SOLUTION BRIEF

Protecting Point-of-Sale Environments Against Multi-Stage Attacks

Who should read this document: Point-of-Sale Device Manufacturers, Integrators and Systems Administrators

Symantec

Overview

The rising intensity and sophisticated nature of cyber attacks has created a hostile and precarious environment for businesses charged with protecting their customers' personal data. The retail industry again has the dubious distinction of being the industry liable for the largest number of identities exposed in 2014, accounting for almost 60 percent of all identities reported exposed, up from 30 percent in 2013.[1] In 2013, 17.8 percent of data breaches contained financial information, but in 2014 this number jumped to 35.5 percent. In most cases, this financial information is credit or debit card details. Point-of-sale systems: the credit card swipe machines that have become so ubiquitous in our retail lives are frequently under attack.

To make matters worse, the financial costs of a personal data breach rarely take into account the potential greater cost from loss of future revenues from disaenchanted customers. The fact is that the lucrative business of selling credit card data on the black market has made point- of-sale (PoS) devices, PoS environments and web kiosks a prime target for cybercriminals.

Anatomy of a Point-of-Sale Attack

Whether part of a retail storefront or restaurant, supporting credit card transaction processes within PoS environments requires a technology infrastructure made up of more than just endpoint PoS devices. From relatively small to large complex PoS environments, that infrastructure might include a variety of different PoS terminals, network servers, desktops and other systems. In many instances, these PoS devices connect to the Internet as well. Additionally, infrastructures that support the operation and maintenance of web kiosks often share many of the same infrastructure characteristics of PoS environments.

The complex nature of both PoS and Web kiosk environments has led cybercriminals to create sophisticated attack methodologies that target the acquisition of your valuable credit cardholder data. The methodologies used to breach these environments often involve multi-stage attacks that typically include the following phases:

1. **Infiltration** – There are a variety of methods an attacker can use to gain access to a corporate network. They can look for weaknesses in external facing systems, such as using an SQL injection on a Web server or finding a periphery device that still uses the default manufacturer password. Alternatively, they can attack from within by sending a spear phishing email to an individual within the organization. The spear phishing email could contain a malicious attachment or a link to a website which installs a back door program onto the victim's machine.

2. **Network Traversal** – The malicious files that the cybercriminals have secreted within your network might stay in hiding for weeks, months or years probing, scanning and gathering information about your network. They will try to gain access to other systems, capture administrator access credentials, and further propagate themselves within the environment until they find a way to access your PoS environment.

3. **Data Capture** – Once inside your PoS environment, the threat will install additional malware, which might include network sniffing tools that collect unencrypted credit card data traveling within the internal network or RAM scraping malware that secretly collects personal data every time customer credit cards are swiped in

[1] Symantec 2015 Internet Security Threat Report, Volume 20

the PoS devices' mag-stripe readers. Forwarded to an internal staging server, the credit card data will continue to accumulate until the time comes for exfiltration.

