



```
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True
```

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 real-time detection, analysis, and automated blocking of cyberattacks. With this joint solution, customers can use the Attivo ThreatDefend® platform to detect infected systems inside the network and configure either automatically or manually push the infected IP addresses and the attack signatures to Check Point Security Gateways for immediate blocking to prevent data exfiltration. Customers can lower the risk of breaches or data loss by reducing the time to detect attacks 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 platform and Check Point is simple and takes minutes to set up.

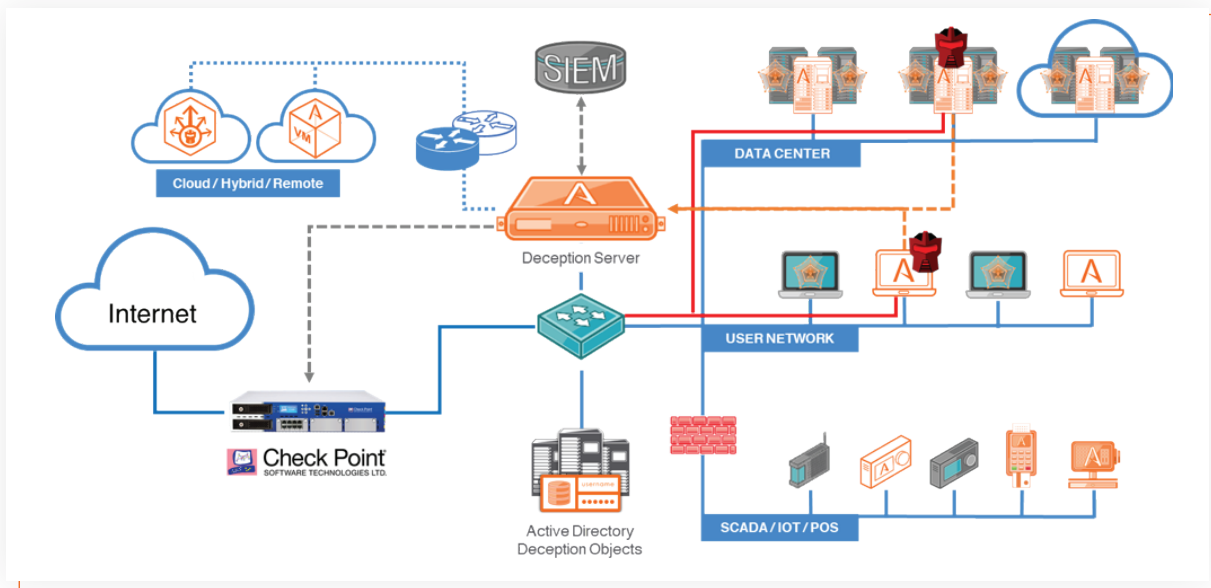
The ThreatDefend platform detects a threat that has evaded traditional prevention systems and has infected systems on the network. As the attacker attempts to conduct discovery, lateral movement, credential theft, and privilege escalation activities, the platform denies access to sensitive data and privileged accounts while redirecting the attack to the decoy environment for engagement. The platform captures forensics of all attack activities to gather adversary intelligence, capture Indicators of Compromise (IoCs), and provide full Tactics, Techniques, and Procedures (TTP) for faster remediation. The platform sends the attacking IP address Check Point Security Gateway, which then automatically blocks it at the edge to prevent Command and Control (C2) communication and data exfiltration.

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, advanced attackers evading security have led to breaches in companies of every size across many different industries. Additionally, many security devices do not communicate with each other – meaning alerts raised by one security control may not pass to others in time to stop the same threat at a different point in the network. The lack of communication allows attackers time to infiltrate further into the environment and cause more significant damage.

ATTIVO NETWORKS THREATDEFEND PLATFORM

The Attivo Networks ThreatDefend® Platform provides early and accurate detection of in-network threats, regardless of attack method or surface, using deception and concealment technologies. It provides a comprehensive fabric that blankets the network with deceptive decoys, credentials, shares, bait, and other misdirections that derail adversaries early in the attack lifecycle. Automated intelligence collection, attack analysis, and third-party integrations accelerate incident response. The platform's components include the BOTsink deception server, the Endpoint Detection Net Suite, and ADSecure for Active Directory protection.



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®, 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 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