SOLUTION BRIEF

Fortinet and Attivo Integrated Security Solution

Security Without Compromise With Integrated Deception-based Threat Management

Introduction

Cybersecurity threats are increasing in sophistication, automation, and diversity. Organizations are seeking an edge in protecting infrastructure, applications, and services that 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.

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 the Fortinet 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 advanced persistent threats (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, Internet of Things (IoT), and supervisory control and data acquisition (SCADA) networks. This process is frictionless 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.

Joint Solution Components

- Fortinet FortiGate, FortiSandbox
- Attivo Networks ThreatMatrix Deception and Response Platform

Joint Solution 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

FORTINET FABRIC-READY

The ThreatMatrix integrates with the Fortinet FortiGate firewall platform by leveraging the Fortinet Security Fabric application programming interfaces (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.

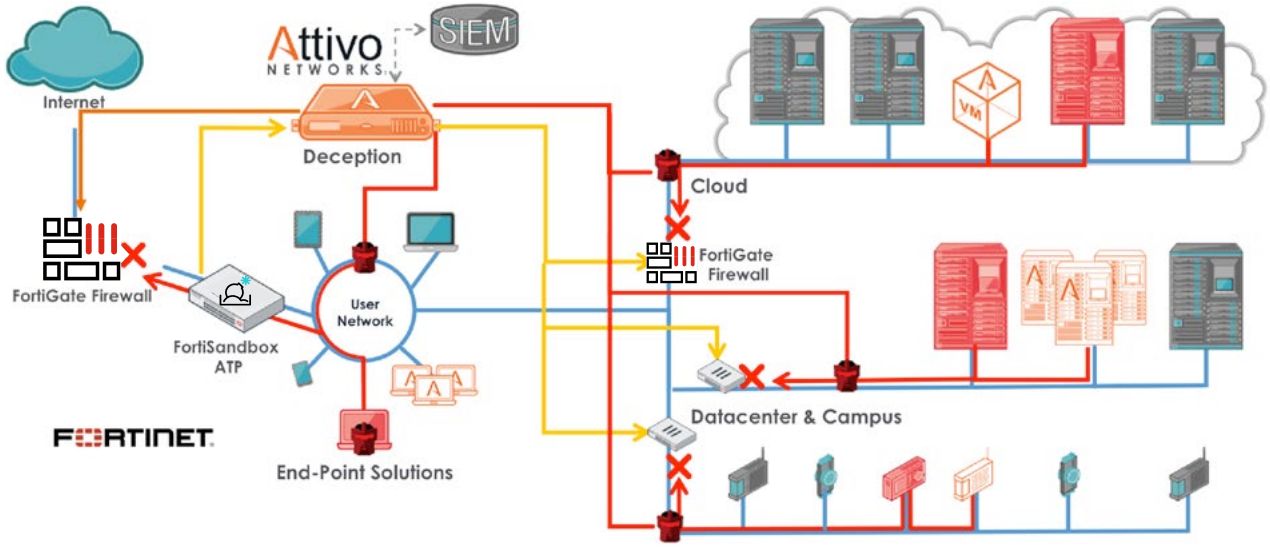

Figure 1: Fortinet and Attivo Networks Integrated Security Solution

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 procedures (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 the Fortinet FortiGate network security platform to protect against sophisticated cyber threats.
- **Leverage global threat intelligence** by using Fortinet 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.

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

August 16, 2021 10:43 AM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working:Attivo:sb-Fortinet-Attivo-Networks

429113-B-0-EN