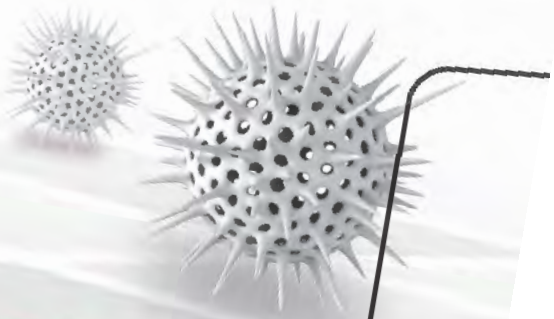
ATM SECURITY SOLUTION BRIEF



Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Since their invention in the late 1960s, Automatic Teller Machines (ATMs) have revolutionized the banking industry. They have made it possible for consumers to access their accounts, withdraw cash, deposit and transfer funds, and conduct a range of transactions from outside the branch. Today's bank transaction devices have evolved into full-service banking kiosks with features even for non-banking applications.

The networking technologies leveraged to create ATMs have also evolved over time. ATMs initially used modems connected with Plain Old Telephone System (POTS) lines eventually migrating over time to private leased lines, ISDN, Ethernet and WiFi. The first ATM with a 4G LTE connection was introduced in 2012.

To authorize transactions and transfer funds electronically, the ATM device must communicate with its Host Processor Network. The Host Processor Network in turn communicates with the card issuing institution.

Many ATM device manufacturers offer multi-site management convenience features such as remote access for resetting their terminals or checking the level of the cash cartridges. At least one attack has leveraged an authentication flaw in the remote access protocol to allow remote attackers full access to the ATM.

As the technology and network access around ATMs has evolved, so also has criminal interest. Since the start of 2012, there have been marked increases in malware targeted for ATM devices with a major spike in activity over the first half of 2014.

Within the security community, it is understood that most ATM systems are built on top of architectures that are not secure at their foundation. Like many other technologies, security has been a low-priority afterthought when it comes to ATMs.

While individual attack approaches may vary wildly, attack vectors against ATMs fall into three main categories:

1. Remote exploits against the operating system or application
2. Remote attacks against the backend processing networks
3. Physical ATM device tampering

An effective security strategy is to take a broad view of incident tactics and implement a multi-layered approach that addresses the individual attack methods across the wider risk environment.

This document takes a broader view of ATM security, following the guidelines outlined in the industry standard PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI) ATM Security Guidelines Information Supplement. The document analyzes ATM security vulnerabilities using the Check Point Software-defined Protection (SDP) Architecture framework:

- **Enforcement Layer:** SDP begins with a simple to follow pathway toward effective and manageable network segmentation. This method leads to a practical way of implementing and locating enforcement technologies across network resources.
- **Control Layer:** The next layer of SDP defines the way administrators can distribute network flow controls safely via security policy and threat prevention technologies.
- **Management Layer:** The last layer of SDP describes how controls and threat prevention technologies can be organized, monitored and managed.

The chapter titles of this document use SDP layers as an organizational guideline. Each section provides more details along with specific recommendations.

This is a multi-level document divided by topic. Individual document sections are sufficient as stand-alone topic descriptions for specific departments. The document as a whole provides a more complete picture of an entire solution.

The areas covered in the pages that follow are:

- An analysis of recent security events and vulnerabilities in the ATM device space
- A summary of primary ATM security guidelines and regulations
- ATM network security design principles
- The ATM network enforcement layer
- Control layer considerations
- Management layers guidelines

Some diagrams and screenshots have been included in the document to help better visualize the controls, policies, enforcement points and network segmentation discussion.

SUMMARY OF RECENT SECURITY EVENTS AND VULNERABILITIES IN THE ATM DEVICE SPACE

Automatic Teller Machines (ATMs) definitely make our lives easier when it comes to banking tasks. We can withdraw, deposit checks and now even deposit cash into our bank accounts after business hours and on weekends. ATMs also make it much easier for criminals to steal money. To accomplish this, attackers must gain access to the network either by stealing customer access information or exploiting vulnerabilities in the ATM network.

The method known as 'card skimming' is a common way to steal ATM user card information. Card skimmers have often been physical devices but software (malware) skimmers are becoming more prevalent.

Physical card skimmers are devices that criminals install over the ATM card insert slot. They read and capture card information for later exfiltration. Physical skimmers can be hard to identify because the good ones appear as if they are part of the manufacturer's design. Skimmers accompanied by small digital video cameras or Personal Identification Number (PIN) pad overlays positioned properly can capture both card data and user PIN information. A camera built into overlays or hidden in a façade can appear to be part of the manufacturer's design making them difficult to identify. The card data and the PIN code capture are usually stored inside the skimming devices' own internal memory. Later, the criminal can retrieve the skimming devices and access the data in private.

