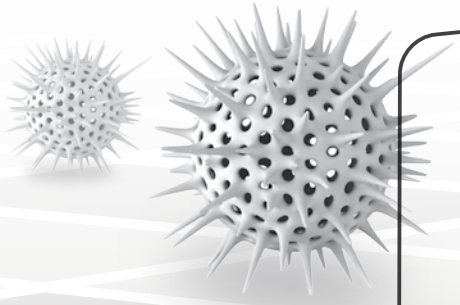
POINT OF SALE SECURITY SOLUTION BRIEF



Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The retail industry has experienced an alarming number of data and security breaches. These attacks resulted in the loss of millions of customer credit cards and personal information. The companies involved experienced negative financial effects from the event, with the largest retailer experiencing a 13% drop in its market valuation and a reduction in comparable-store sales. These breaches impact companies large and small. Notable names like Michaels, Neiman Marcus, PF Chang's, Target and Home Depot have all suffered staggering losses from POS-related data breaches.

Customer concerns over privacy and financial security are shaken, and corporate boards are actively looking for structural changes. The short-term effects are just now coming to light. The long-term impact will only be known in the coming years.

In responding to these types of incidents, companies often pursue knee-jerk reaction tactics. For example, they will focus on the most obvious weakness or choose a method that appears most prominently in the news.

In the case of the recent retail data breaches, much emphasis has been placed on a move to "Chip and PIN" credit cards—payment methods that employ two factor authentication through a physical chip on a card that is tied to a user's personal identification number (PIN). But, a cursory review of the attack methods associated with the retail breaches shows that Chip and PIN would not have prevented these incidents.

The attackers targeting the retail stores used available remote connections to access store networks and installed multiple variants of malware and software tools to capture and export customer data. Shortcomings in store network design and point of sale (PoS) configuration further enabled the attacks by simplifying horizontal movement and malware infestation. Companies need to employ protections across their entire network, not just the parts they believe to be most vulnerable.

Rather than pursue the popular approach, a more effective strategy is to take a broader view of incident tactics and implement a multi-layered approach that addresses the individual attack methods and the wider risk environment.

This document outlines such an approach. It leverages the Check Point Software Defined Protection (SDP) architecture:

- Enforcement Layer: SDP begins with a simple to follow pathway toward effective and manageable network segmentation, which is one of the fundamental controls of the payment card industry's PCI DSS standard. This method leads to a practical way of implementing and locating enforcement technologies across network resources.
- Control Layer: From there SDP looks at the definition and distribution of controls, both in terms of security policies defined by administrators and threat prevention technologies that operate independently and automatically.
- Management Layer: And finally, SDP addresses the management of enforcement points and controls and ensures visibility and operational efficiencies.

These principles serve as the main chapter titles of this document. They also provide context to the recommended controls.

This document operates at multiple levels. It begins at a higher level and then dives into greater detail. Readers can use the document as a single document, or leverage its component sections as stand-alone sub-documents.

The areas covered in the pages that follow are:

- An analysis of recent security events in the retail sector
- Retail network security design principles
- Retail network enforcement layer
- Control layer considerations
- Management layer guidelines

The document includes network diagrams and screenshots for illustration purposes. These assist in the visualization of the location and configuration of enforcement points and controls.

SUMMARY OF RECENT SECURITY EVENTS IN THE RETAIL SECTOR

In September 2014, the largest home improvement retailer in the US announced it had experienced a POS information breach. While details are still emerging as to the entry point and methodology used in this attack, the topic of comprehensive POS security across a company's entire network is front and center in the industry.

The single largest revenue day for retailers in the United States is Black Friday. It occurs on the last Friday of November following the Thanksgiving Day holiday. It also kicks off the Christmas shopping season. In 2013, attackers took advantage of the spending spree by infiltrating a major US retailer with malware. They stole 41 million credit and debit card details and even more personal data.

The actors behind the attack began with a reconnaissance campaign by identifying and targeting a key service provider to the major retailer. After successfully compromising the third party, the attackers leveraged a system designed for electronic billing, contract submission, and project management to breach the retailer. Once inside the retailer network, the attackers were able to access and install a malware specific to POS devices.

The malware operated on POS devices used in payment card transactions. The installed software was a 'memory scraper' that looked inside the POS registry files for payment card information. This variant of malware leveraged a published Inter Process Communication API to know where and when to look inside the device memory.

After the attackers identified the location of the payment card information, they followed a multi-tier process:

- The payment card information was stored in a local file with a .dll extension. This fake .dll file was hidden in a system directory on the POS platform.
- Once a day, between the hours of 10 AM and 5 PM, the malware would copy the fake .dll to a centralized server via a standard windows network share inside the retailer's network. The file transmitted to the destination as text file with a disguised filename that resembled system or user logs.
- This network share was accessed using a known username and password combination from a software system that performed hardware performance measurement used for capacity planning.
- The malware that ran on the windows-based server hosting the file share would FTP the text files containing the credit card information to a hijacked FTP server outside of the retailer's network. These FTP sessions lasted 2 weeks and transferred 11 Gigabytes of data in all.
- Finally, the attackers retrieved the credit card files via FTP from a virtual private server.

The net result of this activity was the theft of tens of millions of customer payment information records.

The attacks hit some of the largest and most trusted retailers in the United States. Events that use methods with similar characteristics affect companies operating in other industries across the globe.

The United States Department of Homeland Security issued an Infection Assessment for the POS Malware, known as 'Backoff', on August 22, 2014. This malware installs remotely by exploiting accounts with administrator privileges. After install, 'Backoff' collects and exfiltrates customer payment card data. The U.S. Secret Service identified seven POS providers/vendors with infected POS systems, impacting over 1,000 large and small U.S. businesses.

By analyzing attacks like the 'Backoff' malware, a set of security implementation principles emerge that can dramatically improve retail network security.

The phases of the attack outlined above reveal principles that can be used to design retail network security architectures.

#1: ENFORCE SEGMENTATION TO PREVENT HORIZONTAL MOVEMENT

The basic fact that attackers can successfully move via a business' network initial breach point to the POS systems implies that there were insufficient controls to limit horizontal network movement.