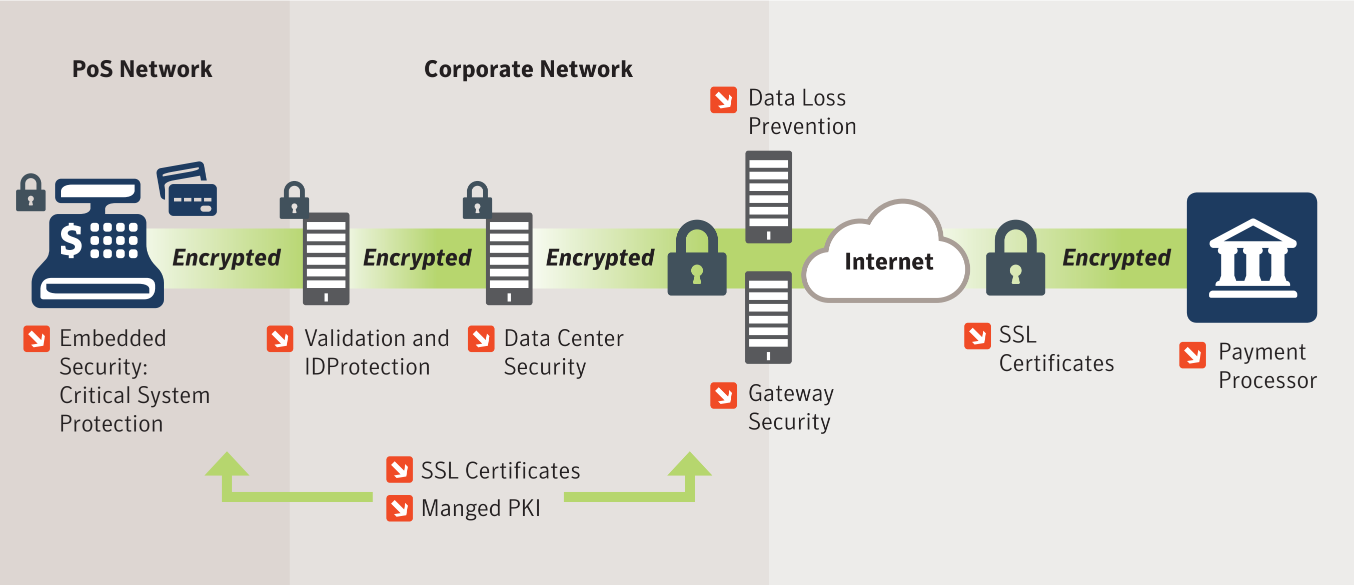
4. **Exfiltration** – To facilitate exfiltration of the credit card data, the data will typically move from the staging server to other systems within the corporate network that have legitimate external access, such as compromised FTP servers or web hosts. The threat manipulates these systems to externally transmit the acquired credit card data to the cybercriminals.

Safeguarding Your Point-of-Sale Environment

Securing your credit card data and PoS environment from sophisticated multi-stage attacks requires multiple layers of protection.

1. Beginning at the endpoint, you need to secure your PoS devices with a strong host protection solution that offers multiple layers of protection.
2. Host-based access controls can safeguard the servers that connect to your PoS devices.
3. Setting up a first line of defense at your gateways—especially email gateways—is key to stopping cybercriminals at what is often their first point of attack.
4. Servers and PoS systems need robust authentication controls to prevent unauthorized access and block malware propagation within your environment.
5. SSL certificates can secure your credit cardholder data by encrypting it while in transit.
6. Finally, a data loss prevention solution can scan traffic leaving your network to ensure confidential data is not leaving your environment.

Through a broad spectrum of unrivaled security solutions and services, Symantec can help defend your PoS environment against even the most persistent and sophisticated attacks.



Symantec™ Critical System Protection Capabilities:

Protection

- Intrusion Prevention
- Intrusion Detection
- System Hardening
- Application Whitelisting
- Application Sandboxes
- Vulnerability and Patch Mitigation

Detection & Compliance

- Real-Time Monitoring and Auditing
- Intrusion Detection
- File Integrity Monitoring
- Configuration Monitoring
- Tracking and Monitoring of User Access
- Logging and Event Reporting

Securing Point-of-Sale Devices

Symantec™ Critical System Protection provides a policy-based approach to endpoint security and compliance.

Symantec™ Critical System Protection has two enforcement components that can be independently activated on Point of Sale systems, prevention and detection.

The prevention component has proactive enforcement rules that can stop malicious activity before it occurs, the detection component monitors for system activity as it occurs and can trigger event based actions. Both components provide granular control over logging using policy settings to give visibility into actionable events as well as the efficient management of high volume events necessary for regulatory or forensic purposes. Thus, in combination, the two components provide unique capabilities to both secure a system and to address regulatory compliance requirements. This includes regulations such as PCI-DSS that requires companies to deploy file integrity monitoring for critical system and application files changes. Detecting that an important operating system binary like svchost.exe was recently modified is very different from preventing the modification in the first place. Symantec™ Critical System Protection lets you configure and use both detection and prevention as needed to address your auditing, compliance, and security requirements.

System Hardening and Application Control

Controlling what applications can run on your PoS devices is one of the most vital steps to protecting against unauthorized access and attack.

Symantec™ Critical System Protection policies provide thousands of pre-built rules that comprehensively monitor and harden the operating system of enterprise systems and require minimal tuning. Memory controls detect buffer overflows and unusual memory allocation and permissions complimenting an effective device hardening strategy.

