Attivo Networks ThreatDefend™ Deception Platform Integrates with the Check Point Management Server

Attivo Networks® has partnered with Check Point® Software Technologies to deliver a simplified solution for the real-time detection, analysis, and automated blocking of cyber attacks. With this joint solution, customers can use the Attivo ThreatDefend™ Deception and Response Platform to detect infected systems inside the network and configure the Deception Platform to either automatically or manually push the infected IP addresses and the attack signatures to the Check Point R80 for prompt blocking to prevent exfiltration of data. Customers will reduce the risk of breaches or data loss by reducing the time-to-detection and the resources needed to identify, block, and remediate threats inside the network.

Highlights

- Real-time Threat Detection
- Attack forensics and threat analysis
- Faster incident response
- Automatic or manual blocking

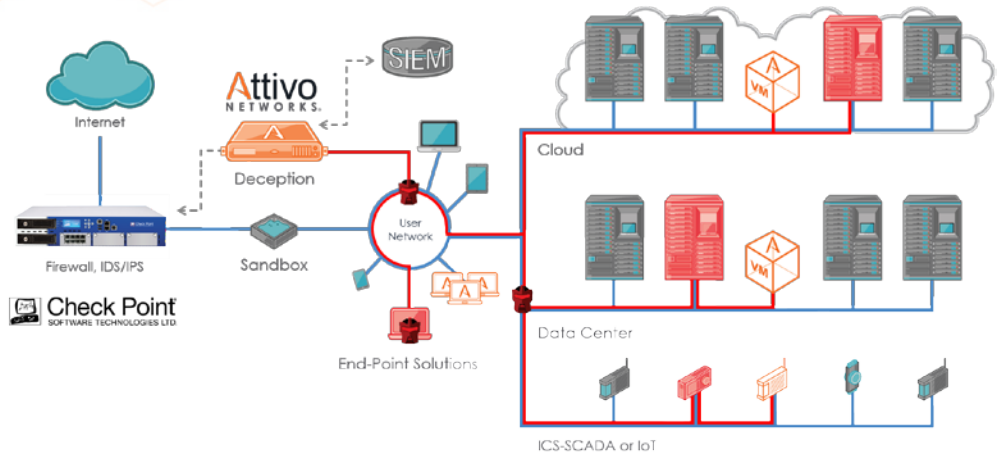
The Challenge

To keep an environment secure from threats, organizations use a wide variety of technologies to protect their critical assets. While the network may seem airtight, gaps in security have consistently led to breaches in companies of every size across many different industries. In addition to the security weaknesses, many security devices do not communicate with each other – meaning alerts raised by one device may not be passed to others in time to stop the same threat at a different point in the network.

The lack of communication leads to networks susceptible to cyber attacks.

Changing the Game

DAs cyber attacks continue to increase in complexity and effectiveness, a modern combination of prevention and detection techniques is needed to effectively protect critical assets in the network. Additionally, as the prevention and detection tools gain more information on attacks and how to prevent them, a common thread of communication needs to exist between them to decrease the time to detect, block, and remediate an attack. The continuous communication will improve the performance of prevention systems as well as incident response, ultimately saving time, money, and limiting risk.



Attivo NETWORKS®

Check Point SOFTWARE TECHNOLOGIES LTD.

Joint Solution Brief

About Attivo Networks

Attivo Networks® provides real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend Deception and Response 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. www.attivonetworks.com

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd., is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. www.checkpoint.com

Attivo NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD.

Joint Solution Brief

The Joint Solution

Integration between the Attivo ThreatDefend Deception and Response Platform and the Check Point R80 is simple to set up and can be completed in minutes.

The process begins with the ThreatDefend Platform identifying a threat that has bypassed traditional prevention systems and has started to infect machines on the network. Once the threat is engaged with the deception platform, the attack can be played out and analyzed in a quarantined environment. Detailed attack forensics including signatures and attack patterns can be relayed to the Check Point R80 which is then able to reinforce the firewall capabilities and automate blocking to prevent exfiltration of data.

The Attivo Networks ThreatDefend Deception and Response Platform

The deception platform, comprised of BOTsink Engagement Servers, ThreatStrike End-point Deception Suite, and ThreatDefend analysis engine is designed to detect inside-thenetwork threats from all threat vectors including targeted, stolen credentials, ransomware, phishing, and insider attacks. Attacks can be detected within user networks, data centers, clouds, IoT, and ICS-SCADA environments. Using deception, the solution lures and misdirects attackers trying to reach or compromise valuable company assets.

Attacks can be detected at any point of infection, from initial reconnaissance to lateral movement within the network, as attackers attempt to escalate privileges and find targeted assets. Once the attacker is engaged, the platform collects and correlates the full Techniques Tactics and Procedures (TTP) with associated forensics and reports via IOC, STIX, CSV, and PCAP file formats. This information can be manually or automatically shared with security prevention systems empowering organizations with notice and attack information required to deflect and stop the attack.

Summary

Fast detection and informed incident response are critical to avoiding a full network breach.

By adding the Attivo ThreatDefend Deception and Response Platform to an organization's security suite, time to detection is improved, detailed attack forensics gathered, and substantiated alerts raised, ultimately improving a company's ability to defend against advanced cyber attackers. Paired with the Check Point R80, customers are able to fortify their incident response capabilities with automatic or manual blocking, detailed information for remediation, and future prevention.