THREATDEFEND® PLATFORM FEATURE HIGHLIGHT: THREATDIRECT®

OVERVIEW

The Attivo Networks® ThreatDefend® platform includes the ThreatDirect® feature that provides organization with the ability to easily and efficiently project deception into remote locations and microsegmented networks, extending their coverage without needing to deploy additional BOTsink® deception servers. Deception projected with ThreatDirect appears in the "local" environment regardless of where it is relative to the organization's other assets.

This functionality is especially useful for organizations that have remote locations they want to cover with deception, such as branch offices, remote datacenters, or Cloud infrastructure.

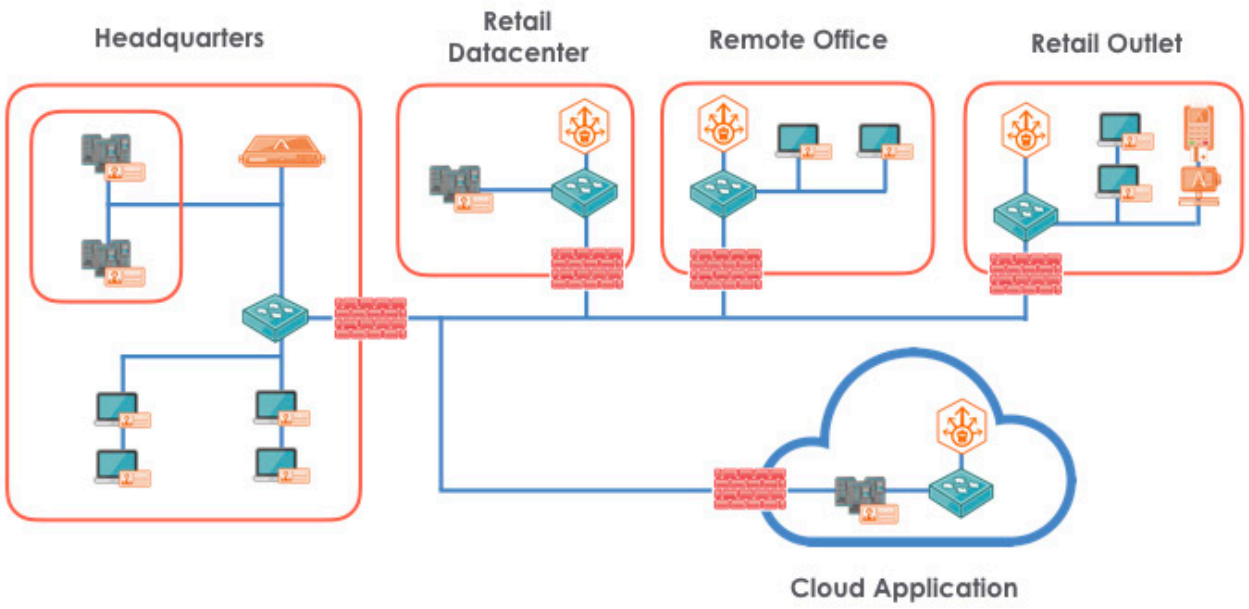
THREATDIRECT®

The Attivo Networks® ThreatDirect component is one part of the ThreatDefend® platform. The BOTsink® deception server sits at the heart of the solution, which can provide comprehensive deception across a large production environment. Organizations with remote offices, sales outlets, branch offices, clinics, remote datacenters, microsegmentation, or cloud instances can use the ThreatDirect component to extend the reach of their BOTsink server to locations that where it may be impractical or unfeasible to deploy a dedicated server.

The ThreatDirect component is a lightweight virtual machine, easily installed in remote locations, that can be managed remotely. It is fully configurable to extend authentic, comprehensive deception into the remote or microsegmented environment, efficiently and economically expanding the deception coverage.

PRACTICAL USE

The ThreatDirect component is specifically designed so organizations can efficiently and effectively project deception into remote locations. For example, a large retail organization has deployed a complete ThreatDefend® platform at their corporate headquarters, including a BOTsink server for network deception and the ThreatStrike® component for endpoint deception. The company has multiple retail locations with PoS terminals and a limited number of workstations and servers at each location. By deploying a ThreatDirect instance in each remote location, then can extend the full benefit of the ThreatDefend platform to their remote locations while requiring only minimal resources.



In another example, an organization has small a corporate office, remote datacenters, and application servers based in the Cloud. Here, they have deployed a BOTsink server in their corporate office and used ThreatDirect instances in their datacenters and cloud environment to extend deception coverage into the remote environments. This makes their information security team more effective and efficient without adding to their overhead.

AVAILABILITY

The ThreatDirect component is compatible with all versions of the Attivo Networks BOTsink server in any of its deployment formats: physical, virtual, or cloud. The ThreatDirect component runs as a virtual machine on multiple platforms, giving organizations a range of deployment options.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend™ Deception Platform provides a comprehensive and customer-proven platform for proactive security and accurate threat detection within user networks, data centers, clouds, and a wide variety of specialized attack surfaces. The portfolio includes expansive network, endpoint, application, and data deceptions designed to efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning makes preparation, deployment, and operations fast and simple to operate for organizations of all sizes. Comprehensive attack analysis and forensics provide actionable alerts, and native integrations automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. The company has won over 70 awards for its technology innovation and leadership.