Single use devices such as point of sale terminals perform predictable functions, meaning the device should always be in a known state, with known applications performing known behavior Symantec™ Critical System Protection can be configured to enforce application whitelisting, ensuring only predefined programs can be executed with specific attributes controlling the manner in which they are called. Furthermore, program execution can be contained within a sandbox, allowing strict control over the behavior of the application. This particularly useful where operating system permission levels allow unnecessary actions to be carried. Symantec™ Critical System Protection application whitelisting and sandboxing form part of a least privilege protection strategy permitting only known applications to perform known functions.

Adding another layer of security to your defenses, Symantec™ Critical System Protection provides rules based system level and as well application level firewalls to block network-based attacks against your PoS devices. The firewall lets you restrict which applications on PoS systems can communicate on the network, which ports they can use, and what they are allowed to talk to.

To circumvent network restrictions and application controls, some cybercriminals will try to steal credit card data through physical access to a PoS device. As PoS terminals become more advanced with computer-like characteristics, the methods for unauthorized physical access often increases. Symantec™ Critical System Protection enables you to block and granularly control devices connected to your PoS systems' communication interfaces, such as USB, firewire, serial, and parallel ports. It can prevent all access to a port or only allow access from certain devices.

Intrusion Detection

The Symantec™ Critical System Protection detection policies monitor files, settings, events and logs, and report anomalous behavior. Features include sophisticated policy-based auditing and monitoring; log consolidation for easy search, archival, and retrieval; advanced event analysis and response capabilities. To further harden the device it provides a combination of file integrity monitoring and registry integrity monitoring.

Deployment

Symantec™ Critical System Protection can be deployed in managed and standalone mode. This is particularly useful for device manufacturers who create an out of the box security policy for their product ensuring the device is adequately hardened from the moment it is activated. Retailers, integrators and device operators may choose to deploy the agent after market on devices being newly deployed or previously installed. Administrators can opt for configurations where the agent will communicate with the management console for policy updates and reporting providing real time visibility of your security posture. Symantec™ Critical System Protection allows the creation of customer agent installers, deploying only the code required to perform the protection and/or detection functions as defined in the agent configuration. This allows manufacturers and device operators to efficiently deploy in resource constrained environments.

Securing Thin Clients, Kiosks & Tablets

If you have thin clients, kiosks, or tablets in your Point-of-Sale environment, Symantec™ Endpoint Protection also provides you with multiple layers of protection to safeguard your endpoints. In addition to standard signature-based antivirus, Symantec™ Endpoint Protection offers application control, network threat protection, device control and advanced behavioral and reputation malware detection to harden your thin clients and kiosks. Its application control capabilities enable you to lock down and to prevent attacks through powerful and flexible blacklisting and whitelisting capabilities. You can lock down system security even further by limiting application execution to only the essential applications that your thin clients and kiosks need to operate. In whitelist mode, Symantec™ Endpoint Protection uses checksum and file location parameters to verify whether an application is actually approved. Additionally, Symantec makes it even easier to harden your thin clients and kiosks with application control templates that contain predefined policies blocking application behaviors known to be malicious.

Defending Gateways Against Infiltration

During the infiltration stage, cybercriminals try to establish an initial foothold inside your corporate network with the hope of eventually compromising your PoS environment and stealing credit cardholder data. While the actual point of attack varies during this stage, the threat typically tries to gain entry through a web or email gateway. Symantec offers a combination of solutions to protect your gateways against the various types of infiltration attacks. **Symantec™ Web Gateway** and **Symantec™ Web Security.cloud** protect against network-borne threats such as malware and spyware allowing you to block new and unknown malware at the gateway level, before it ever reaches your endpoint.

Symantec™ Web Gateway detects and automatically quarantines devices that display suspicious behavior or that contact malicious command and control destinations on the Internet. Symantec™ Web Security.cloud offers outbound data protection policy to detect and contain attempts to exfiltrate sensitive and confidential data from the network while Symantec Web Gateway can control data loss by directly integrating with the market leading **Symantec™ Data Loss Prevention** platform. **Symantec™ Messaging Gateway** and **Symantec™ Email Security.cloud** provide proactive protection across email platforms. Both solutions allow you to secure your email with effective and accurate real-time antispam and antimalware protection, targeted attack protection, and advanced content filtering. Symantec™ Email Security.cloud includes Skeptic™ predictive analysis with real-time link following to block emails with malicious, shortened links before these emails can even reach your users. Symantec™ Messaging Gateway features "Disarm™", an innovative new Symantec technology that thwarts targeted email attacks and removes exploitable content hidden inside an attachment. It then creates a clean copy for delivery to the user.

