SOLUTION BRIEF:
PROTECTING POS DEVICES & BROADER ENVIRONMENT

Solution Brief

Protecting PoS Environments Against Multi-Stage Attacks

Who should read this paper

Point-of-sale systems administrators and end users

Symantec

Content

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. In 2012, credit card and debit card fraud resulted in losses amounting to $11.27 billion[1]. While it's not yet known how much higher the cybercrime costs were for 2013, cybercriminals exposed more than 342 million identities worldwide in 2013[2]. A single cyber attack in November of 2013 alone exposed 110 million identities, while a different attack in January 2014 exposed more than 105 million identities[3].

News headlines have been inundated with stories of massive personal and credit card data breaches. According to analysts, a single orchestrated breach of credit card magnetic stripe data that occurred recently will likely cost the victimized business about $240 million. To make matters worse, the financial costs of such personal data breaches often don't take into account the potential greater cost from loss of future revenues from disenchanted 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 PoS 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 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.

1- Nilson Report, August 2013
2- Symantec Intelligence Report, December 2013
3- Symantec Intelligence Report, January 2014

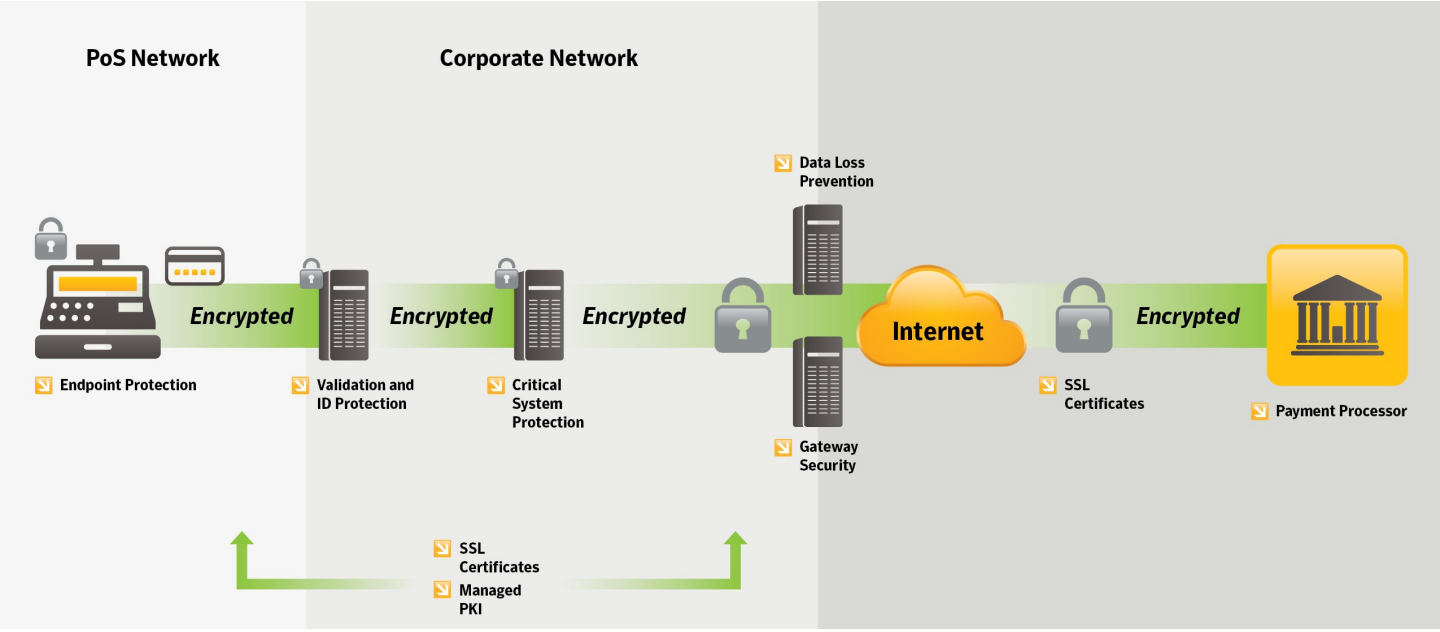
4. **Exfiltration** – To facilitate exfiltration of the credit card data, the data will typically move from the staging server to other systems within the corporate network that have legitimate external access, such as compromised FTP servers or web hosts. The threat manipulates these systems to externally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

Safeguarding Your PoS 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 endpoint 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.



Payment Card System Infrastructure and Symantec Solutions

Securing Windows and Windows Embedded POS Devices

Symantec™ Endpoint Protection integrates multiple layers of protection to safeguard your endpoints, including PoS devices or web kiosks running Windows Embedded or other versions of Windows. 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 PoS devices and safeguard your customers' credit card data.