The latest and most interesting criminal development in skimming was the multi-million dollar fraud ring that somehow installed Bluetooth enabled skimmers inside certain gas pumps in the southeast United States. The criminals were able to retrieve captured card data via Bluetooth by simply driving up and getting a tank of gas in broad daylight.

Skimming will become more of a problem in the future, as 3D printer blueprints for skimming device facades are now readily available. Additionally, the cost of 3D printing is declining rapidly making this option more accessible.

Skimming digitally with malware is also possible. Similar to the skimming malware used in recent retail attacks on Point of Sale (POS) terminals, malware skimmers take over function calls inside the ATM software to capture card and PIN code data. This type of malware will typically store captured data locally to be either physically retrieved by the criminals or exfiltrated over the ATM network connection via remote command.

An attack technique known as Ram-Raids has also been demonstrated effective. In a Ram-Raid, a large vehicle drives right into a storefront and the attackers physically take the ATM off-premises. This allows the criminals to take their time when cracking the safe offsite. In these cases, the attackers often use explosives to force open the safe and access the cash it protects. In the instance when and ATM cassette is tampered with or opened without a proper key, many ATM cash cassettes are equipped with an Intelligent Banknote Neutralization System (IBNS) that activates upon tamper detection. The most common form of IBNS is cash degradation via ink staining.

While stealing the information from one ATM machine may yield a few hundred thousand dollars, organized crime rings have masterminded heists totaling $9 to $45 Million USD. These larger heists have involved a chain of infractions:

- Stealing magnetic stripe data
- Creating counterfeit cards with the stolen magnetic stripe data (AKA: Carding)
- Hacking ATM authorization backend processing networks to increase the daily withdraw limit for the counterfeit cards
- Employing gang members (AKA: Cash Mules) to withdraw high amounts of cash at various locations around the globe

A review of underground forums and forensic analysis found that malware-based ATM attacks have increased exponentially in the last few years. The following is a high-level description of several of the most popular approaches:

- **Dillinger**—Remote network attack tool that exploits an authentication flaw to perform a number of functions such as: retrieve settings, retrieve magnetic stripe data, retrieve and replace camera images, retrieve master password, upload malware, and empty cash cassette (AKA: Jackpotting).
- **Scrooge**—Malware that is activated via a special key sequence or a custom ATM card with hooks that capture ATM card data and PIN code entries with built in remote command parser.
- **Ploutus**—Embedding a burner cell-phone behind a fake façade panel inside the ATM. This combination allows criminals to dispense cash from the ATM via SMS messages.
- **Tyupkin (AKA: Backdoor.Padpin)**—Malware activated via a secret key sequence on the PIN pad. Commands include: display available cash, dispense cash from a given cassette, dispense all cash, disable networking, and malware self-destruct.
- **Trojan.Skimer.19**—Activated via a custom ATM card this malware can dispense cash, collect card data, or reboot the ATM.

ATM system documentation is readily available to anyone willing to look for it. This makes it easy for anyone to understand how to operate these machines. An international news story broke in July of 2014 when two teenagers from Canada obtained the manual for a well-known ATM manufacturer. They were able to access the administrative features of the system using default credentials. The teens did not steal anything and followed responsible disclosure practices by informing the bank of the need to update their ATM passwords.

PCI AND ATM

The PCI Security Standards Counsel recognizes the lines are blurring between retail Point of Sale (POS) devices, unattended payment kiosks, and ATM devices. Use of ATM cards with a PIN entry is becoming commonplace to buy retail goods at POS terminals and most ATMs accept credit cards.

Groups called ATM interbank networks also known as ATM consortiums, allow member institutions to issue global cards. These cards are usable at any network-supported ATM around the world. MasterCard Worldwide Cirrus and VISA Plus interbank networks mandate compliance with Payment Card Industry standards for Data Security (PCI-DSS), Payment Application Data Security Standard (PCI PA-DSS), PCI PIN Security Requirements and PCI PIN Pad (EPP) Security Requirements.

Many of the aforementioned PCI standards apply to ATM machines as well as POS terminals. They include guidelines for Electronic PIN Pad encryption to protect PIN code entries. They also have guidelines for securing track data stored in a traditional card's magnetic stripe or on a smartcard's microchip.

As evident in the name, the *PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI)—Information Supplement: ATM Security Guidelines* contains recommendations mostly specific to ATMs.

ATM NETWORK SECURITY DESIGN PRINCIPLES

Properly designed network security architectures would thwart the remote attacks outlined above.

#1: ENFORCE SEGMENTATION TO PREVENT REMOTE ACCESS

The basic fact that the attackers can remotely access ATM devices via an IP address implies that there are insufficient controls to limit network access.

