

```
mirror_mod.use_x = False
mirror_mod.use_y = False
elif operation == "MIRROR 2":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
```

ATTIVO NETWORKS THREATDEFEND® PLATFORM INTEGRATION WITH JUNIPER NETWORKS SRX FIREWALLS

Attivo Networks has partnered with Juniper Networks 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 Juniper Networks SRX firewalls 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 JUNIPER NETWORKS JOINT SOLUTION

Integration between the Attivo ThreatDefend platform and Juniper Networks SRX Firewall is simple and takes minutes to set up.

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.

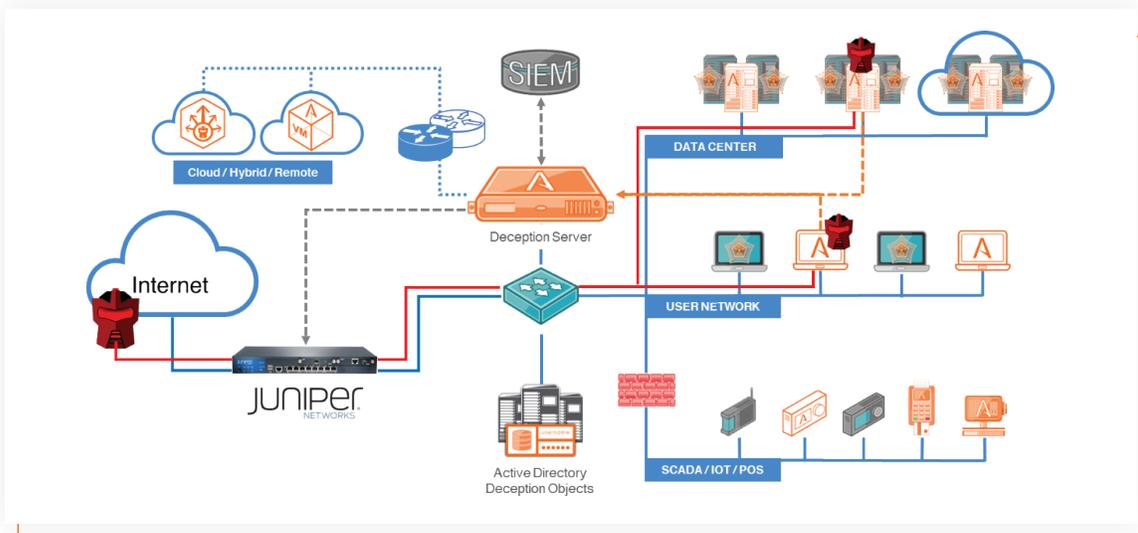
The ThreatDefend platform detects a threat that has evaded traditional prevention systems and has infected systems on the network. As the attacker attempts to conduct discovery, lateral movement, credential theft, and privilege escalation activities, the platform denies access to sensitive data and privileged 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 the Juniper Networks SRX Firewall, which then automatically blocks it at the edge to prevent Command and Control (C2) communication and data exfiltration.

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 Juniper Networks SRX firewalls, organizations can accelerate their incident response and strengthen their overall security posture.



ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in cyber deception and attack lateral movement detection, delivers a superior defense for revealing and preventing insider and external unauthorized threat activity. The Attivo ThreatDefend® Deception Platform provides scalable protection, detection, and data concealment solutions for endpoints, Active Directory, and network devices. Comprehensive coverage is available for user networks, data centers, clouds, remote worksites, and specialized attack surfaces. It streamlines incident with forensics, automates attack analysis, and includes third-party native integrations.

www.attivonetworks.com

ABOUT JUNIPER NETWORKS

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide.

www.juniper.net