Mitigating Security Risks at the Network’s Edge

Best Practices for Distributed Enterprises

WHAT YOU’LL GET:

+ Threats in the distributed enterprise and strategies for safer networks.
+ Network configuration must-dos.
+ Information on cloud-based security, PCI compliance, and parallel networks.
+ 2 methods for increasing security.
Every year, the public relations specialists from at least one blue-chip company invariably find themselves working around the clock on a crisis communications effort, attempting to explain to an angry and justifiably fearful public what led to their company compromising customer data. There’s always an immediate hit to the company’s reputation, resulting in a loss of brand loyalty, as customers take their business elsewhere. Of course, security breaches are rife with many other consequences.

**Potential impacts of a data breach:**

- Legal costs
- Loss of revenue or production due to unavailability of production resource
- Privacy compliance violation fines
- Payment Card Industry Data Security Standards violation fines
- Loss of intellectual, competitive or proprietary information
- Loss of future profits resulting from an inability to demonstrate a strong security process to clients, vendors, and partners

As the enterprise’s gateway to the Internet, distributed enterprises at the network’s edge are highly vulnerable to security threats.
RISKS AT THE EDGE

Enterprises with hundreds or thousands of locations face ongoing, massive challenges in maintaining network security and are at a particularly high risk of suffering data breaches. The highly vulnerable network edge must be carefully protected against vulnerabilities, threats, and malicious attacks. Criminals view the network’s edge as a soft target, since the distributed locations frequently process highly sensitive data (e.g. credit cards) while often employing weaker security practices.

Factors contributing to security weaknesses in distributed edge networks include:

+ **No onsite IT support.** Security measures like firmware updates and policy enforcement (e.g. firewall rules, access control lists, wireless configurations, and VLANs) should be conducted consistently, but can be easily be overlooked with no IT personnel on site. Even branches with local IT rarely have the resident expertise required to implement and maintain complex security configurations.

+ **Lack of employee security awareness.** In the age of “Bring Your Own Device,” employee devices accessing the corporate network present vulnerabilities through rogue access points, phishing and other social engineering attacks. If not properly educated, employees put companies at risk by opening emails or clicking links that allow malware onto their device and the network.

+ **Third parties & customers accessing the network.** Many enterprises interface with third parties that require Internet access. For example, an HVAC vendor may request to use the company’s network to monitor and adjust heating and air settings. Kiosks within stores require network access to transmit data, and customers demand WiFi for their handheld devices while shopping.

With multiple parties requiring Internet access and countless risks for security breaches, enterprises must be ever vigilant in developing, updating, and enforcing security policies on the network’s edge.

**ENTERPRISES WITH SMALL DISTRIBUTED LOCATIONS OR BRANCH OFFICES ARE AT THE HIGHEST RISK OF SUFFERING DATA BREACHES.**

**80% OF DATA BREACHES IN THE RETAIL INDUSTRY OCCURRED IN STORES WITH FEWER THAN 100 EMPLOYEES.**

**24% OF ATTACKS AFFECT INFORMATION AND PROFESSIONAL SERVICES INDUSTRIES.**

**34% OF DATA BREACHES IMPACT FINANCIAL ORGANIZATIONS.**

**20% OF ATTACKS TARGETED MANUFACTURING AND RELATED INDUSTRIES.**

**30% OF DATA BREACHES ARE ACCESSED THROUGH USER DEVICES.**

---

NETWORK ARCHITECTURES FOR THE DISTRIBUTED ENTERPRISE

HUB-AND-SPOKE: CONTROLLED ACCESS TO A CENTRALIZED DATA CENTER

“Hub-and-Spoke” describes architectures that leverage Virtual Private Networking (VPN) or Private Cloud Gateways. Some virtual private networks may not use encryption to protect the privacy of data. While VPNs often provide security, an unencrypted overlay network does not neatly fit within the secure or trusted categorization. VPNs should be configured to act as a gateway to one or more segments of the environment, leveraging robust authentication requirements, endpoint inspection capabilities, and integration with virtual desktop, proprietary device or Point-of-Sale technologies.
**BENEFITS**

**Security.** For multiple remote locations, a VPN can save the cost of a dedicated Internet connection. The maintenance of establishing a LAN connection through an Internet VPN is very low compared to traditional dedicated line solutions. With the proper encryption and authentication, the VPN architecture is a cost-effective and highly scalable solution for transmitting data securely.