The PCI PTS ATM Security Guidelines Information Supplement specifies:

> *The communication interface(s) of the ATM should not accept connection requests from unauthorized sources.*[1]

The most effective way to address this issue is to implement tight segmentation of the ATM network. PCI-DSS v3 specifically outlines the principle of segmentation. 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.*[2]

[1] PCI Security Standards Council, LLC, PCI PTS ATM Security Guidelines Information Supplement
[2] PCI Security Standards Council, LLC, Payment Card Industry (PCI) Data Security Standard v3.0 (2013), 11.

While the PCI-DSS v3 does not require segmentation, the standard strongly recommends it. It notes that it can reduce risk, scope and cost of the PCI assessment. Considering the cost of recent events, segmentation should be thought of as a fundamental security requirement and not just a recommendation. The diagram in Figure 1 visualizes methods for separating ATM networks into different component elements.

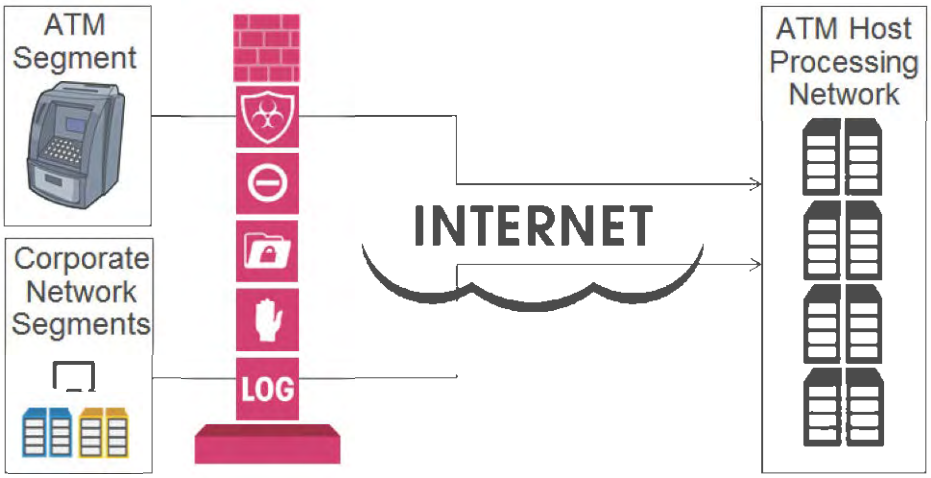


Figure 1 - Sample Segmentation Topology

The following hierarchical trust framework defines logical segments suitable for any ATM network architecture. Once clearly defined, the network architect should assign risk factor values to each network communication between segments. The basis of the risk value should be the level of critical information transmission, whether within the ATM management plane or backend Host Processing Networks.

The segmentation architecture is as follows:

- **ATM Segment:** Contains ATM devices
- **Application and Maintenance Segment:** Contains all supporting application and maintenance infrastructure.
- **Host Processing Segment:** Contains supporting database servers and associated administrative machines. The Host Processing Network (HPN) will be outside the scope of control for small to medium businesses deploying ATMs. However, knowing what IP addresses and protocols are required to access the HPN will allow for tighter controls and can limit data exfiltration from compromised ATMs.
- **Bank Processing Segment:** Typically third party relationships drive the bank-processing segment. This is not typically under the control of the ATM owner-operator. However, large banks may facilitate an entire ATM transaction from the initial card swipe at the ATM device through the Host Processing Network to the Bank Processing Segment.

THE PRIMARY PAYMENT CARD INDUSTRY (PCI) SECURITY REQUIREMENTS FOR ATM

Stakeholders in the financial industry formed the Payment Card Industry Security Standards Council in 2006. In an effort to provide a framework for gauging an individual business' security posture regarding the acceptance or handling of ATM and Credit Cards, this PCI Council established a set of standards called PCI Data Security Standards (PCI-DSS).

PCI-DSS has many regulations, directives and guidelines. PCI compliance has become an easy way for business and customers to recognize whether a place of business has met a baseline set of protection and security measures.

Section 4.2 of the PCI PTS ATM Security Guidelines discusses Security Objectives for Software and Network connectivity for ATM devices. These objectives include:

- Preventing Operating System and application exploitation,
- Reducing exposed attack surfaces,
- Preventing attacks from third-party supply-chains,
- Protecting against unauthorized modification or installation of software,
- Logging OS activity and,
- Using effective network isolation and intrusion detection/mitigation tools.

SECURE COMMUNICATIONS TO FURTHER ISOLATE ATMS

The owner-operator networks within which ATMs reside 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 place of business, between branch offices, stores, and 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 connection cannot be avoided, an additional effective protection is the encryption of sensitive data and transmissions. Implementing secure encrypted communications is an effective method to protect 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.

Securing communications between ATMs and supporting architecture protects card account 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

Without access controls and data security measures, a single ATM breach could invite attackers to move horizontally to other ATMs or computers within the owner-operator network. This additional access opens the door for an attacker to install new software, gain access to sensitive networks, and transfer files within and outside the network.