An effective way to address this issue is to implement tight segmentation of the retail store network. The principle of segmentation is in PCI-DSS v3. The relevant language in the standard reads:

> *Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network. To be considered out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE, such that even if the out-of-scope system component was compromised it could not impact the security of the CDE.*[1]

The diagram in Figure 1 visualizes one possible method for separating retail networks into different component elements. PCI-DSS v3 does not require segmentation. Instead, the standard strongly recommends it and notes that it can reduce risk and scope and cost of PCI assessment. Considering the cost of recent events, it would seem that segmentation is a fundamental security requirement and not just a recommendation.

The diagram below visualizes how retail networks can be separated into different component elements.

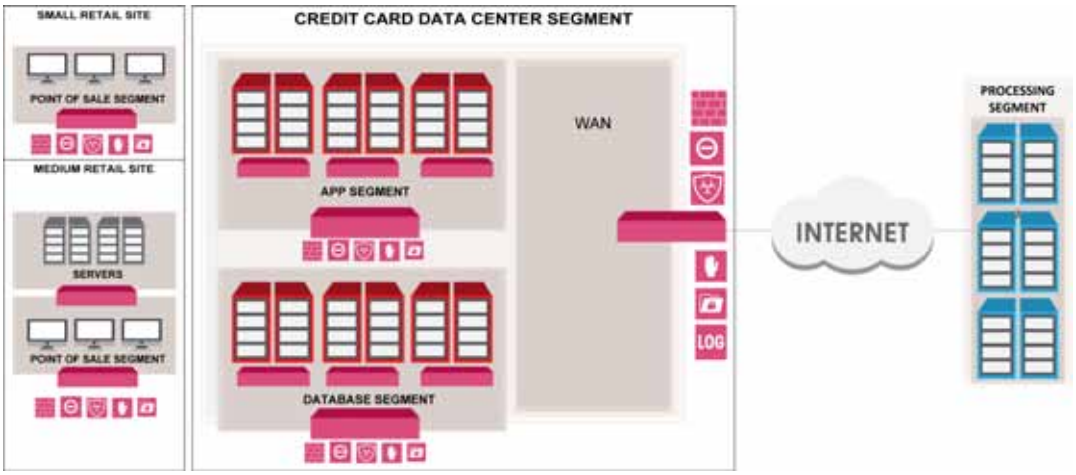


Figure 1 - Sample Segmentation Topology

[1] PCI Security Standards Council, LLC, *Payment Card Industry (PCI) Data Security Standard v3.0* (2013), 11.

RETAIL NETWORK SECURITY DESIGN PRINCIPLES

The following hierarchical trust framework defines logical segments suitable for any POS architecture. It follows a zero-trust framework approach. All network communication between segments should be clearly delineated and assigned an associated risk factor value based on three main factors: (1) whether the transmission is of critical information, (2) whether it is within the POS management plane, and (3) whether it contains critical credit card data.

The segmentation architecture is as follows:

- POS Segment: Contains POS devices and all other credit card processing supplementary equipment.
- Application and Maintenance Segment: Contains all supporting application and maintenance infrastructure.
- Database Segment: Contains supporting database servers and associated administrative machines.
- Process Segment: Typically, third party relationships drive the payment-processing segment. This is not typically under the control of the POS owner-operator. However, large banks may facilitate an entire POS transaction from the initial card swipe through the Host processing network to the Bank Processing Segment.

A SUMMARY OF PRIMARY PAYMENT CARD INDUSTRY (PCI) SECURITY REQUIREMENTS

The Payment Card Industry Security Standards were developed to encourage broad adoption of consistent data security measures globally. The PCI standard provides a baseline of technical and operational controls designed to specifically protect credit card data. PCI consists of three core components that establish security practices for each phase of the credit card transaction lifecycle. While PCI DSS is the most commonly referenced standard, the industry also has the Payment Application Data Security Standard (PA-DSS) and PCI PIN Transaction Security (PTS) Point of Interaction (POI) requirements. These address the payment application as well as physical terminal and PIN acceptance, respectively.

The PA-DSS provides a data standard for software vendors that develop payment applications. The standard aims to prevent payment applications designed by third parties from storing prohibited secure data including magnetic stripe, CVV2, or PIN. The most common method for accepting credit and debit transactions are those devices that require PIN entry. Unfortunately, these devices are the most targeted for criminal attacks. To combat these threats and meet industry needs, the PCI council created the PTS POI standard to ensure payment security standards.

SECURE COMMUNICATIONS TO FURTHER ISOLATE PAYMENT SYSTEMS

Stores today often support multiple communications applications: customer Wi-Fi, vendor and third-party systems, employee productivity tools, inventory management systems and POS systems. To save money, companies will often leverage shared transport networks within the store, between stores, and to the Internet.

Shared networks introduce risk. Mitigating this risk requires extra controls. As noted above, segmentation helps alleviate such risk. In instances where sharing a network connection cannot be avoided, an additional effective protection is the encryption of sensitive data and network transmissions. Implementing secure encryption protects transactions and communications. Encryption protects all outbound traffic and creates a natural barrier against all non-approved inbound traffic. This maintains customer data integrity and confidentiality. It also helps companies comply with Requirement 4 of PCI DSS v3: "Encrypt transmission of cardholder data across open, public networks." [2]

Securing communications between POS devices and the supporting architecture protects credit card information in transit from other devices or 'prying eyes.' Employing Virtual Private Network (VPN) infrastructure encrypts data at the packet level. Even if an attacker uses packet sniffers, any data they capture would be secure. The underlying VPN infrastructure additionally provides integrity to detect any instances of tampering with transmitted messages.

#2: DEFINE CONTROLS TO RESTRICT ACCESS, LIMIT APPLICATION USE AND SECURE DATA

In the above-described attack, the initial network breach then followed horizontal movement to the POS Network. The attackers exploited inadequacies in the network's access control and data security measures. The attackers were able to install new software on devices using generic passwords and gain access to sensitive networks. They then transferred files within and outside the network via FTP.

PCI-DSS v3 requires "strong access control measures." For the most part, the requirements of PCI-DSS v3 section 7 refer to user passwords and the implementation of user access controls based on "need to know" and "job responsibilities." [3] Both are standard best practices for all environments and in all types of industries, not just PCI.