**Threat detection.** Data can be analyzed as it moves through the network and used to identify potential threats or breaches. Leveraging the same intrusion prevention infrastructure in the core of the network for the branch offices minimizes chances of misconfiguration at the edge of the network.

**Governance.** Enterprises charged with transmitting or storing highly sensitive data can be more confident that they are in control of implementation and maintenance of the security architecture.

**RISKS**

**Planning and configuration mistakes.** Deploying a VPN requires a high level of planning and configuration, along with consistent updating of router firmware and enforcement of security policies. Networks must be properly configured and regularly maintained. Improperly configured segments may create security holes within the core network, which hackers may exploit to access sensitive data.

**Physical security** is also important to prevent theft of the edge router/gateway, which can be used to access corporate networks and sensitive data.

---

**KEY TO SUCCESS**

**Secure the hub-and-spoke architecture with isolation and segmentation.** In the past, many organizations used single- or dual-firewall architecture that divided networks into segments at Layers 3 and 4, limiting IP address ranges and Transmission Control Protocol (TCP) and User Diagram Protocol (UDP) ports that could traverse one segment or another. While this network security architecture is still the most common, more organizations are starting to control traffic at higher layers and use emerging technologies that facilitate traffic capture, analysis and control. For more information, refer to page 11, "Two Methods for Increasing Security."

**THE CLOUD FOR SECURITY SERVICES**

Many organizations want the cost savings and efficiencies of the cloud, but don't want to sacrifice traditional levels of control and security. Traditional network security solutions require expensive and over-featured hardware, archaic command line interfaces, intensive multi-day training courses, certification programs, and 400-page manuals.

When security is made too complex, the chances of configuration errors and unintended consequences increase. For distributed enterprises with little to no onsite IT support, cloud-based security provides visibility, configuration, and control of thousands of devices, anywhere in the world. Distributed enterprises should ideally deploy security solutions that combine the immediacy of on-premise management with the simplicity and centralized control of the cloud.
BENEFITS

Scalability and concentration. Increasing the scale of the cloud-based security architecture can be done in an easier, more cost-effective manner, requiring less planning than traditional hardware-based architectures. Security related processes, threat responses, updates, and security patches can be applied more quickly through cloud-based security applications architecture.

Threat management. Web traffic can be quickly and dynamically authenticated, encrypted, and filtered with near-zero latency. External Internet-based attacks can be rejected while detecting and preventing local malware.

Threat response. In contrast to many on-premise solutions, event logs and alerts can be dynamically filtered through cloud-based algorithms for more detailed monitoring and actionable analytics.

More flexible traffic routing. Simplified cloud-based tunnels and security protocols to protect data in transit can be configured and deployed between remote sites and corporate headquarters much faster and without the cost of traditional hardware headends.

Data isolation. Enterprises can isolate frequently targeted applications like email from sensitive data like cardholder information.

RISKS

Loss of governance. In a cloud-based model, data and information are stored with a third party. It may be difficult to inspect the provider’s data handling practices. And while rare, there is always a possibility that a rogue employee of the cloud provider could compromise data.

Time to resolution. For companies with appropriately staffed IT organizations, problems with on-premise solutions can be addressed by logging on directly to the appliance to engage vendor support faster. With cloud-based solutions, IT has to open a ticket and work externally to resolve issues, which may increase the time to resolution.

Customization. With the appropriate level of budget, resourcing, and time, on-premise solutions can be customized to meet an organization’s specific security needs while providing a robust solution set. With cloud-based security offerings, IT can address network vulnerabilities but loses a level of customization as a trade-off to speed and scalability.

Resource sharing and isolation failure. In a cloud-based security model, customers will share provider resources with other customers. Cloud providers generally implement isolation measures to prevent “guest-hopping” or pivot attacks (wherein a hacker exploits vulnerabilities of one operating system to obtain access to another hosted on the same physical hardware), but there is always a risk that these measures will fail. Because cloud services are extended to multiple clients with different risk levels, multi-tenant segmentation (separation of tenant resources by the cloud provider) is critical.

In addition, the provider may be incapable of completely deleting data from hardware, as clients often share or reuse hardware used by other clients.