Achieving the levels of security needed to prevent the types of attacks outlined above requires more stringent access controls beyond just those for system access. Specifically:

- Limiting the types of applications accessible by employees and systems is a prudent security posture. Companies should develop access control rules that specify such limits.
- Administrators should create policies that restrict the flow of specific application traffic only to specific network segments that require such applications.
- Bind application usage to validated user identity checks by business function ensuring usage access is consistent with broader company guidelines.

ENDPOINT PROTECTION

A critical element of a network's security posture is the endpoint. Unmanaged endpoints are often blind spots for any security administration team and even more so when the endpoints are viewed as un-patchable always-on devices like ATMs. It is important to note that, behind the scenes, ATMs run full blown operating systems with complete network stacks and filesystems.

Check Point Endpoint Security products provide a valuable layer of protection and visibility with a rich set of features.

- **Full Disk Encryption**—When an ATM is stolen Full Disk Encryption will prevent criminals from reading data on the drive by providing automatic security for all information the hard drive, including user data, operating system files and temporary and erased files.
- **Media Encryption**—To prevent the installation of malware via insertion of rogue USB Flash drives or other media, Media Encryption provides centrally-enforceable encryption of removable storage media such as USB flash drives, backup hard drives, CDs and DVDs, for maximum data protection.
- **Anti-Malware & Program Control**—To prevent installation of malware via zero day vulnerabilities in ATM applications or protgrams that must run on the ATM device, Anti-Malware & Program Control efficiently detects and removes malware with a single scan. Viruses, spyware, keystroke loggers, Trojans and rootkits are identified using signatures, behavior blockers and heuristic analysis. Program control allows only approved programs to run the endpoint.
- **Firewall and Compliance Check**—If an ATM Device is compromised, exfiltration of data as well as command and control traffic can be prevented with host based firewalls. Firewall and Compliance Check protects endpoints by controlling inbound and outbound traffic and ensuring policy compliance, with centralized management from a single console. Definable zones and security levels protect endpoint systems from unauthorized access. Integrated stealth technology makes endpoints invisible to attackers.
- **Endpoint Remote Access VPN**—When an attacker controls another system in the environment, ATM communications can be rendered un-usable to criminals by securing the traffic with Endpoint Remote Access VPN. It provides secure, seamless access to trusted networks and resources. Privacy and integrity of information is ensured through, endpoint system compliance scanning and encryption of all transmitted data.

INTEGRATED DATA SECURITY

The PCI ATM Security Supplement refers to PCI-DSS v3 for data protection recommendations. Requirement three of this document is entitled, "Protect stored cardholder data." [3] This requirement includes a range of controls that protect card information and evaluate the effectiveness of enforcement measures. Included in this requirement are standards for storage, encryption and obfuscation, key management and recommendations for implementing 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." [4]

This more general guidance provides solid, best practice recommendations. All organizations should assess how data flows across their networks and should determine if segmentation rules allow unauthorized data flows.

In effort to stop data exfiltration, owner-operator networks should also implement data loss prevention (DLP) technologies as an integrated part of their security policies. Implementing systems that enforce data flow restrictions should not be only at the network level, but higher in the stack as well. Administrators should create rules that look specifically for data constructs that match ATM card data. They should also include policies that identify the types of methods that attackers use to exfiltrate data, such as large encrypted and compressed files, and block their attempted transfer across networks.

#3: LEVERAGE THREAT PREVENTION

As previously noted, the number of malware occurrences in ATM devices has risen sharply in the last three years. The best defense against this type of attack is for owner-operator companies to continuously update their anti-malware systems and to regularly monitor for activity that is consistent with malware behavior.

A review of malware occurrences also shows that ATM malware is evolving at an alarming rate. ATM manufacturers should not only have anti-virus and anti-malware software installed on their devices from the factory but should develop a plan to update their software regularly. Owner-operators of ATMs should also evaluate if they need to install anti-virus software on other types of systems connected to the ATM network.

#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 more routine maintenance warnings can be challenging at best. Attackers have become adept at disguising malware as routine tasks.

It can be very difficult for even the most sophisticated IT security teams to identify critical activity. Indeed, the lessons learned from prior incidents include a need to activate protections and not just monitoring technologies. 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. When event management and security management are visualized separately, security teams have 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 monitoring tools of security technologies. For example, Check Point SmartEvent is a security event monitoring tool which is tightly integrated with the Check Point Management Dashboard. This allows users to configure rules and policy directly from the security event monitor view.

[3] PCI-DSS v3, 34
[4] PCI-DSS v2, 11

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.

The next section includes many specific implementation examples. While each of the examples below come from actual implementations, they may or may not be appropriate for your company's configurations or rule-base needs.

NOTE: Before employing any specific security solution shown here, you should review your organization's specific business objectives, deployment architectures and risk profiles.

ENFORCEMENT LAYER: RECOMMENDED CONFIGURATION

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.