Achieving levels of security that can prevent these types of attacks requires more stringent access controls at every level, not just for system access. Specifically:

- Companies should develop access control rules that limit the types of applications used by employees and systems.
- Administrators should create policies that restrict the flow of specific application traffic only to specific network segments that require such applications.
- Policies should bind application use to validated user identity checks based on business function that is consistent with broader company guidelines.

[2] PCI-DSS v3, 44.
[3] PCI-DSS v3, 61

INTEGRATED DATA SECURITY

The focus of PCI-DSS v3 is data protection. Requirement 3, entitled "Protect stored cardholder data" [4] includes a range of controls intended to protect payment card information and evaluate the effectiveness of enforcement measures. These include standards for storage, encryption and obfuscation, key management and ensuring least privilege for employees with access to sensitive data.

The standard also states, "Documenting cardholder data flows via a dataflow diagram helps fully understand all cardholder data flows and ensures that any network segmentation is effective at isolating the cardholder data environment." [5]

This more general guidance is a best practice recommendation. All organizations should assess how data flows across their networks and should determine if segmentation rules allow unauthorized data flows.

Considering the scope of the recent attacks, retail store networks should also implement data loss prevention (DLP) technologies as an integral part of their security policies as an emergency stopgap measure.

Deployed systems should enforce data flow restrictions not just at the network level, but also higher in the stack. Administrators should create rules that look specifically for data constructs that match payment card data. They should also include policies that identify the types of methods attackers use to exfiltrate data, such as large encrypted and compressed files, and block their attempted transfer across networks.

#3: LEVERAGE THREAT PREVENTION

PCI-DSS v3 has a variety of requirements associated with malware, including:

- Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs[6]
- Requirement 10: Track and monitor all access to network resources and cardholder data[7]

The controls of these requirements call on PCI-relevant companies to operate and continuously update anti-malware systems and regularly monitor for activity consistent with malware behavior.

The PCI language associated with malware focuses on anti-virus software, specifically personal computers and servers. It notes that malware evolves and recommends companies implement anti-virus software both within and on any network that touches their POS network. Finally, the standard recommends companies supplement anti-virus with additional anti-malware solutions.

Malware played the key role in the retail attacks of this past year. According to recent press coverage and company announcements, the victim companies had employed a variety of systems designed to identify malicious activity on the network. A major vulnerability was the security solution employed was configured to monitor and report on suspected malware events, but not prevent them.

[4] PCI-DSS v3, 34
[5] PCI-DSS v2, 11
[6] PCI-DSS v3, 46
[7] PCI-DSS v3, 82

Anti-virus software and monitor-only malware detection systems are insufficient to protect customer payment data. Instead, companies should integrate comprehensive threat prevention technologies across their networks. These systems should draw on an understanding of threats and threat behavior. They should pull data from collaborative real-time threat intelligence received from the community, and they should automatically update protections that adapt to the real-time threat landscape without the need for security administrators to follow up manually on thousands of advisories and recommendations.

#4: INTEGRATE SECURITY AND EVENT MANAGEMENT

Network administrators and analysts are barraged daily by a deluge of warnings and logs. Separating the critical events from the routine warnings can be challenging at best. Attackers have become adept at disguising malware as routine tasks allowing them to hide in plain sight.

The events of 2013 demonstrated that it could be very difficult for even the most sophisticated IT security teams to identify critical activity. Indeed, the lessons learned from the breaches include a need to activate protections and not just use monitoring technologies. The post-mortem analysis also shows that companies require methods to understand the significance of events more quickly and to link event management and protection controls into a single process.

This last point is critical. Visualizing event management security management separately gives security teams no effective method of responding to security threats. Advanced Security Operations Centers (SOCs) are important. Just as important are hands-on tools integrated into the management tools of security technologies themselves.

The pages that follow provide sample configurations and examples of settings associated with the security guidelines outlined above. Users of Check Point solutions can use these examples as pointers towards the enforcement technologies integrated into their Check Point infrastructures.

NOTE: As with all security programs, organizations must consider their unique business requirements and risk profiles before implementing any specific solution. The examples below may not be appropriate for individual company configurations or rule-bases so consult your Check Point representative or security expert before implementing any specific solution shown in these examples.

The first step in securing the enterprise is to identify where to implement enforcement points on both the network and hosts in order to mediate interactions between users and systems.

ENFORCEMENT LAYER: SAMPLE CONFIGURATION

Segmentation is critical for the survival of an organization under attack and is therefore the main principle behind the Enforcement Layer. Segmentation in the SDP Architecture prevents a threat from proliferating within the network. This keeps an attack targeting a single network component from undermining the entire enterprise's security infrastructure.

FIREWALL—ALL SEGMENTS: ESTABLISHING THE ZERO-TRUST POLICY

The POS device atomic segment is the segment of elements that share the same policy and protection characteristics. It should adhere to strict physical segmentation guidelines in addition to strict firewall policies. Segment policies should define directional pathways of dataflow between the POS devices and the required backend server architecture. Any deviation or abnormality from established policy should immediately trigger automated alerts and automated isolation from the network.

EXAMPLE FIREWALL POLICY

Allow PoS to App Servers	PoS-Systems	Application-Servers	MyIntranet	ghttps	accept	Log
Allow PoS to DB Servers	PoS-Systems	Database-Servers	MyIntranet	MS-SQL	accept	Log
Allow only App & DB Servers	Application-Servers Database-Servers	Credit-Card-Processing-	Any Traffic	ghttps	accept	Log
Drop & Alert	Any	Any	Any Traffic	Any	drop	Alert

Figure 2 - Point of Sale Relevant Firewall Rules

In the firewall policy example shown in Figure 2, only the segmented POS systems can communicate with the Application-Servers via the HTTPS protocol or Database-Servers via the MS-SQL protocol. It also allows Application-Servers and Database-Servers to communicate with credit card processing systems via the HTTPS protocol. Any other communication would generate alerts.

