SOLUTION BRIEF

PROTECTING POINT-OF-SALE SYSTEMS WITH THE ATTIVO NETWORKS® THREATDEFEND® PLATFORM

Organizations have experienced numerous high-profile breaches across retail, hospitality, food service, and other industries that use Point of Sale (POS) terminals over the last few years, leaving impacted customers angry and frustrated (and the breached organizations' reputations tarnished). Attackers take advantage of vulnerabilities to infect POS systems and devices, gain access to transactional data, and steal personal or financial information for fraud.

The Attivo Networks ThreatDefend platform gives organizations a means to defend their POS systems against attacks. Through early detection, attack misdirection, and threat intelligence development, the platform detects attackers, denies their ability to remain undetected, and deflects their attacks away from production assets.

POS ATTACKS

Today's POS systems, an integral part of virtually every brick-and-mortar business, collect vast amounts of data, including sensitive customer information. Modern POS devices can process transactions, manage inventory, record orders, and connect to other POS systems. However, recent POS-related data breaches and security issues highlight how vulnerable and at-risk these POS systems are. All POS systems have some level of risk when it comes to security. Many attackers target vulnerable networks and launch automated attacks on their POS environments.

According to the SANS Institute, "the basic POS breach phases include infiltration, propagation, exfiltration, and aggregation." In the first phase, attackers gain access to the targeted systems, often exploiting system vulnerabilities or using social engineering techniques like phishing emails. Once inside, the attackers install malware, which spreads until it can access system memory and collect the desired data. From there, attackers move the data to another location within the target's environment for aggregation and finally offload it to an external server accessible to them.

POS security is challenging because of the sheer volume of both known and unknown threats that exist, coupled with the value that POS system data holds for cybercriminals. Attackers frequently create new or update existing POS malware. Many POS systems run older versions of Microsoft Windows or other operating systems, posing security issues and risks as most manufacturers do not provide security patches for outdated operating systems. Cybercriminals can easily exploit such unpatched systems to gain access to POS data. Some businesses send security and system updates to POS devices over corporate networks. If attackers gain access to the corporate network, they can access the POS data on the devices or in storage or infect them with malware during a patch update.

Once attackers gain a foothold inside a network, they can move around undetected to access the POS subnets, install malware on the devices, steal stored data, use the patch servers to compromise the terminals, access servers that hold the transaction data, or conduct other malicious activities. Without a means to detect these actions, organizations that rely on POS systems for transactions remain vulnerable. The ThreatDefend platform provides deception and concealment technologies they can use to protect their POS systems.