Such 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 HIERARCHICAL-TRUST POLICY

The ATM 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

In the firewall policy example shown in Figure 2, only the segmented ATM_Devices network can communicate with the Host Processing Network Application-Servers via the HTTPS protocol. Any other communication would generate alerts.

Allow ATM to Host Processing	ATM_Devices	Host_Processing_Network	TCP https	accept	Log
Drop and Alert	Any	Any	Any	drop	Alert

Figure 2 – ATM Device Relevant Firewall Rules

VPN—ALL SEGMENTS: ESTABLISH TRUSTED CHANNELS

While an ATM device typically encrypts sensitive card data, it is possible that other management plane traffic transmits in the clear or through insecure methods. Management plane traffic can include passwords, software updates, configurations and other critical confidential data. It is highly recommended to establish a trusted VPN channel from the atomic ATM segment located in the owner-operator network to the Host Processing Network servers. This will guarantee confidentiality of all data in transit. By establishing secure communication channels between the ATM segments and the required backend support architecture, all ATM traffic would be treated as critical. This also makes all communication immune to inter-segment interaction. An example of an architecture employing a trusted channel is shown in Figure 3.

EXAMPLE TRUSTED CHANNEL TOPOLOGY

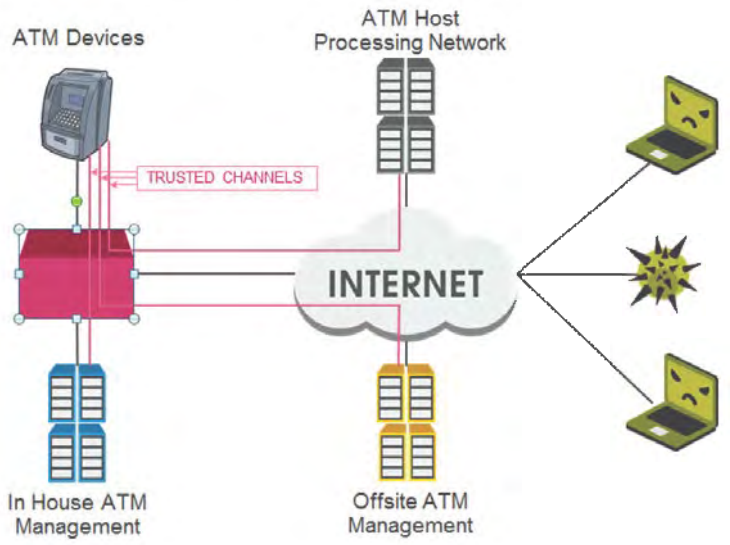


Figure 3 - POS Security Topology

PROTECTIONS ON THE ATM

The characteristics of the ATM terminal present significant security challenges. The age of the operating systems that run on the terminals can pose serious risk. This issue is consistent for in-store devices, kiosks and even POS devices.

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.[5] The end of support date occurred on April 8, 2014 and estimates indicate that on that date, 95% of the 210,000 U.S. ATM machines still utilize this operating system.[6] 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 remains problematic
2. A lack of available security tools—many security vendors stopped supporting old Microsoft platforms, or at least they don't issue new protections for old platforms at the same rate as they do for newer systems
3. Increased costs—support contracts for end of life platforms are often more expensive than equivalents for current releases and versions

[5] "Banks to be hit with Microsoft costs for running outdated ATMs," http://www.reuters.com/article/2014/03/14/us-banks-atms-idUSBREA2D13D20140314.
[6] "95% of bank ATMs face end of security support," http://money.cnn.com/2014/03/04/technology/security/atm-windows-xp/

To mitigate these challenges, ATM owner-operators 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
- Prevent the installation of trojan programs with an Anti-Malware solution
- Ensure criminals can not read stolen drives by installing Full Disk Encryption
- Limit network traffic to and from the device with network and host firewall
- Secure network traffic to and from the device with Remote Access VPN

Applying Operating System security updates and installing enterprise endpoint security suites on ATMs are steps that will result in hardening these devices. Depending on the ATM device operating system, properly configured anti-malware, application control and firewall software could prevent the attacks outlined above. Using port protection and full disk encryption on supported version of ATM Operating Systems can also thwart physical attacks. Additionally, employing the Check Point ATM Endpoint VPN client will encrypt all communications.

CONTROL LAYER: SAMPLE SETTINGS

The Control Layer is the core of the SDP Architecture. Its role is to generate software defined protections and to deploy them for execution at the appropriate Enforcement Layer enforcement points, whether implemented using dedicated hardware or as host-based software in the network. 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 does not need to be replaced when a new threat or attack method is discovered. 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 environment such as 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 recommends a combination of layered enforcement, firewall segmentation and Active Directory authentication. With this architecture, detecting and containing administrative logins from non-designated administrative machines becomes possible.