Security compromise from within. If user permissions and roles are not set up carefully, a user might have the ability to delete or modify their data within the cloud solution. For example, an employee new to the solution with administrative access to the cloud solution could delete important data while they are trying to learn the new solution or a malicious employee may compromise data intentionally.
**Data portability.** It may be difficult, if not impossible, to move data should you ever need to switch cloud providers, unless there is prior agreement between the provider and the enterprise that the information is owned by the enterprise.

**KEYS TO SUCCESS**

**Maximize and automate cloud services with threat management services.** In addition to implementing isolation techniques and controls, distributed enterprises can reduce costs and network complexity by collapsing their infrastructure to some extent, while still employing multi-layered security throughout their sites. Threat management services offer a combination of services like anti-malware defense, anti-spam and mail protection, content filtering, traditional Layer 3 and 4 firewall rules, VPN and web proxy capabilities.

Many of these systems also include centralized, scalable cloud-based security as a service offering to augment and automate traffic inspection and provide tighter controls for sites with limited staff or monitoring tools.

For many enterprises, compliance is the major driver for changes in both security and general IT operations. Any technology or internal design change that can limit or reduce the scope of the environment subject to compliance can save money and time. Isolation of systems, applications, and network segments that handle payment card data, for example, can go a long way toward limiting the scope of PCI-DSS 3.0 audits.

**EVEN COMPANIES THAT DON’T PROCESS CREDIT CARD PAYMENTS SHOULD CONSIDER IMPLEMENTING PCI-DSS 3.0 AS A GENERAL SECURITY BASELINE. MANY PCI SECURITY STANDARDS ADDRESS GENERAL NETWORK RISKS OUTSIDE THE SCOPE OF CARDHOLDER DATA SECURITY.**
STRATEGIES FOR A SAFER NETWORK

ENFORCE DEVICE VISIBILITY — THE KEY TO ANY SECURITY STRATEGY

With many new mobile devices joining the enterprise WLAN network, visibility into mobile applications is becoming critical. Network administrators need the ability to identify, track, and categorize all devices accessing the network. Device visibility provides IT with real-time inventory and security intelligence for active remediation while allowing users to seamlessly connect to the network without disruptions or changes in end-user experience.

Best practices for enforcing device visibility:

- Use several criteria to identify devices in addition to MAC and IP addresses (which can be spoofed) like device IDs and system identifiers that use specific naming conventions
- Leverage compliance and auditing tools to provide additional insight into risks and vulnerabilities
- Enable alerting and enforcement actions for devices attempting to plug into the network
- Regularly audit and maintain up-to-date and accurate network topologies (logical and physical)
- Use a common set of security controls for policy management
- Institute governance, risk, and compliance security best practices
- Collaborate and communicate across teams within the IT organization

PHYSICALLY SECURE DEVICES & NETWORKS

PCI Security Standards require that servers, networking equipment, and other payment card system components be kept in a locked, access-controlled room—preferably with video surveillance. This mitigates the risk of an unauthorized individual stealing a device with access to the network. Physical security of devices also prevents attackers from attaching extraneous devices to the router that could monitor and steal data from the network.

CONDUCT REGULAR SECURITY ASSESSMENTS

During a security assessment, a professional assessor “attacks” the network to identify and recommend controls around any weaknesses in security architectures, including physical security, device key strength, network configuration, and client device vulnerabilities.

Regular network penetration tests, or security assessments, are required for PCI Compliance. The goal is to test access from low-security environments to high-security environments. This practice evaluates whether cardholder data is isolated from other segments on the network and verifies that no connectivity exists between in-scope and out-of-scope networks (networks that hold cardholder data and networks that do not). Businesses with high numbers of facilities or system components may assess only a sample of the total number of components, though the sample should be large enough to provide reasonable assurance that all business facilities or components are configured per the standard process. The security assessor must verify that the standardized, centralized controls are implemented and working effectively. PCI Security Standards recommend annual penetration testing, at a minimum.
TEACH EMPLOYEES TO RECOGNIZE NETWORK ATTACKS

Unfortunately, no firewall or antivirus software can perfectly protect the network against every type of malware. Therefore, it is imperative for enterprises to teach and enforce employee security protocols. In particular, employees should be trained to recognize and report phishing emails.