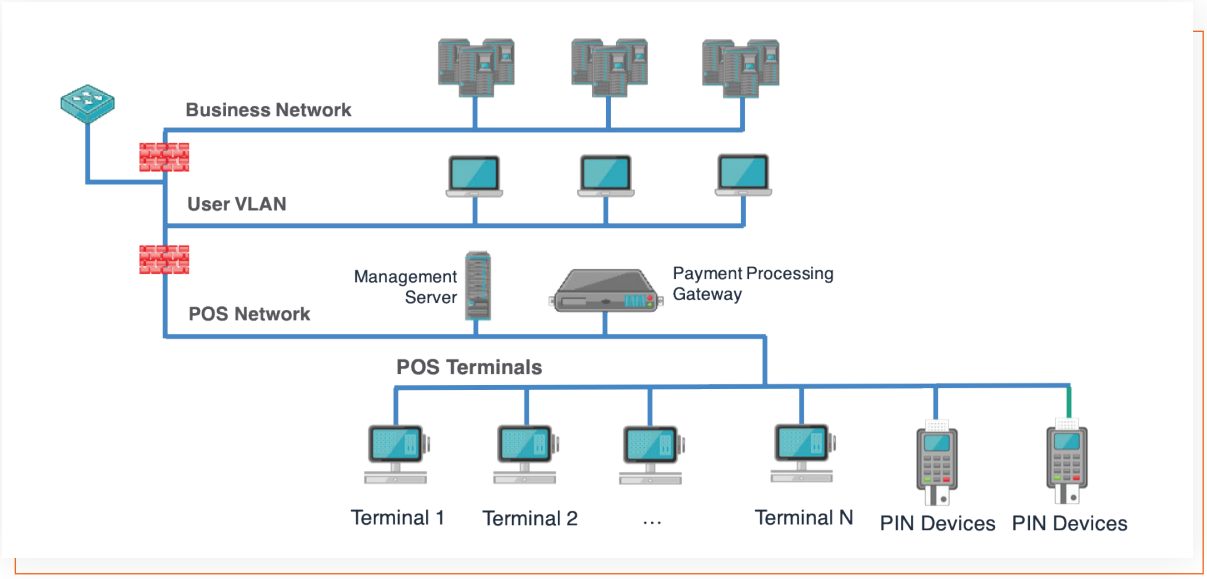

Figure 1: Typical IT infrastructure in a retail enterprise

THE ATTIVO NETWORKS THREATDEFEND PLATFORM

The Attivo Networks ThreatDefend platform uses deception and concealment technologies to provide early and accurate detection of in-network threats, regardless of attack method or surface. 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.

The ThreatDefend Deception Platform creates a threat-informed defense against attackers using its many modular components. The Attivo BOTsink® deception servers provide decoys, the Informer dashboard for displaying gathered threat intelligence, as well as the ThreatOps® incident response orchestration playbooks. The Endpoint Detection Net (EDN) suite includes the ThreatStrike® endpoint module, ThreatPath® for attack path visibility, ADSecure for Active Directory defense, the DataCloak function to hide and deny access to data, and the Deflect function to redirect malicious connection attempts to decoys for engagement. The ThreatDirect deception forwarders support remote and segmented networks, while the Attivo Central Manager (ACM) for BOTsink and the EDN Manager for standalone EDN deployments add enterprise-wide deception fabric management.

The ThreatDefend platform enhances existing security controls to give the organization internal network visibility, prevention, and detection for those tactics that attackers use to bypass traditional controls. With native integration to many of these security controls, the platform accelerates incident response and enables efficient information sharing.

PROTECTING POS SYSTEMS WITH THE THREATDEFEND PLATFORM

The ThreatDefend platform addresses several tactics attackers use to target POS systems, evade detection, move laterally, steal credential, escalate privileged, and collect data.

Attackers inside the network must first find the POS devices or subnets to target, so they conduct discovery activity. They look for POS devices by conducting reconnaissance to find and compromise POS terminals, management servers, patch servers, or databases holding the transaction data. They hunt for credentials that give them access to these assets, either on compromised endpoints or from Active Directory. They will even search for systems to compromise where they can store and aggregate the data for later exfiltration and establish covert communications channels to their Command and Control (C2) servers. They conduct these activities using stealthy tactics that evade traditional internal threat detection, but that the ThreatDefend platform can prevent, detect, and derail.

Before attackers infiltrate the network, organizations can configure the EDN suite to hide and deny access to sensitive files, folders, shares, privileged or local domain accounts, and Active Directory objects to prevent their exploitation, theft, or compromise. When attackers establish a foothold with an internal system, they will look for these sensitive files and accounts. The EDN suite's DataCloak and ADSecure components prevent access or visibility to this data, providing fake accounts and objects that lead the attackers to network decoys for engagement while alerting security teams to the activity. The fake credentials appear real, and the organization can configure them to look like accounts for POS systems, whether for the devices, the servers, or the databases. As the attackers follow them, they engage with the decoys and generate alerts.

The organization can configure the ThreatDefend platform decoys to look like POS terminals, management servers, patch servers, databases, or any other system. These decoys respond when the attackers conduct reconnaissance to find targets for their attacks. The organization can create fake databases, SMB shares, and other services on these decoys to engage the attackers while collecting tactics, techniques and procedures (TTPs), and forensic evidence on all their activities to continually bolster their security posture against similar attacks. The EDN Deflect function identifies illicit inbound or outbound port and service scans, redirecting the connection attempts to decoys for engagement while alerting security teams to the discovery activity. The decoy environment allows the attackers to connect to their C2 servers, capturing all the network traffic for later analysis, but does not enable pivoting back to the production environment.