VPN—ALL SEGMENTS: ESTABLISH TRUSTED CHANNELS

While a POS system typically encrypts sensitive credit card data, it is possible that other management plane traffic transmits in the clear or through insecure methods. Management plane traffic can include passwords, configurations and other critical confidential data. It is highly recommended to establish a trusted VPN channel from the atomic POS segment located in the retail stores to the Data Center servers. This will guarantee confidentiality of all data in transit. By establishing secure communication channels between the retail POS segments and the required backend support architecture, all POS traffic becomes critical. This also makes all communication immune from other inter-segment interactions. The example in Figure 3 shows an architecture employing a trusted channel.

EXAMPLE TRUSTED CHANNEL TOPOLOGY

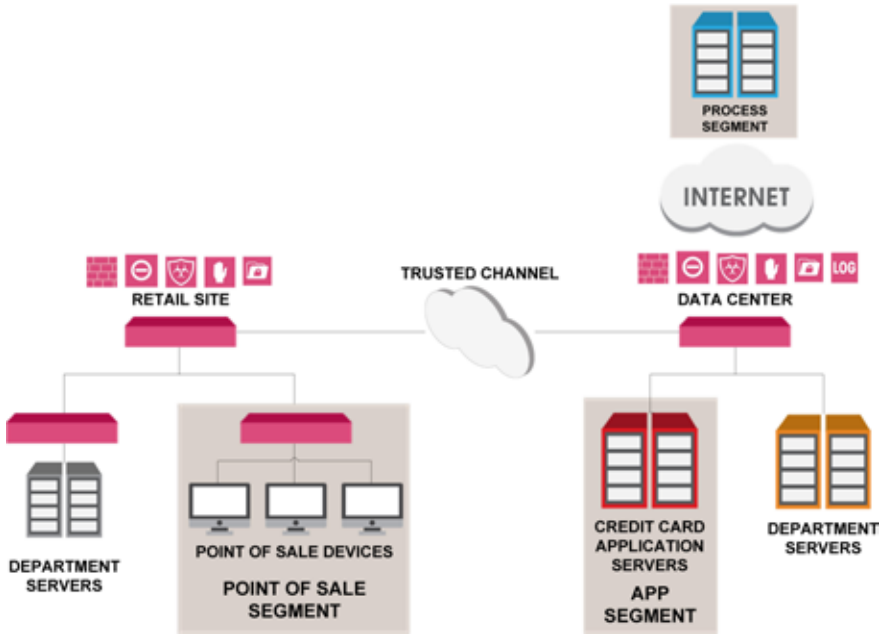


Figure 3 - Point of Sale Security Topology

PROTECTIONS ON THE TERMINAL

The characteristics of the POS terminal present significant security challenges. Primary among these is the age of the operating systems that run on the terminals. This issue is consistent for in-store devices, kiosks and even automated teller machines (ATMs).

In many cases, terminals use old versions of embedded Windows, including Windows XP. Microsoft announced the end of support schedule for XP back in 2007.[8] The end of support date occurred on April 8, 2014. The continued use of such platforms carries with it a range of risks including:

1. A range of vulnerabilities for attackers to exploit—Microsoft has significantly improved the security of newer versions of Windows, but older versions remain problematic
2. A lack of available security tools—many security vendors stopped supporting old Microsoft platforms, or at least they issue fewer protections for old platforms than for newer systems
3. Increased costs—support contracts for end of life platforms are often more expensive than equivalents for current releases and versions

To mitigate these challenges, retail companies should implement protections on the terminal. These should include best practice steps, like:

- Ensuring that terminals do not share the same administrator password
- Limited administrative privileges for the terminal's user account
- Stringent operating system hardening and deletion of unnecessary applications and tools
- Integrity checks to identify and prevent changes to terminal configurations and files stored on the systems

[8] "Banks to be hit with Microsoft costs for running outdated ATMs," http://www.reuters.com/article/2014/03/14/us-banks-atms-idUSBREA2D13D20140314.

Companies should also consider installing enterprise endpoint security suites on terminals and enabling regular updates of security functions. Enabling features such as application control, firewall and anti-malware would go a long way towards preventing the types of security breaches that occurred in 2013. Additional functions, such as port protection and full disk encryption are also relevant and would help address physical attack methods.

Figure 4 shows a screen shot of these protections in the Check Point Endpoint solution:

Figure 4 - Endpoint Protections

CONTROL LAYER: SAMPLE SETTINGS

The Control Layer is the brain of the SDP Architecture. Its role is to generate software defined protections and to deploy them for operation at the appropriate enforcement points, whether implemented using dedicated hardware or as host-based software.

Software-defined Protections provide the flexibility needed to cope with new and dynamic threats and changing enterprise network configurations. The Enforcement Layer provides a robust platform that can execute protections at enforcement points throughout the enterprise. Protections controlled by software means the underlying hardware deployed at these enforcement points should not require replacement when countering a new threat or attack method. The software can also be easily adapted independent of the hardware. Introducing new technologies into the organization becomes more transparent as the software can adapt to changes in hardware architecture. Protections can automatically adapt to the threat landscape without requiring manual follow-up or review of thousands of advisories and recommendations.

IDENTITY AWARENESS—ALL SEGMENTS: DESIGNATED ADMINISTRATIVE MACHINES AND ACCOUNTS

Scaled environments implement a controlled authentication system such Microsoft Active Directory, which provides centralized services to the entire organization. Active Directory provides robust authentication and logging mechanisms that in turn become the basis for additional enforcement layers. Best practices in security recommend integration of a firewall that segments a network and Active Directory. This approach will authenticate users and detect anomalous activity such as one or multiple Administrative logins from non-designated administrative machines. This approach quickly detects and contains activity within the segment.

For example, most POS networks include statically-assigned service account passwords used for maintenance and configuration changes. The use of these accounts is highly restricted to certain individuals and purposes such as maintenance, reconfiguration or other routine tasks. Firewalls performing segmentation can ensure the use of these accounts originate from designated administrative machines within the Data Center environment. The same authentication function can also limit the reach of the designated administrative machines.

The Identity Awareness access rule shown in Figures 5 and 6 specifies that only designated point of sale administrative service users physically residing on specific machines within a specific subnet will have the ability to access POS machines.