Employees should know the common signs of a phishing email:

- Encouragement to click on links, especially ones that are unfamiliar or do not match the supposed source’s web address
- Urgent requests to provide information, call a phone number, or download attachments
- Bad spelling or unusual grammar

NETWORK CONFIGURATION MUST-DOS

1. LOCK DOWN THE ROUTER ENTRY POINTS

- Disable Universal Plug & Play. Don’t allow unprivileged users to manipulate network configuration.
- **Disable WAN Pings.** Don’t let hackers probe security vulnerabilities.
- **Disable Remote Administration.** Don’t let intruders access the router’s user interface.
- **Use MAC Filtering.** Create a list of devices that have exclusive access or no access to the wireless network. While MAC addresses can be faked, this creates an extra barrier for the attacker.
- **Use IP Filter Rules.** Restrict remote access to computers on the local network.
- **Do not use public addressable WAN IP addresses at the edge.** Doing so leaves the edge of the network open to attacks.

WEB & EMAIL THREAT VECTORS ARE THE MOST SIGNIFICANT SOURCE OF NETWORK ATTACKS. WEB-DERIVED ATTACKS ARE 5x MORE LIKELY THAN EMAIL-DERIVED ATTACKS OVERALL.\(^6\)
2. CONFIGURE THE NETWORK FIREWALL FOR PCI COMPLIANCE

Five controls for PCI Compliance:

+ **Stateful Packet Inspection (SPI).** Monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass through the firewall.

+ **Port Forwarding Rules.** Opens ports on the firewall in a controlled manner for specific applications.

+ **Anti-Spoof.** Checks packets to protect against malicious users faking the source address in packets to hide themselves or impersonate someone else.

+ **De-Militarized Zone.** Keeps most computers running behind a firewall, while one or more computers also run outside the firewall, or in the DMZ, to add an additional layer of security to the enterprise network and give attackers access only to computers on the network within the DMZ.

+ **Updated Firmware.** In addition to being an important security practice, up-to-date router and modem firmware is required for PCI Compliance.

While improved practices for network implementation, maintenance, and security enforcement are important strategies for reducing the risk of a data breach, we recommend network segmentation or, better yet, application-specific parallel networks to ensure that the security vulnerabilities of one application cannot be compromised and pivoted off of to access data from other applications, like Point-of-Sale systems.

---

TWO METHODS FOR INCREASING SECURITY

1. CREATE SECURITY ZONES FOR NETWORK SEGMENTATION

Network segmentation allows for the partitioning of the network into “security zones,” or segments separated by firewalls. Properly configured segments separate applications and prevent access to sensitive data. A Point-of-Sale system, for example, should operate on a segment separate from third party applications, employee email, or public WiFi.

This limits the ability of attackers to pivot from one application to another, and allows network administrators to manage the quality of service (QoS) on specific segments, prioritizing bandwidth usage for mission-critical applications.

**First Steps for Network Segmentation**

Network segmentation is complex and requires meticulous, ongoing monitoring. This architecture, while highly secure if configured properly, presents many opportunities for configuration mistakes. Here are three steps to get you started:

+ **Create Ethernet port groups.** Logical groupings of Ethernet ports allow computers physically connected to Ethernet ports within a group to freely communicate. You may wish to disable one or all router SSIDs, or even the entire WiFi radio.

+ **Use WPA2/Enterprise, RADIUS/TACACS+, and PKI infrastructure.** This will provide a central repository for users or devices allowed to access the network and uses certificates to authenticate server and device.
+ **Leverage a PKI infrastructure for stronger security.**

+ **Use 2-Factor Authentication to minimize theft of user accounts being used by third parties.**

+ **Create and configure VLAN segments.** A VLAN enables devices to be grouped together. After creating a VLAN, select the LAN port(s) or Ethernet groups to which the VLAN ID should correspond.

Each segment should have its own IP address configuration, Routing Mode, Access Control, and Interfaces (i.e. WiFi SSIDs, Ethernet Groups, and VLANs). Currently, no tool exists to automatically monitor and search for vulnerabilities within a segmented network or between segments—such oversight must be conducted manually. For this reason, many enterprises will find that parallel networking is a better overall solution for keeping sensitive data secure.
2. KEEP IT SIMPLE WITH PARALLEL NETWORKS

In contrast to segmenting a single network, creating multiple parallel networks is a relatively simple solution. Separate applications are assigned completely separate networks, or “air-gapped.” This physical separation of data further prohibits attackers from using a compromised device to pivot to other servers and networks, including those that hold sensitive data.