Most ATM devices include statically assigned service account passwords used for maintenance and configuration changes. The use of these accounts is highly restricted for 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 owner-operator or ATM provider environment.

For example, the Identity Awareness Access Role shown in Figure 4 and Figure 5 specifies that only designated ATM administrative service users physically residing on specific machines within a specific subnet will have the ability to administer ATM devices.

EXAMPLE IDENTITY AWARENESS POLICY

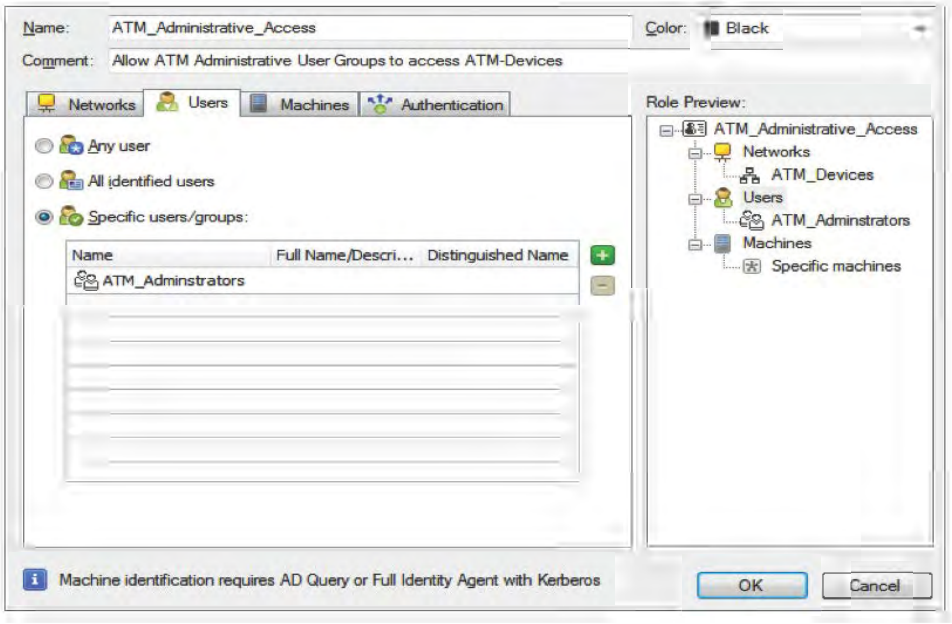


Figure 4 - User Access Rules

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 ATM segment.

Figure 5 - User Controls ATM Administration Rules

ATM Devices themselves can also be managed with Identity Awareness through the control of their VPN certificates.

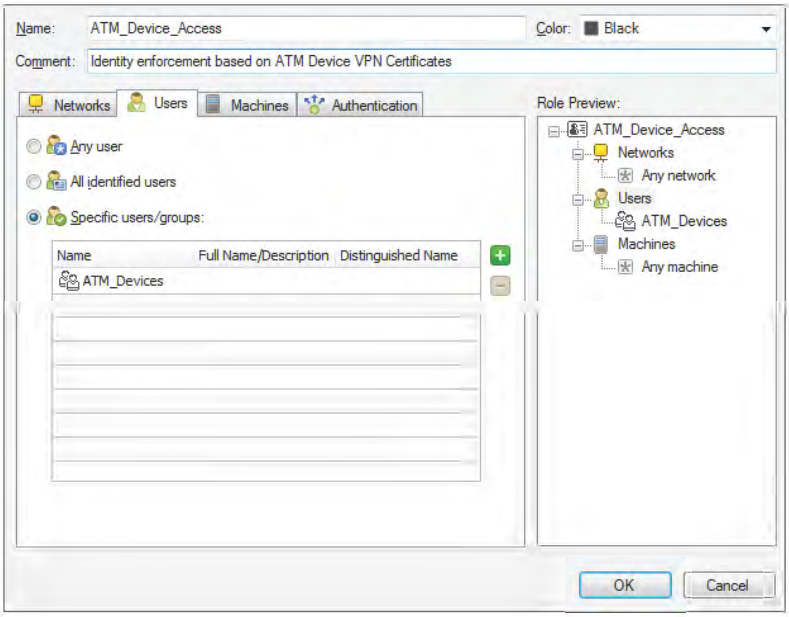


Figure 6 - Identity enforcement based on ATM Device VPN Certificates

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

The Application Control and URL Filtering policy implement 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:

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.

Allow RDP for Admin	ATM_Administrator_Network	ATM_Devices	Remote Desktop Protocol	Allow	Complete Log
Allow ATM HTTPS to Host Processing Network	ATM_Devices	Host_Processing_Network	SSL Protocol	Allow	Complete Log
Block & Alert	ATM_Devices	All_Internet	Any Recognized	Block	Alert

Figure 7 - ATM Application Rule-base

The example in Figure 7 shows how an Application Control policy can be established that limits ATM communication with Host Processing Network application servers. In this example, only those within the strict protocol standards established in 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

ATM systems sometimes utilize the Secure Socket Layer (SSL) protocol for transmitting card authorization data to a Host Processing Network. Malware has evolved to leverage the SSL protocol to encrypt and obfuscate communication channels between compromised systems and established 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 any 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 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 data payloads is possible.