EXAMPLE IDENTITY AWARENESS POLICY

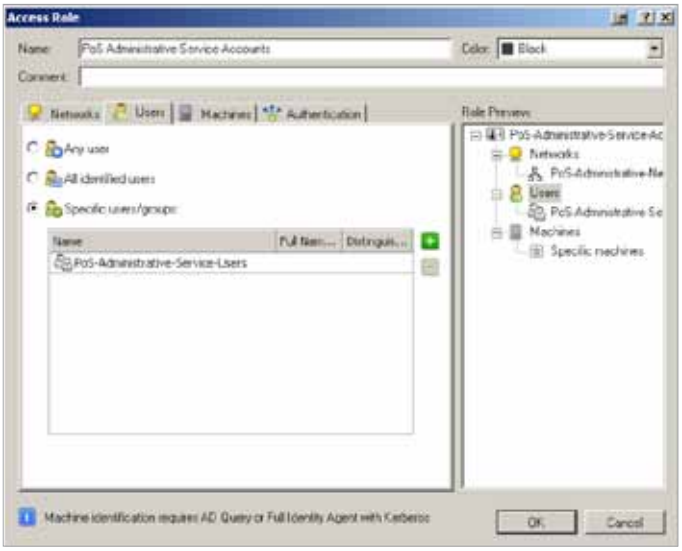


Figure 5 - Access Rule Configuration

By restricting access to only designated and audited individuals, any attempts to circumvent this policy would result in immediate alerts and detailed logs of the attempt.

Additionally, the use of unauthenticated access roles can provide an additional layer of protection from attackers physically attempting to connect to the infrastructure from trusted point of sale segment.

Figure 6 - User Controls in Point of Sale Application Rules

APPLICATION CONTROL/URL FILTERING—ALL SEGMENTS: PREVENT APPLICATION MASQUERADING

The Application Control and URL Filtering policy implements strict use of only defined applications and protocols over specified ports allowed within the firewall policy. This action also blocks all other known and unknown traffic.

EXAMPLE APPLICATION CONTROL AND URL FILTERING POLICY:

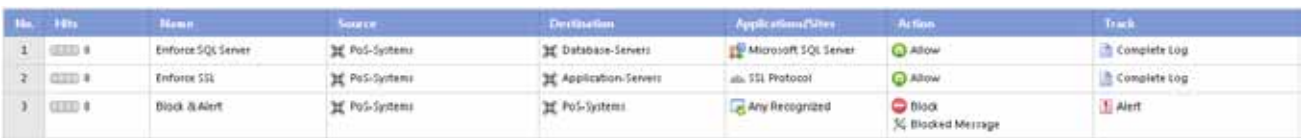


Figure 7 - Point of Sale Application Rule-base

Attackers leverage well-known open ports with alternate protocols to obfuscate malicious actions. As an example, attackers routinely leverage port 80 (HTTP) and port 443 (SSL) for alternate data flows as a way to circumvent policy.

The example in Figure 7 shows how an Application Control policy can be established that limits POS system communication with both the database and application servers. In this example, only those within the strict protocol standards established first within the firewall policy can control the application. Additionally, logging this traffic in detail creates a consistent and auditable information trail for forensic purposes.

SSL INSPECTION—ALL SEGMENTS: INSPECT AND DROP ALL UNTRUSTED OR REVOKED CERTIFICATES

POS systems sometimes use the Secure Socket Layer (SSL) protocol for transmitting credit card authorization and charge data to a credit card processing agency. Malware has evolved to leverage the SSL protocol to encrypt and obfuscate communication channels between compromised machines and command and control (C&C) systems.

Implementing SSL inspection on the gateway enables multiple layers of control, including verification of trust certificates, revoking trust of rogue certificates, and full inspection of SSL traffic. Addition of this control layer dramatically limits the option of attackers obfuscating their malware traffic or exfiltrating rogue data. Attempts to access resources with unsigned and/or revoked certificates would result in immediately triggered automated alerts and automated isolation from the network.

EXAMPLE SSL INSPECTION POLICY:

The foundation of the SSL trust-model is mutual and shared trust cascading from a top-level certificate authority down to individual endpoints and clients. This shared inherent trust certificate authority has also become a prime target for attackers. There exist many examples where attackers have successfully breached very large and well-known institutions by duplicating valid certificates. Once an attacker possesses trust certificate authority, full interception and decryption of the “secured” data payloads is possible.

Figure 8 - Point of Sale SSL Inspection Rule

Figure 8 example shows one method of how to establish SSL Inspection rules for the primary communication path between the physical POS systems and the defined application servers. Possible attacks are prevented by clearly defining the encrypted data flow between segments enabling detection of anomalous behavior.

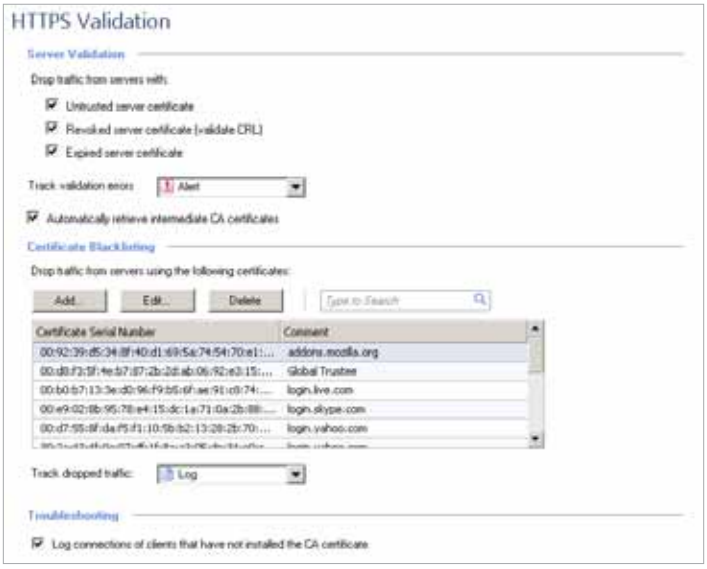


Figure 9 - HTTPS Validation Interface

In the example in Figure 9, validation policy ensures that only trusted certificate authorities, controlled at the network level, can pass through the data path to the necessary segments. In the event of a certificate authority breach, an administrator can revoke the certificate at the network level and revoke trust across the entire network infrastructure.