Minus the malware, the clean copy contains an exact replica of the original attachment, enabling the user to still receive the expected content.

Securing Access to Your Environment

Once a threat infiltrates your environment, it tries to spread across your network by capturing high-level access credentials to your servers and PoS systems. **Symantec™ Validation and ID Protection Service** and **Symantec™ Managed PKI Service** help stop the spread of these threats through cloud-based strong authentication services. Leveraging two-factor authentication, these services help block malicious unauthorized attackers from accessing your networks, PoS devices, and applications. Additionally, Symantec™ Validation and ID Protection facilitates your compliance with the Payment Card Industry Data Security Standards (PCI-DSS) requirement for merchants to "incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties." The service offers a wide choice of PCI-compliant two factor authentication options, including software, hardware, mobile tokens, risk-based authentication, user certificates, and device certificates.

Securing Network Traffic

To protect your credit cardholder data from cybercriminals, it's vital to encrypt it when transmitted over public networks, such as when it's sent from your retail location to a payment processor. However, it's also a best practice to encrypt your credit cardholder data traffic inside your network as well. Symantec has an extensive **Secure Sockets Layer (SSL) certificate** product offering to meet all of your corporate network needs. Symantec offers a wide range of robust and scalable security options, including **Elliptic Curve Cryptography (ECC)**, Digital Signature Algorithm (DSA) and RSA encryption. Its SSL validation services leverage a robust validation infrastructure that has experienced 100 percent uptime since 2004 and processes an average of 4.5 billion hits per day. Symantec makes it easy to manage the complete SSL certificate lifecycle from a central management console with delegated administration, role-based access and instance issuance of certificates.

Keeping Customer Data Safe from Internal and External Threats

During the exfiltration phase, cybercriminals attempt to move credit card data from a staging server to systems with legitimate external access. To prevent threats from transmitting data through these channels, data loss prevention technology can be used to scan servers and monitor network protocols for credit card data before it has the chance to leak outside the corporate network. To stop this exfiltration or leakage, **Symantec™ Data Loss Prevention** discovers, monitors and protects cardholder data wherever it is stored or used, including endpoints, data centers and networks. To prevent improper use or theft of data, it can identify any unusual or anomalous activity, including questionable accumulation of credit card data in improper data stores or inappropriate access to any sensitive data. Its central management console makes it easy to manage data loss policies, remediate incidents and gain visibility into vulnerabilities and at risk data. Symantec™ Data Loss Prevention reduces the risk of confidential data loss and theft by helping you understand where your data is going, how it's being used, and how to prevent its loss or theft.

Multi-Layered Security for Point-of-Sale Devices and Environments

Symantec provides the comprehensive security expertise and broad spectrum of solutions needed to protect your credit cardholder data from even the most persistent and sophisticated cyber attacks.

At PoS terminals and kiosks, Symantec delivers multi-layered protection to harden these endpoints against the most sophisticated attacks. It provides comprehensive security for servers, helping to prevent threats from infiltrating your network in the first place. Symantec adds additional defense layers with gateway protection offerings that block attempts to breach your environment via email or web attacks. It further protects against sophisticated attacks with cloud-based two-factor authentication services that block unauthorized user access, Secure Sockets Layer (SSL) certificate offerings to encrypt in-transit credit cardholder data, and data loss prevention to ensure that your PoS data is not lost or stolen.

Powered by the Symantec Global Intelligence Network that consists of millions of security sensors in more than 150 countries, Symantec's security intelligence feeds into our solutions through sophisticated detection capabilities, such as Disarm™ and Skeptic™ technologies. This deep security expertise coupled with our broad spectrum of industry-leading solutions makes Symantec the ideal partner to help protect your PoS environment from today's sophisticated attacks.

For more information on how Symantec can help secure your PoS devices and environment, visit http://go.symantec.com/pos-protection

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com