Inspect SSL Traffic from ATMs	ATM_Devices	ATM_Administrator_Network Host_Processing_Network All_Internet	https	Inspect	Log
Inspect SSL Traffic to ATMs	All_Internet ATM_Administra... Host_Processing...	ATM_Devices	https	Inspect	Log

Figure 8 - ATM SSL Inspection Rule

The Figure 8 example shows one method of how to establish SSL Inspection rules for the primary communication path between the physical ATM systems and the defined networks for processing and administration. We now know, however, that malware C&C connections are capable of using SSL. As a result, we also need to inspect SSL to any other destination.

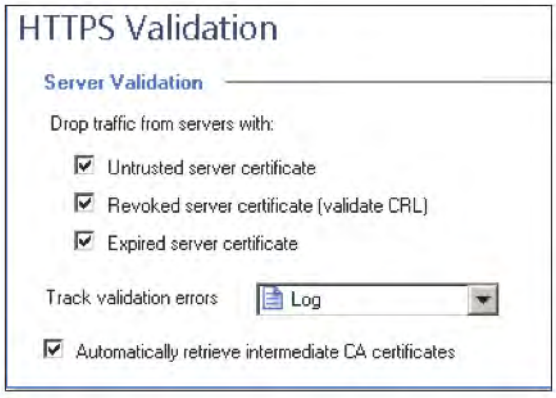


Figure 9 - HTTPS Validation Interface

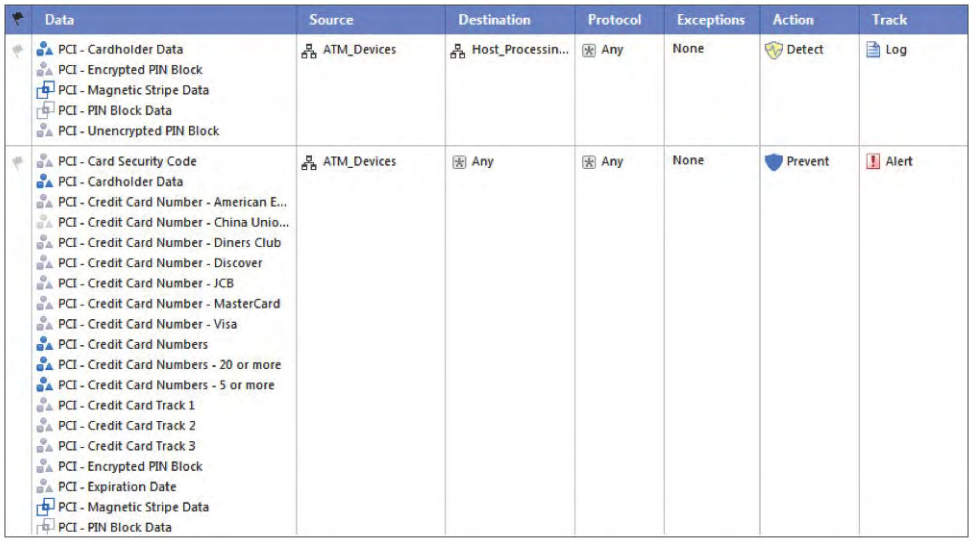
In the event of a policy or configuration error, inspecting SSL traffic to unknown destinations from critical assets can help prevent unwanted communication and can assist in Incident Response. Anomalous behavior can be identified and possible attacks prevented by clearly defining the encrypted data flow between segments.

In the example shown in Figure 9, validation policy ensures only trusted certificate authorities, controlled at the network level, 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 ATM 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.

In the example shown in Figure10, DLP policy allows and logs ATM card data from the ATM-Systems network segment to a Host Processing Network system while preventing and alerting data passing to any other destination.



Data	Source	Destination	Protocol	Exceptions	Action	Track
PCI - Cardholder Data PCI - Encrypted PIN Block PCI - Magnetic Stripe Data PCI - PIN Block Data PCI - Unencrypted PIN Block	ATM_Devices	Host_Processin...	Any	None	Detect	Log
PCI - Card Security Code PCI - Cardholder Data PCI - Credit Card Number - American E... PCI - Credit Card Number - China Unio... PCI - Credit Card Number - Diners Club PCI - Credit Card Number - Discover PCI - Credit Card Number - JCB PCI - Credit Card Number - MasterCard PCI - Credit Card Number - Visa PCI - Credit Card Numbers PCI - Credit Card Numbers - 20 or more PCI - Credit Card Numbers - 5 or more PCI - Credit Card Track 1 PCI - Credit Card Track 2 PCI - Credit Card Track 3 PCI - Encrypted PIN Block PCI - Expiration Date PCI - Magnetic Stripe Data PCI - PIN Block Data	ATM_Devices	Any	Any	None	Prevent	Alert