DLP—DATA CENTER SEGMENT: PREVENT CREDIT CARD DATA EXFILTRATION

The DLP policy should define and enforce the flow of credit card and other critical data to the expected destination. This approach prevents any attempts to transfer password protected, obfuscated or otherwise encrypted files. Any deviation will result in immediate automated alerts and automated isolation from the network.

	Data	Source	Destination	Exceptions	Action	Track		Install On	Time	Category
	None (2)									
	PCI - Credit Card Track 2	PoS-Systems	CC-Payment-Verification-System	None	Detect	Log		DLP Blades	Any	None
	PCI - Card Security Code PCI - Cardholder Data PCI - Credit Card Numb... PCI - Credit Card Track 1 PCI - Credit Card Track 2 PCI - Credit Card Track 3 PCI - Encrypted PIN Block PCI - Expiration Date PCI - PIN Block Data PCI - Sensitive Authent... PCI - Unencrypted PIN ... Credit Card Numbers o... Credit Card Numbers o...	PoS-Systems	Any	None	Prevent	Alert		DLP Blades	Any	None

Figure 10 - Point of Sale Data Loss Prevention Rule

In the example shown in Figure 10, DLP policy allows and logs credit card track 2 data from the POS-Systems network segment to a payment verification system. The same rule also prevents and alerts on credit card data passing to any other destination.

THREAT PREVENTION: PROTECT MODE

Threat prevention blocks attackers and denies exploitation of vulnerabilities and delivery of malicious payloads. The threat prevention policy is simple: “All threats should be prevented.” This policy is generic and overarching. Applying it across all organizations protects the entire network.

There are two basic groupings of threat prevention protections: pre-infection and post infection. Pre-infection protections provide proactive detection and prevention of threats that attempt to exploit vulnerabilities in internal applications and protocols. They also protect against attempts to deny service to authorized applications. Post-infection protections provide agile defenses that detect, contain and disarm threats after they have successfully subverted one or more network entities. These protections curtail the spread of malware and block bot connections to C&C servers.

IPS—ALL SEGMENTS: PREVENT KNOWN ATTACK VECTORS

Intrusion Prevention Systems (IPS) are effective pre-infection protections. A deep understanding of the segmented point of sale network and the underlying architecture are critical when designing an IPS policy to protect each segment.

IPS policies and profiles should reflect the overall architecture including patch level and security posture of the POS systems. Once a known attack pattern is recognized, the IPS should immediately trigger automated alerts and automated isolation from the network.

For example, a policy focused on Windows XP protections would be ideal for a segment running legacy Microsoft point of sale terminals. Likewise, if the segment contains other resources, such as printers, enabling protections for these specific devices is also necessary.

ANTI-BOT, ANTI-VIRUS AND THREAT EMULATION: MOVING FROM MONITOR TO FULL PREVENTION

Anti-Virus and Threat Emulation also address pre-infection issues. Anti-Bot focuses on post-infection.

The three protections provide comprehensive defense, updated in real-time against advanced known and unknown threats. Early stages of an attack require the attacker to deliver and execute binaries on the target platforms in order to establish connections to C&C systems and to begin data collection.

Bidirectional inspection of traffic flows originating from the POS segments and the Data Center builds a multi-layered defense system that employs real-time prevention coupled with real-time intelligence.

- Integrated Anti-Malware protections enable the security gateway to inspect and block known threats.
- Threat Emulation, which leverages sandboxing emulation environments, can identify new variants of malware.
- Anti-Bot looks for known patterns and information datasets that indicate botnet activity.
- Intelligence is fundamental to the effectiveness of these types of protections.

The Check Point ThreatWiki is the repository of Check Point intelligence for threat data. The image in Figure 11 shows a search result in the ThreatWiki for a banking Trojan called Eurograbber, classified as a Zitmo malware family member. The lower right panel shows that the risk is High and that the protection against Eurograbber was added to the Check Point Anti-Bot & Anti-Virus product via ThreatCloud on October 28th 2012.

The Check Point ThreatWiki is an easy to use tool that allows searching and filtering of Check Point's Malware Database. The URL is publically available for searching at http://threatwiki.checkpoint.com.

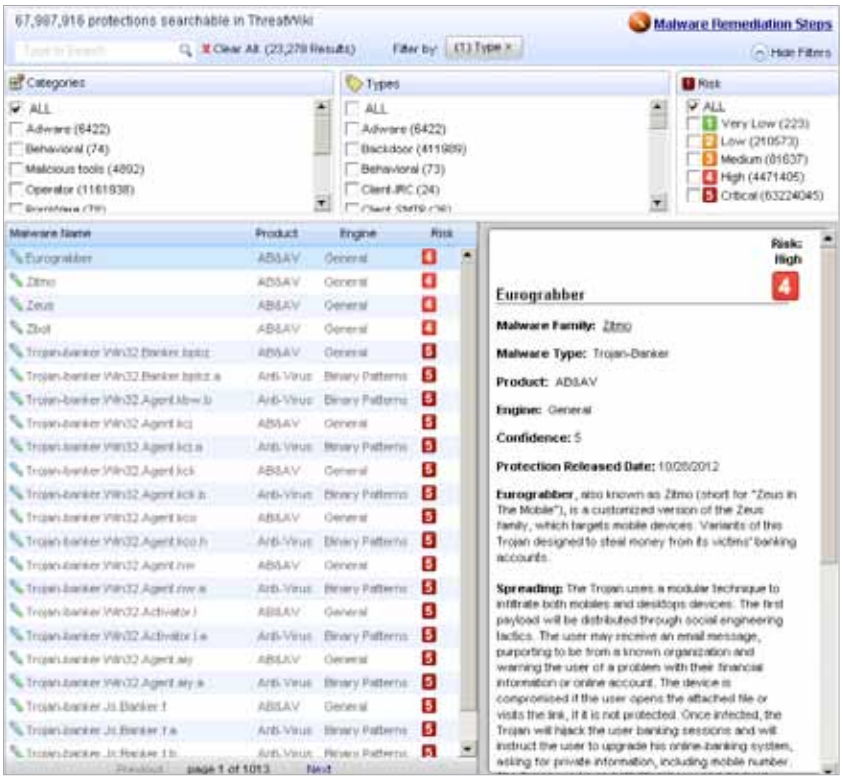


Figure 11 - ThreatWiki Interface

MANAGEMENT LAYER:
VISIBILITY COUPLED WITH AUDIT AND ALERT

Correlating seemingly disparate logs and alerts can cause significant delays and challenges in identifying and quarantining an attack. Check Point SmartEvent performs big data analysis and real-time security event correlation. It offers the ability to provide a consolidated and correlated view of an incident based on multiple sources of information. SmartEvent's accurate event view, shown in Figure 12, helps incident responders quickly identify the necessary actions needed to defend the network.

