ThreatDirect™ Virtual Deception Scaling

The ThreatDirect™ solution is a virtual deception-based detection system that provides deception in remote and branch offices without the need for additional BOTsink appliances. The solution is designed to seamlessly integrate with a centrally deployed BOTsink appliance to engage attackers and alert on malicious activity. The ThreatDirect solution is typically deployed in an environment where a full BOTsink deployment is not feasible or cost is a determining factor.

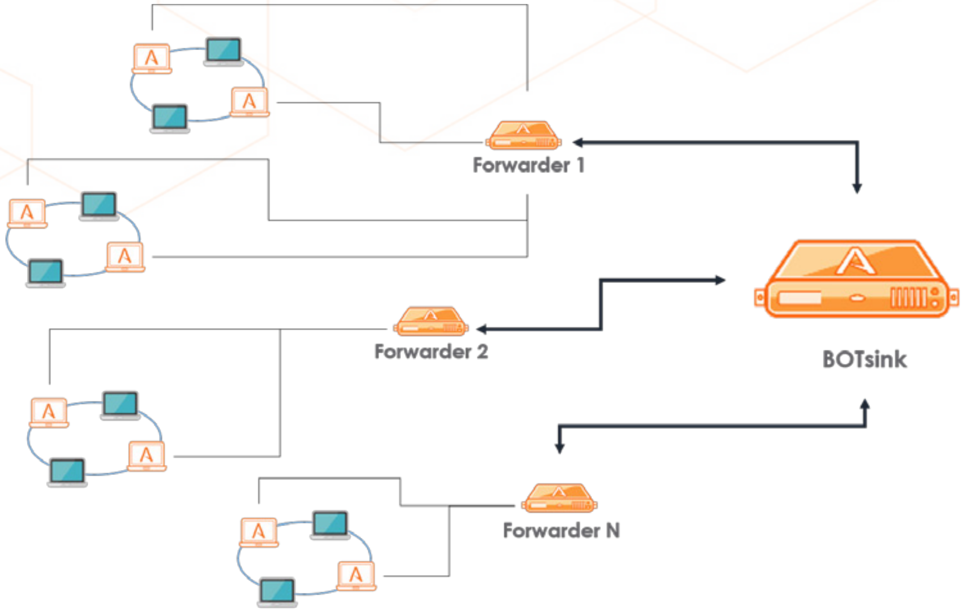
The ThreatDirect solution is designed for scalability; multiple systems can be deployed to implement deception in all the subnets of a heavily segmented network. For example, the ThreatDirect solution can be deployed in multiple branch offices across vast geographical locations with one central BOTsink appliance acting as a deployment hub.

Remote/Branch Office, Cloud, and Datacenters

While Remote/Branch Offices (ROBO) are still part of the organization's security infrastructure, security teams often lack visibility into that portion of the network because it is far removed from headquarters and lacks local skilled professionals to operate its security infrastructure. Additionally, ROBOs face physical security issues that larger offices or headquarters do not face. For instance, a ROBO may not have 24-hour security guards, scan badge access, or provide a highly secure security infrastructure storage room.

These differences present unique challenges to security teams looking to secure their network from cyberattacks. The ThreatDirect solution addresses those challenges by providing organizations the ability to not only gain visibility into but also limit the physical security infrastructure needed within the ROBO.

The ThreatDirect solution can also deploy in a cloud or datacenter environment to extend the reach of a BOTsink, particularly in micro-segmented networks. These environments present similar challenges as ROBO environments. It is difficult to gain visibility into traffic within a cloud environment or in micro-segmented networks, whether in a datacenter or cloud. The ThreatDirect solution can bridge that visibility gap.



Solution for Virtual Deception Scaling

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

- Projection of deception to remote network locations vs. needing a physical appliance
- Visibility into ROBOs, cloud, or datacenter by forwarding traffic targeting deception IP address to a centrally deployed hardware or virtual BOTsink
- Detecting Man-in-the-Middle (MITM) attacks
- Network activities through the analysis of multicast and broadcast traffic
- Identification of reconnaissance and lateral movement activity originating from within remote networks
- Allows the BOTsink to scale in difficult environments like micro-segmented networks or multiple remote locations.

Managed Security Service Providers

The ThreatDirect solution provides MSSPs an additional ability to offer Deception as a Service. By deploying a BOTsink virtual appliance in the cloud, or housing a BOTsink appliance in their datacenter, an MSSP can run engagement servers on their infrastructure, while monitoring the alerts in their SOC. MSSPs would deploy the ThreatDirect solution instances to their subscriber's networks, and can handle the associated configuration, monitoring analysis, and actioning of alerts. Subscribers who may not be able to deploy a standalone BOTsink appliance can still take advantage of the Deception as a Service, and gain all the benefits listed above, while having policies configured specifically 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 gain the time-to-detection advantage to stop a threat before a serious breach occurs.

About Attivo Networks

Attivo Networks® is the leader in dynamic deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyber-attacks. The ThreatDefend Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments. www.attivonetworks.com