Figure 10 - ATM Data Loss Prevention Rule

THREAT PREVENTION: PROTECT MODE

Threat prevention protections block attackers and deny 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

A deep understanding of the segmented ATM network and the underlying architecture is critical when designing an Intrusion Prevention System (IPS) policy to protect each segment. IPS policies and profiles should reflect the overall architecture including patch level and security posture of the ATM 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 ATM 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

The Anti-Bot, Anti-Virus and Threat Emulation Blades provide comprehensive protection, 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 C&C and begin data collection.

By leveraging sandboxed emulation environments along with known patterns and information datasets collected from Check Point and other industry sources, the Security Gateway can inspect and block both known and unknown threats even to the furthest segment. Bidirectional inspection of traffic flows originating from the ATM segments and the Host Processing Network builds a multi-layered defense system that employs real-time prevention coupled with real-time intelligence. Any recognized malware behavior immediately triggers automated alerts and automated isolation from the network.

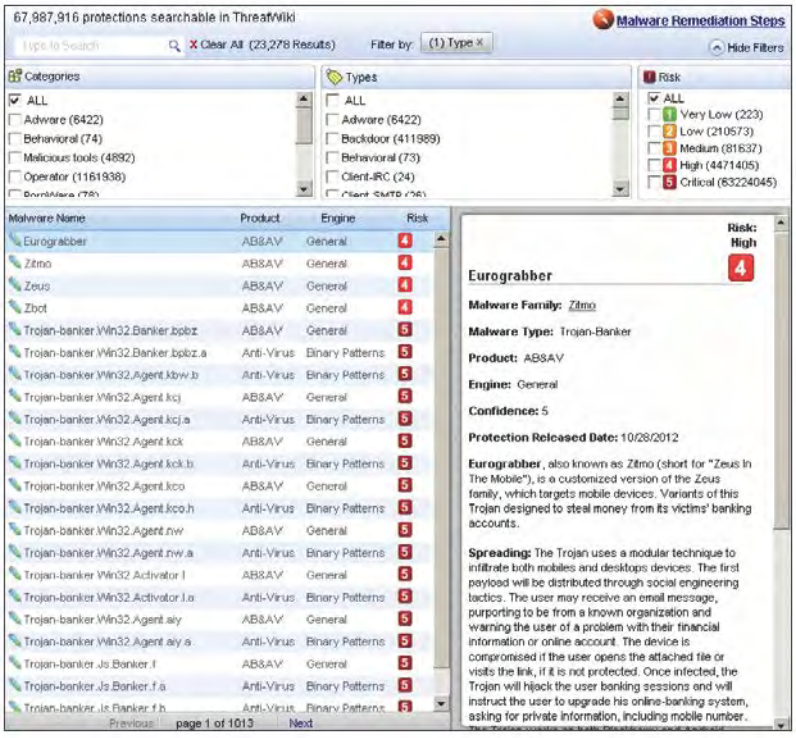


Figure 11 - ThreatWiki Interface

The image in Figure 11 shows a snapshot from the Check Point Threat Wiki. The results shown are for a banking Trojan called Eurograbber classified as a Zitmo malware family member. The lower right panel shows the risk as 'High' and that the protection against Eurograbber was added to the Check Point Anti-Bot and 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 Check Point Threat Wiki URL is publically available for searching at http://threatwiki.checkpoint.com.

MANAGEMENT LAYER: VISIBILITY COUPLED WITH AUDIT AND ALERT

A recent retail breach event documented approximately 60,000 suspicious activity alerts during and after the event. Security visibility leveraging management tools such as SmartEvent is an integral part of a resilient security posture. The Management Layer provides both comprehensive situational awareness as well as incident response capability.

EVENT MANAGEMENT AND MONITORING

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, a sample of which is 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

THREATCLOUD SERVICES AND INTELLIGENCE

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

Check Point's ThreatCloud extends this intelligence infrastructure to provide proactive alerting and monitoring for incidents, behaviors and trends specific to the retail and hospitality industry. ThreatCloud continuously collects intelligence information in real-time from independent corporate entities enabling identification, correlation and containment of threats in near real-time. Check Point ThreatCloud contains constantly updated hashes that identify and block most of the malware used in ATM attacks. ThreatCloud regularly investigates new malware samples, constantly adding the latest intelligence.

SUMMARIZING THE SOLUTION

In order to protect against fast-evolving attacks, companies must adopt an ATM architecture capable of handling fast growing network traffic and rapid expansion. Equally important is an ATM architecture that is 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
    - Segment ATM systems from other network connected machines and ensure customer card 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 distribute 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.

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