SOLUTION BRIEF

SCALING DETECTION WITH THE THREATDIRECT® SOLUTION

To the unfamiliar, extending a deception-based detection footprint out to remote locations may seem like a cost-prohibitive measure, particularly where the decoy systems must operate in concert within the corporate environment, continue to detect accurately, and engage attackers as "real" systems to identify cyberattacks. The ThreatDirect® solution, a component of the ThreatDefend® platform's BOTsink server, removes these concerns and seamlessly scales the deception fabric across geographically dispersed sites. The solution comes as either a standalone Virtual Machine, a container app, or an endpoint component. It offers a spectrum of possibilities when extending the centrally-deployed detection footprint remotely without requiring a remote deception server. Instead, the ThreatDirect solution leverages local resources to project decoy services to a remote location without increasing the footprint. It seamlessly integrates with a centrally deployed BOTsink server over a WAN connection to present deceptive service as if a local server was hosting them. This type of deployment exacts minimal configuration changes at the remote sites, allowing for rapid deployment across terrestrial and virtual data centers alike, even when they exist within a vendor's cloud.

REMOTE/BRANCH OFFICE, CLOUD, AND DATACENTERS

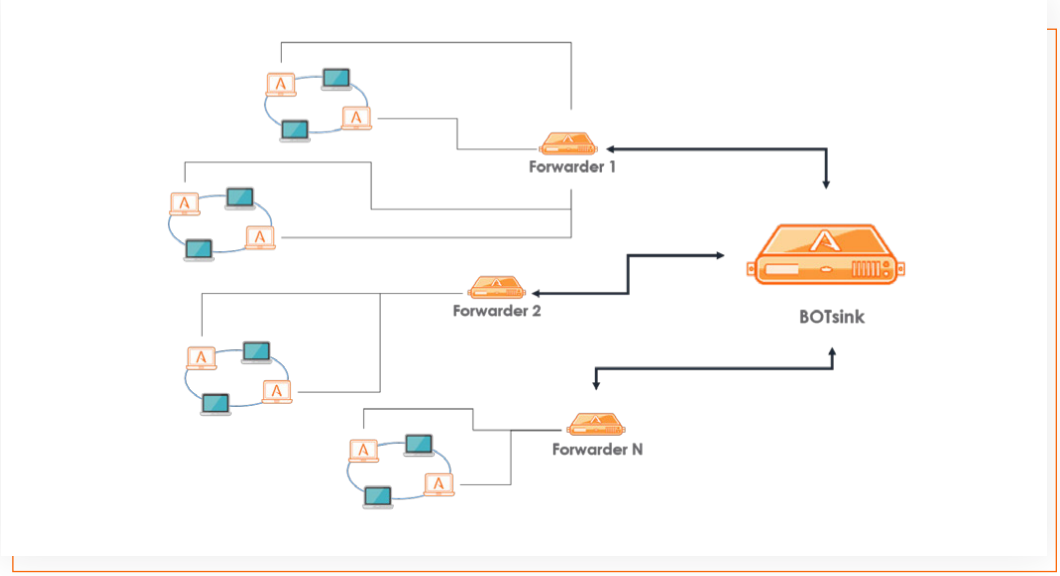
Remote and home offices are becoming a long-lasting extension of the corporate network. Organizations expect individuals to remain as productive as before while operating remotely out of their home offices, accessing remote cloud applications in an environment where the organization's security tools and security teams often lack visibility. Moreover, the remote environments may not possess the same physical security controls as headquarters, and potentially lack the experience and knowledge to patch, operate, and monitor all aspects of their remote infrastructure. EDR may identify nefarious activity on an endpoint but won't provide notification of a remote IoT device passively conducting Man-in-the-Middle (MitM) attacks, or alert when an unmanaged device newly attached to the network attempts reconnaissance by engaging the corporate directory server. Even in scenarios where a directory server operates locally within a remote office, the physical security at the location may make it possible for attackers to conduct offline attacks or physical access to steal passwords. Remote personnel may often overlook an attack impersonating the remote gateway via a MitM attack. Home offices, remote offices, or even distributed virtual datacenters present a unique challenge because they are cost-saving necessities, but also can become easier targets from the attacker's perspective.

Organizations need to accept that advanced attackers can successfully compromise an endpoint, even after deploying traditional security controls such an EDR. Once attackers have control of an internal system, they will

conduct discovery and lateral movement activities to advance their attack. This activity is much more problematic to prevent or detect at remote sites, and as such, the addition of a layered defense becomes critical.

Deploying EDR on a remote system will seek to solve the visibility challenges by subsequently starting a new flow of logs from the endpoint. However, it can be susceptible to evasion, doesn't protect against passive MitM attack, and can be noisy, leading to more alert fatigue.

Adopting the ThreatDefend platform allows organizations to expand their attack surface, whether on-premises, in the cloud, or at remote locations. The platform creates a deceptive fabric where attackers can't move laterally without setting off false alerts, and the ThreatDirect component delivers this capability to extend this detection to remote locations without reconfiguring the centrally- hosted decoys at a minimal cost.



In either a ROBO environment, cloud, or micro-segmented datacenter, the ThreatDirect solution achieves visibility by providing:

- Projections of decoy IPs and services to remote network locations vs. needing a physical appliance
- Visibility into ROBOs, cloud, or datacenter by forwarding traffic that targets decoy IP addresses to a centrally deployed hardware or virtual BOTsink server
- Detecting Man-in-the-Middle (MITM) attacks
- Visibility into network activities by analyzing multicast and broadcast traffic
- Identification of reconnaissance and lateral movement activity originating from within remote networks
- Scaling for the ThreatDefend platform to challenging environments like micro-segmented networks or multiple remote locations.

MANAGED SECURITY SERVICE PROVIDERS

The ThreatDirect solution is also designed MSSPs and provides the ability to offer Deception as a Service. By deploying a BOTsink virtual server in the cloud, or housing a BOTsink server in their datacenter, an MSSP can run decoys on their infrastructure, while monitoring the alerts in their SOC. MSSPs would deploy the ThreatDirect solution instances to their subscriber's networks and handle the associated configuration, monitoring, analysis, and actioning of alerts. This capability can be ideal for subscribers who may not be able to deploy a standalone BOTsink server, but can now take advantage of Deception as a Service, and gain all the benefits listed above while having policies configured explicitly for them.

CONCLUSION

It is critical to have visibility across the entire network with no gaps based on location or resource limitations. With the ThreatDirect solution, organizations can now scale their adaptive defense across remote areas of their network with full-featured deception-based detection, automated attack analysis, and accelerated incident response capabilities. By implementing the ThreatDirect solution, organizations can detect all threat vectors, including Man-in-the-Middle, ransomware, stolen credential, and insider threats, in previously low- visibility areas of their network such as ROBOs and micro-segmented sections. With full network detection, security teams gain confidence that they will receive accurate alerts when threats hit remote or hard-to-detect parts of their network, and that they will have the time-to-detection advantage to stop an adversary before a serious breach occurs..

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides organizations of all sizes with an active defense for early and accurate threat detection. The Attivo ThreatDefend® Platform delivers comprehensive detection for on-premises, cloud, and specialized attack surfaces with a deception fabric designed to efficiently misdirect and reveal attacks from all threat vectors. High-fidelity alerts are backed with company-centric threat intelligence and automated attack analysis, forensics, native integrations streamline incident response. The company has won over 130+ awards for its technology innovation and leadership.
Learn more: www.attivonetworks.com