ThreatCloud distributes threat indicators derived from security event analysis enabling customers to prevent attacks from the latest threats. Automated response mechanisms can provide threat containment, allowing responders to take necessary actions before resuming operations.

Figure 12 - SmartEvent Interface

The above image shows the "Overview" screen of the SmartEvent solution. From there, administrators and auditors can dive deeper into specific events to analyze specific incidents and plot remediation courses.

The example in Figure 13 shows the summary view for a DLP incident:

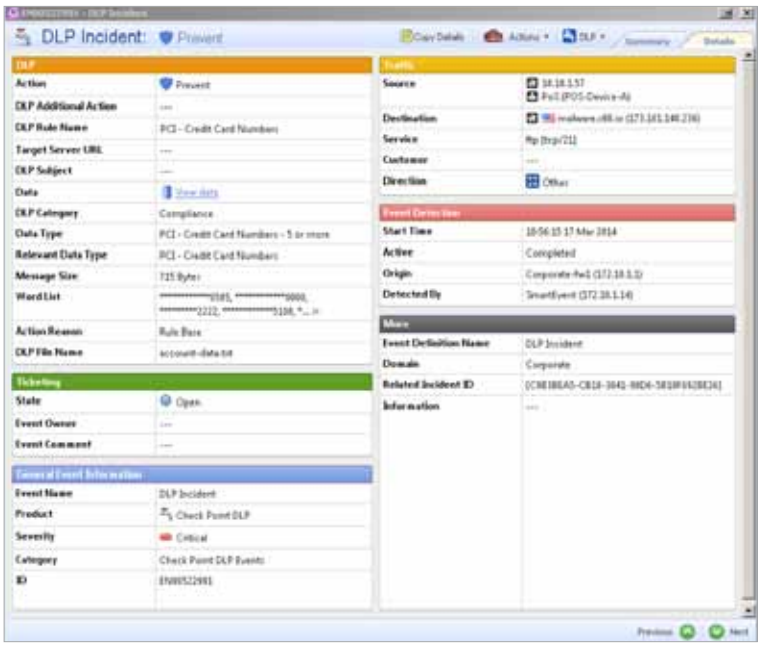


Figure 13 - DLP Incident Event View

It shows that IP address 10.10.1.57, corresponding to a POS system, is sending more than five credit card numbers in a text file called, “account-data.txt,” to an external domain named malware.x90.io, with an IP address of 173.161.140.236.

The same SmartEvent platform aggregates logs from multiple protections so that administrators can build a kill-chain view of the event in question. SmartEvent helps answer a range of questions associated with the event including:

1. Did the point of sales system attempt to send the information on its own?
2. Has it been in touch with suspicious external sources?
3. Is the attempt part of a broader campaign?

By correlating events associated with the same POS system at IP address 10.10.1.57, the administrator is able to gather more intelligence to answer these questions. The event log shown in Figure 14 shows the relevant answers:

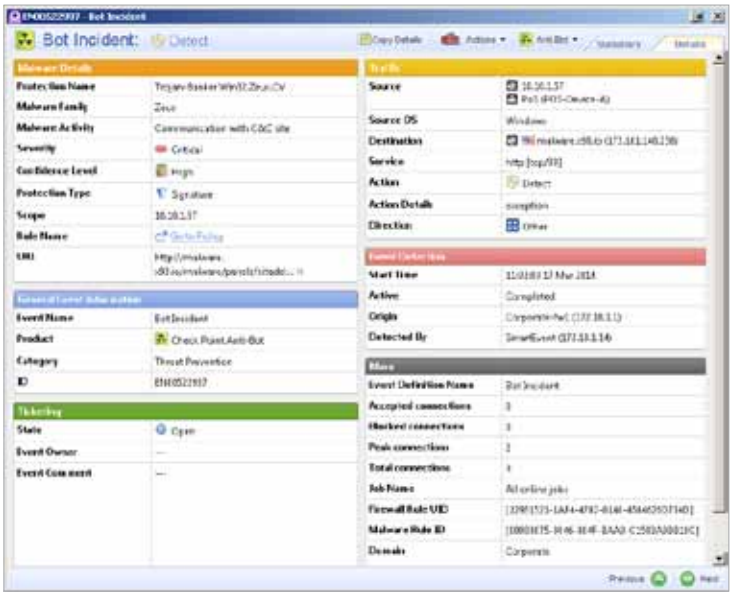


Figure 14 - BOT Incident Log

In this second event record, the administrator sees that the same POS system triggered an Anti-Bot rule for the Zeus botnet. By looking at the event details, we gain the following information:

1. Did the point of sales system attempt to send the information on its own?
   ANSWER: No. The point of sales system was infected with a Zeus variant that was attempting to exfiltrate the credit card data.
2. Has it been in touch with suspicious external sources?
   ANSWER: Yes. It was attempting to communicate with a known malicious C&C server.
3. Is the attempt part of a broader campaign?
   ANSWER: Yes. The DLP incident is part of a financial fraud botnet.

With this information in hand, a retail company's security administrators can pursue a range of mitigation and remediation steps, many of which were already initiated due to the "Prevent" status of the DLP and Anti-Bot rules.