The ThreatDefend platform addresses these and many other tactics the attackers use to prevent the attack, misdirect activities away from production assets and into decoys, and collect adversary intelligence and forensic evidence to strengthen the organization's security posture.

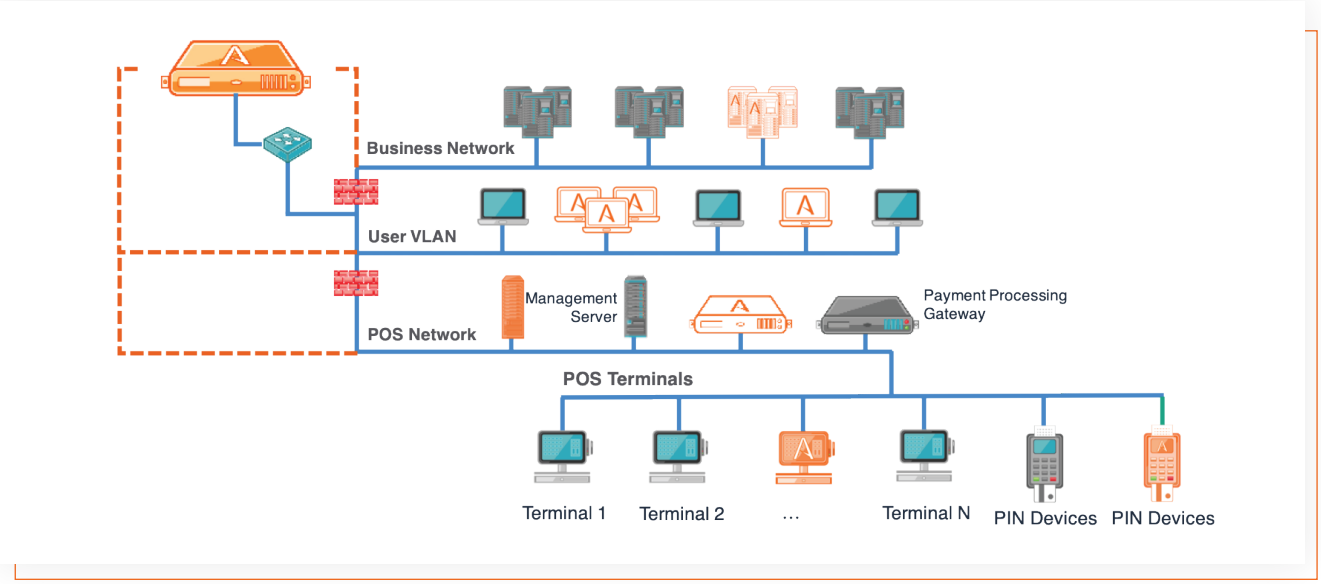

Figure 2: The ThreatDefend fabric protects POS at multiple layers of the network

CONCLUSION

Attackers looking to commit financial fraud and data theft are targetting POS systems because of the difficulties in securing the infrastructure and for transaction data they collect and store. While organizations can take reasonable precautions and adopt security controls to prevent compromises through phishing, malware, or other attack vectors, attackers can evade these defenses to get inside the network and steal data.

The Attivo Networks ThreatDefend platform addresses these evasive tactics with overlapping detection and concealment technologies that deny, detect, and derail the attacker's discovery, lateral movement, credential theft, privilege escalation, and data collection activities inside the network. Prevention solutions do an excellent job of preventing the initial compromise. Should the attacker succeed and evade these security controls, the ThreatDefend platform stands ready to prevent them from breaking out undetected, detecting their illicit activity, and diverting their attacks away from production assets and into decoys for engagement.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.