

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

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH MICRO FOCUS ARCSIGHT® ESM

Attivo Networks® has partnered with Micro Focus to provide advanced, real-time, in-network threat detection and improved automated incident response. With the joint solution, customers receive improved threat intelligence with high fidelity alerts based on suspicious activity. Organizations can reduce time and resources required to detect threats, analyze attacks, isolate attackers, and to remediate infected endpoints, ultimately decreasing the organization's risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine and Blocking
- Expedited Incident Response
- End-point Deception Credentials

advanced attacks. However, even with this investment, less than half of the breaches are detected internally. Adding to the challenge, security analysts are bombarded with undifferentiated alerts, increasing the risk of missing real threats while chasing false positives.

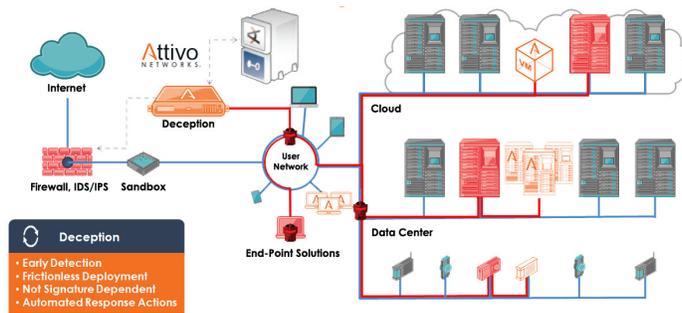
THE ATTIVO THREATDEFEND PLATFORM AND MICRO FOCUS ARCSIGHT JOINT SOLUTION

Attivo Networks® has integrated the ThreatDefend™ solution with the ArcSight Enterprise Security Manager to provide advanced adaptive security with real-time in-network threat detection, attack analysis, event correlation, and improved incident response for cyber-attacks. BOTsink, the core of the ThreatDefend platform, sends detailed events from the deception environment to the ESM where the high-fidelity alerts and detailed attack information augments the data available to incident responders from ArcSight. Additionally, BOTsink regularly queries ESM to identify any attempt to use its deceptive credentials anywhere in the production environment.

THE CHALLENGE

Cyberattackers have proven repeatedly that they can, and will, infiltrate the networks of even the most security-savvy organizations. Whether the attacker gets in using stolen credentials, a zero-day exploit, an email-based attack, or simply starts off with insider access, they will establish a foothold and move laterally through the network until they reach their intended target. Attackers have also proven that they can evade the remaining security solutions and traverse the network undetected once inside.

Organizations have responded to these threats by reinforcing their defenses, including an investment in SIEMs, to improve their security monitoring in the hopes of detecting



REAL-TIME IN-NETWORK VISIBILITY & THREAT DETECTION

ThreatDefend for Continuous Threat
Management

ATTIVO NETWORKS THREATDEFEND PLATFORM

Recognized as the industry's most comprehensive deception platform, the Attivo Networks solution provides network, endpoint, and data deception across an organization. The system has proven highly effective in detecting threats from all vectors, including reconnaissance, stolen credentials, Man-in-the-Middle attacks, Active Directory compromise, ransomware, and insider threats.

The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink engagement servers delivering decoys, lures, and breadcrumbs to an attacker, ThreatDirect® to extend deception into remote locations, the ThreatStrike® endpoint deception suite, ThreatPath® for attack path visibility, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM) to

coordinate the entire deception suite. Together, these components create a comprehensive early detection and active defense platform against advanced cyber threats.

SUMMARY

The Attivo Networks ThreatDefend Platform plays a critical role in enabling an active defense with in-network threat detection and native integrations to dramatically accelerate incident response. The combination of early detection, attack analysis, and comprehensive forensic information provides a highly efficient platform for detection of advanced threats and continuous threat management. The ArcSight ESM can leverage the Attivo Networks ThreatDefend Platform's detection, reporting, and integrations to monitor for threats, enabling faster incident investigations and adaptive responses, resulting in effective threat containment.

ABOUT ATTIVO NETWORKS®

Attivo Networks® provides the 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, ICS-SCADA, POS, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

ABOUT MICRO FOCUS

Micro Focus is one of the largest pure-play software companies in the world, focused from the ground up on building, selling, and supporting software. This focus allows Micro Focus to deliver on our mission to put customers at the center of innovation and deliver high-quality, enterprise-grade scalable software that Micro Focus's teams can be proud of. Micro Focus helps customers bridge the old and the new by maximizing the ROI on existing software investments and enabling innovation in the new hybrid model for enterprise IT.

www.microfocus.com