threat vectors of both known and unknown attackers.

As attackers evade detection and compromise internal systems, they must conduct discovery, lateral movement, and privilege escalation activities. Any touch with a decoy asset creates high-fidelity alerts and triggers automated response actions. The combination of early detection, attack analysis, and automated response actions provide a highly efficient platform for continuous threat management.

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

Figure 1: Fortinet and Attivo Networks integrated security solution



1 BOTsink identifies infected Endpoint

2 Infected Endpoint IP address is pushed to Fortinet Fortigate appliance

3 Infected IP address is added to the firewall rules (internal or external)

SOLUTION BENEFITS

- Real-time, early, in-network threat detection. Authentically matches production assets to deceive attackers into revealing themselves.
- Enhanced prevention. Shared attack analysis through API integration improves incident response by automatically blocking and quarantining attackers.
- Detailed attack analysis and actionable forensics. Collect Tactics, Techniques, and Practices (TTP) of in-network attackers, APTs, and insider threat actors from captured attack activity.
- Accelerate 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 in-network threats, arming them with critical and detailed forensic information required for blocking the attacker and preventing exfiltration of valuable data.

It provides security teams 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 occur.

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.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership.

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