System Lockdown 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. The application control capabilities in Symantec™ Endpoint Protection enable you to lock down your PoS systems and prevent attacks through powerful and flexible blacklisting and whitelisting capabilities. You can use blacklists to block any unapproved applications or use whitelists to allow only known-good applications from running on your systems.

You can lock down system security even further by limiting application execution to only the essential applications that your PoS devices 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 PoS devices with application control templates that contain predefined policies that block application behaviors known to be malicious.

Network Threat Protection

Adding another layer of security to your defenses, Symantec™ Endpoint Protection provides Intrusion Prevention System (IPS) and rules-based 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 do.

The IPS component of Symantec™ Endpoint Protection analyzes all inbound and outbound communications for data patterns characteristic of typical attacks. If it detects a known attack signature in a data packet, it automatically discards those data packets. The IPS can also sever the connection with the system that sent the offending data packet for a specified period of time.

Device Control

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™ Endpoint 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 with a specific vendor ID.

Advanced Behavioral and Reputation Malware Protection

For PoS devices connected to the internet, Symantec™ Endpoint Protection lets you take advantage of the advanced reputation and behavioral-based malware detection powered by Symantec Insight™ and SONAR™. These security technologies leverage the Symantec Global Intelligence Network (GIN) – the largest and most sophisticated security intelligence network in the world.

Symantec Insight™ uses reputation security technology that tracks billions of files from millions of systems to identify new threats as they are created. It utilizes contextual awareness to separate files at-risk from safe files for faster and more accurate malware detection. Additionally, it significantly reduces scan overhead by only scanning at-risk files, while reducing the risk of false positive detections by verifying a file's reputation before conviction. Furthermore, with Symantec™ Insight for Private Cloud you can host an on-premise instance of Insight that allows you to leverage its benefits without internet exposure.

SONAR™ uses artificial intelligence and sophisticated behavioral analysis to detect emerging and unknown threats. It monitors more than a thousand file behaviors as they execute in real-time to identify suspicious behavior and remove malicious applications before they can do

harm. To enhance detection of zero-day threats, SONAR™ works with Symantec Insight to monitor and stop emerging and previously unknown malware.

Securing Servers and Non-Windows POS Devices

In environments with PoS devices that run on variations of Linux, Unix or other non-Windows operating systems, **Symantec™ Critical System Protection** can provide the strong protection these devices need. The fact that Symantec Critical System Protection has a small resource footprint and doesn't require any definition files also makes it ideal for non-Windows PoS devices with low resource needs.

Symantec™ Critical System Protection is also the ideal solution to safeguard your network servers from sophisticated, multi-stage attacks. During multi-stage attacks, cybercriminals frequently target servers either in the PoS environment or an associated corporate network. Attack techniques vary from sophisticated penetration techniques, to exploiting unintentional configuration errors on a server. Symantec™ Critical System Protection employs a combination of host-based intrusion detection (HIDS), host intrusion prevention (HIPS), and sandboxing or least privilege access control technologies to pro-actively harden servers and block attacks. It utilizes granular, prevention and detection policies to define at a very low and strict level what and how system resources can be used or accessed, and by whom.

The ability of Symantec™ Critical System Protection to strictly limit actions on systems and prevent the execution of malicious processes derives from a variety of solution features. It employs application whitelisting and protected whitelisting with "default deny" policies as well as the option to allow applications not in the whitelist to run in a restricted sandbox. To protect against new classes of threats, it utilizes comprehensive IPS protection that includes sandboxing and Process Access Control (PAC). Its compensating HIPS controls restrict application and operating system behavior using policy-based least privilege access control. The solution's firewall controls inbound and outbound network traffic to and from the system. To further harden the device it provides a combination of file and system tamper prevention, as well as application and device control.

In both your data center and PoS environments, Symantec™ Critical System Protection minimizes network bandwidth consumption due to its limited need to communicate over the network or internet. The solution has minimal impact on an organization's operations through pre-defined and targeted protection policies, as well as its ability to mitigate out-of-band patch cycles and secure out-of-support legacy systems by shielding servers and PoS devices from attack. Additionally, Symantec™ Critical System Protection gives you real-time visibility into the security posture of your servers and your PoS devices through a combination of real-time monitoring, consolidated event logs, reports, and IT analytics cube integration.

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. With its Verisign acquisition, 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 PoS 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 web 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 200 countries, Symantec's security intelligence feeds into our solutions through sophisticated detection capabilities, such as Insight™, SONAR™, 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 Go.symantec.com/sep12.

Glossary

About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

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