THREATCLOUD SERVICES AND INTELLIGENCE

Check Point's ThreatCloud infrastructure provides real-time classification and identification of known and unknown threat vectors. Through the use of dynamic updates, real-time threat intelligence and automated analyses of unknown threats, ThreatCloud based services provide a deep technical understanding as well as contextual intelligence surrounding known actors, motives and behavioral patterns.

Through sharing of intelligence information in real-time between independent corporate entities, near real-time identification, correlation and containment of threats is a reality. Check Point ThreatCloud contains constantly updated hashes that identify and block the malware used in the retail breaches. New malware samples are regularly investigated and intelligence is constantly added.

SUMMARIZING THE SOLUTION

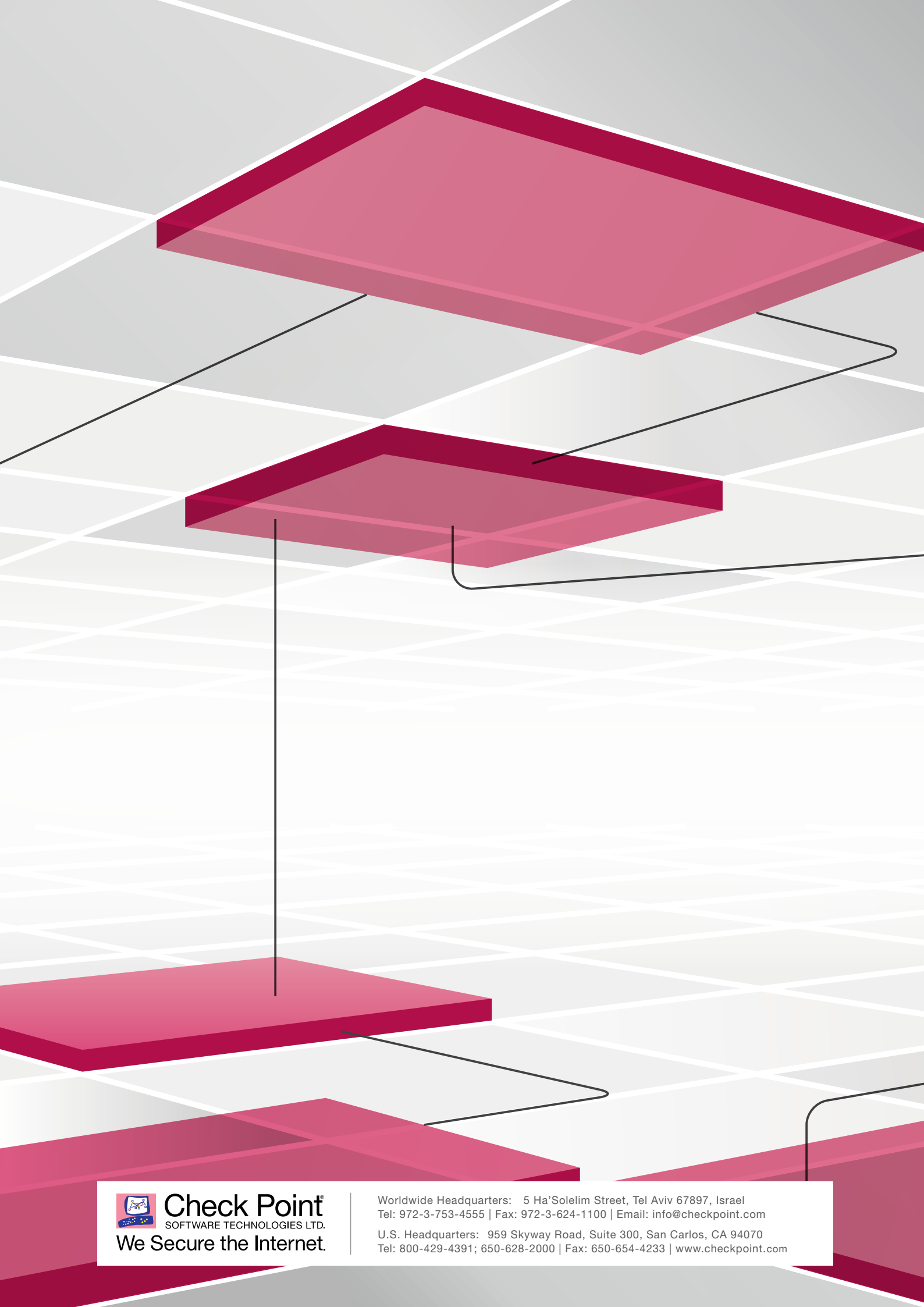
In order to protect against fast-evolving attacks, companies must adopt a POS architecture capable of handling fast growing network traffic and rapid expansion. Organizations must also implement security architectures that are dynamic and up-to-date with real-time protections.

The Software-defined Protection architecture suggests a three-layer security approach that includes the following elements:

1. The Enforcement Layer: Gateway and Endpoint-based protections that:
   - Segment POS systems from other network connected machines and ensure customer payment data only flow to required areas of the network
   - Scan, identify and block malware, botnets and weaponized content designed to infect machines, collect and exfiltrate customer information
   - Bind network and application access to authentication rules to prohibit unauthorized users and systems from accessing sensitive areas of the network
   - Restrict applications and system behavior according to least privilege guidelines
   - Secure data at rest and in transit and proactively block exfiltration attempts
2. The Control Layer: Administrator-determined security policies and automated protections
   - Create rules that specifically define access control and data security policies with enforcement points
   - Implement intelligence-based threat prevention that updates independently and proactively distributes new protections to enforcement points
3. The Management Layer: Business-aligned administrator privilege and comprehensive reporting
   - Segment management profiles and bind administrator access only to systems over which the business determines they should have control
   - Implement event management, logging and reporting tools that identify events in real-time and include filtering and analysis tools to ensure administrators have visibility into attacks without getting lost in less critical “noise”

The interaction between these three layers provides a modular and manageable security program architecture that can help address today and tomorrow’s security challenges. SDP is relevant for all companies in all industries. As this guide illustrates, SDP can also serve as a method for implementing effective security in retail environments.

For more information on Check Point’s SDP, please visit: https://www.checkpoint.com/sdp/, or contact your Check Point account team.



Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Worldwide Headquarters: 5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters: 959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com