For example, the enterprise should consider hosting customer WiFi, employee devices, and Point-of-Sale systems on their own respective networks. Enterprises with parallel networks expect third parties such as vendors, partners and kiosks who require Internet access to “Bring Your Own Network.” By expecting third-parties to provide their own parallel networks, the company can retain governance over its own network functions, while reducing the overall scope of work to maintain network security.

Parallel networks significantly reduce the amount of time and expertise needed to segment networks based on application, and limit the scope of work for maintaining PCI Compliance on the network used for transmitting cardholder data.
CRADLEPOINT SOLUTIONS

DESIGNED FOR SECURITY AT THE NETWORK’S EDGE

Cradlepoint’s router/firewall devices and cloud-based management software are designed to mitigate security risks and maintain PCI Compliance for distributed enterprises using all types of network architectures. A growing number of enterprises are transitioning to parallel networking, finding that Cradlepoint’s 4G solutions enable simpler and safer network segmentation. Additionally, parallel networks often reduce enterprises’ soft costs, including the need for complex network configurations that are subject to human error, more complicated PCI Compliance audits, and the general quality of service (QoS) settings for specific applications on the network.

ENTERPRISE CLOUD MANAGER FOR CENTRALIZED COMMAND AND CONTROL

Massive scalability: Monitor and manage thousands of remotely deployed devices

Enterprise Cloud Manager, Cradlepoint’s network management and application platform, allows IT managers to rapidly deploy and dynamically manage networks at geographically distributed stores and branch locations. Cradlepoint solutions are cloud-enabled for rapid deployment, dynamic management, and enhanced intelligence. Enterprise Cloud Manager provides an out-of-band control plane that separates network management data from user data. Management data (such as configuration, statistics, and monitoring) is transmitted from Cradlepoint devices to the Cradlepoint cloud over a secure Internet connection. User data (web browsing, internal applications, etc.) does not go through the cloud, but is transmitted directly to its destination on the LAN or across the WAN.

Designed for security: Management features enable security compliance and device tracking

Enterprise Cloud Manager’s user interface and analytics help automate security configurations and checklists, such as PCI DSS 3.0 Compliance. Geo-fencing and location services give enterprises real-time physical location of deployed devices utilizing GPS, WiFi, and location-based insights information. Enterprises can be notified when devices leave their normal locations, reducing the risk that hackers will be able to use stolen devices to access the network.

Enterprise Cloud Manager: A securely hosted solution

Cradlepoint Enterprise Cloud Manager is hosted at a world-class, third party storage facility on a secure, enterprise-class server, providing equipment redundancy, always-on power, multiple Internet channels, and backup and restoration service. Enterprise Cloud Manager servers are hardened, with unnecessary services disabled, permissions limited, and logs monitored. The servers are under patch management control to keep software versions and security patches current. In addition, the servers and application undergo regular vulnerability assessments and remediation.

All customer configurations reside in this secure physical facility, with access limited to authorized individuals only. Passwords stored within configurations are Advanced Encryption Standard (AES) encrypted. The facility is constantly monitored and recorded, while access to the facility requires multifactor authentication. Access records are available and auditable.
Fig 3. Enterprise Cloud Manager

Fig 4. Enterprise Cloud Manager
Easily manageable: Integrated, best-in-class security software

Through a RESTful API, Cradlepoint has integrated cloud-based security solutions for web filtering and anti-malware into Enterprise Cloud Manager. These security solutions allow IT and security personnel to inspect web traffic with near-zero latency.

Secure connectivity for always-on performance

Cradlepoint’s routing solutions are designed for the distributed enterprise to intelligently manage converged wired and wireless connectivity for a highly reliable “connected experience” at the edge. Router 4G LTE Private Networking capability leverages the cellular connection to become an extension of the private network without increasing the vulnerability of the network.

Secure at the edge: Extensible hardware and software features

Cradlepoint devices are designed for PCI Compliance protecting assets with stateful firewall, advanced encryption, network segmentation, and VLAN support. Cradlepoint devices also support Carrier Independent Overlay Private Network solutions and advanced VPN options.

Improve ease of security configuration with Ethernet ports and WiFi SSIDs that can be individually assigned to specific network segments. Intrusion Detection and Prevention functionality scans packets for attacks, malware, and Denial of Service attacks that can be blocked based on policy. Applications can be identified, along with behaviors indicative of exploitation.

Sources

1. Source: ZK Research Nov 2011
5. PCI Security Standards 3.0, p.15

TO LEARN MORE, VISIT CRADLEPOINT.COM