

## ATTIVO NETWORKS THREATDEFEND™ PLATFORM INTEGRATION WITH CHECK POINT MANAGEMENT SERVERS

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 Check Point Security Gateways 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 ATTIVO THREATDEFEND PLATFORM AND CHECK POINT JOINT SOLUTION

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

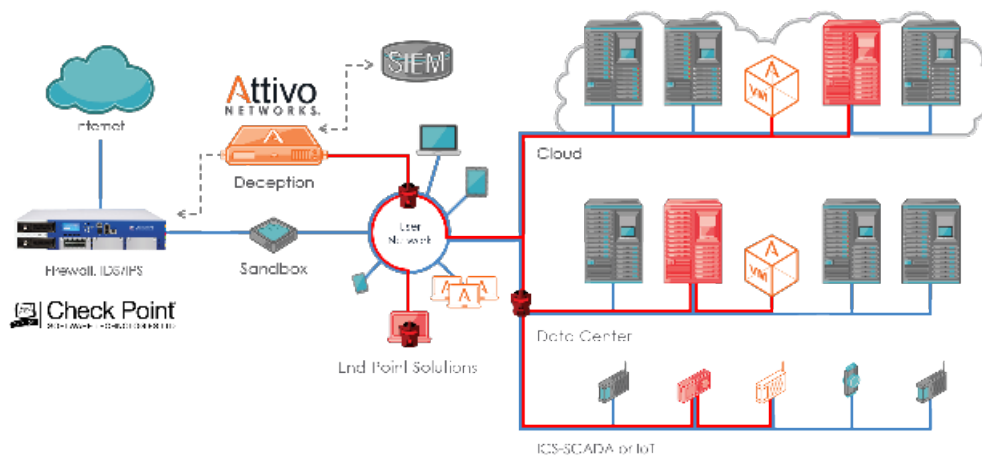
### THE CHALLENGE

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 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.

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 Check Point which is then able to reinforce the firewall capabilities and automate blocking to prevent exfiltration of data.

# ATTIVO NETWORKS THREATDEFEND PLATFORM

Recognized as the industry's most comprehensive deception platform, the solution provides network, endpoint, and data deceptions and is highly effective in detecting threats from all vectors such as reconnaissance, stolen credential, Man-in-the-Middle, Active Directory, ransomware, and insider threats. The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink® engagement servers, decoys, and deceptions, the ThreatStrike™ endpoint deception suite, ThreatPath™ for attack path visibility, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM) which together create a comprehensive early detection and active defense against cyber threats.



## SUMMARY

Fast detection and informed incident response are critical to avoiding a full network breach. Organizations adding the Attivo ThreatDefend Platform to their security suite improve mean-time-to-detect and mean-time-to-respond, with unparalleled visibility to inside-the-network threats. By combining the ThreatDefend platform with Check Point security solutions, organizations can accelerate their incident response and strengthen their overall security posture.

## 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](http://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](http://www.checkpoint.com)