ARE YOU PROTECTING YOUR NETWORK FROM EVERY ANGLE?

In the face of growing cyber security threats coming from every angle, a multi-layered approach can help you defend your network against attacks and breaches. Explore ways to protect your enterprise while saving time, costs, and resources.

NCR

PATCH MANAGEMENT

Because prevention is better than the cure

The Online Trust Alliance's 2017 Cyber Incident & Breach Trends Report indicates one of the key avoidable causes of being compromised is a lack of prompt security patching. Most organizations have a blend of OS across the enterprise, further complicating the undertaking of continuous patching. The right managed services provider can help you establish preventative measures, and automate and streamline your patch management with services such as:

- Lab-testing patching for Microsoft, Adobe and Java prior to deployment
- Applying critical patches within one month of release, to comply with PCI mandates
- Continuously installing and validating patches across your ecosystem, regardless of OS
- Applying updates to FOH devices without the need for Internet connection
- Reporting and detailing detected vulnerabilities and updates when patches are applied

PCI COMPLIANCE

Reducing risk to both your enterprise and your customers

Maintaining full compliance with the PCI-DSS standard can be a daunting task, and one that requires constant upkeep to avoid the risk of fines and, if audited, even disqualification for payment card receipt. With nearly 250 requirements across 12 main categories – which must maintain compliance throughout the 12-month certification period – it's easy to see how it can quickly become overwhelming. With a suite of security solutions that help you manage this effort, here are some examples of how we can support your PCI-DSS compliance.

If you face challenges in this area...	...Here's how we can help
Build and Maintain a Secure Network 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters	NCR Site Shield is a commercial-grade multi-featured firewall that NCR sets up and manages on your behalf. It helps restrict dangerous connections to and from the internet, while allowing the necessary business applications to function.
Protect Cardholder Data 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks	NCR Site Shield can provide encryption technologies for helping to secure networks via VPN and locking down wireless networks where necessary.

If you face challenges in this area...	...Here's how we can help
Maintain a Vulnerability Management Program 5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications	NCR Threat Defender helps to safeguard Windows systems by scanning for security weaknesses. It also uses whitelisting to control the applications that can run on the network. Our Managed Anti-Virus service offers increased malware protection on the designated systems and our Patch Management automatically addresses vulnerabilities in common third-party software.
Implement Strong Access Control Measures 7. Restrict access to cardholder data by business need-to-know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data	NCR Secure Access provides a way of accessing systems over the Internet for remote control and file transfers. This service can restrict cardholder network access to designated individuals and supports two-factor authentication.
Regularly Monitor and Test Networks 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes	NCR Secure Access logs user network access and our Log Management functionality can capture system-level security events and provide logs for you to review. We also offer PCI Compliance Services that can be used to schedule internal and external network security scans.
Maintain an Information Security Policy 12. Maintain a policy that addresses information security for all personnel	Our PCI Compliance Services provides templates for generating security policies and web-based training modules that can be used as part of your security program.

SMART OR IOT-ENABLED DEVICES

Efficiency and vulnerability are sometimes two sides of the same coin

A recent Hewlett-Packard study posits that 70% of IoT devices are currently vulnerable to an attack, and Innovation Enterprise reports that 66% of IT leaders can't be sure how many devices are even in their environment. As your IoT infrastructure expands, so does the need for your network protection and security that covers the new potential ways cyber criminals can gain access to your IT stack. Look for ways to implement a set of multi-layered defenses across your enterprise that can automatically help to identify, mitigate, contain and protect against an attack the moment it happens. This can be accomplished through network tricking segmentation, rights-based access, controlled connectivity, encryption and performing scans of your endpoints to help identify potential security vulnerabilities.

NEW, SOPHISTICATED MALWARE

Cyber criminals blend tactics old and new to find and exploit weaknesses

According to Kapersky, in 2016 every 40 seconds a business was infected by malware; and Cybersecurity Ventures predicts ransomware will cost $6 trillion annually by 2021. Some of the most prominent types of malware CSO magazine warns against include:

Viruses	Though they typically comprise less than 10% of all malware these days, this is the only type of malware that actually "infects" other files, making cleanup difficult.
Worms	Like viruses, these may seem like a relic from decades ago, but can cause significant damage as they are self-replicating and can spread without end-user action.
Trojans	Favored by cyber criminals for their ease of execution (DIY kits are for sale on underground sites), Trojans deceive end-users into executing malicious instructions, bypassing patches, firewalls, and other traditional defenses.
Hybrids / Exotic Forms	Botnets, infected networks that are controlled as a group, are a prime example of hybrids that blend different types of traditional malware. Remediation requires finding, identifying, and removing the controlling component from memory.
Ransomware	One of the most talked-about forms of malware, ransomware holds enterprise data hostage every 40 seconds. More alarmingly, an estimated 30% of those who pay the ransom still do not get their data unlocked.
Fileless Malware	This growing distribution method comprises over 50% of all malware and continues to grow. This is malware that doesn't directly use files or the file system. Because they don't rely on files or file systems to spread, instead using memory or other "non-file" OS objects, they are extremely difficult to detect and deter.

WI-FI & OTHER CONSUMER-FACING TOUCHPOINTS

Don't let customer convenience threaten your network

One bad actor can use your Wi-Fi network to wreak havoc and put your business on the wrong side of the law. Even if you're not the person committing illegal acts, law enforcement officials can trace the source of the copyright theft to your business' IP address and hold your brand accountable.

Help protect your brand from users downloading illegal content, accessing age-restricted sites, accessing your corporate network, or abusing free Wi-Fi by starting with these initial easy fixes:

- Separate your public and business Wi-Fi
- Restrict access to unsavory websites
- Limit the length of time users can use your public Wi-Fi in a single session
- Prohibit open connections
- Secure your Wi-Fi and change the password regularly – patrons won't mind asking for it

NCR offers a managed Wi-Fi service with dedicated wireless access points that provide a scalable, cost-effective and reliable wireless infrastructure without the need for dedicated access point controllers. This can help reduce single points of failure found in other WLAN solutions, which require separate access point controllers.

VISIT NCR.COM/NSS TO LEARN MORE

WHY NCR?

NCR Corporation (NYSE: NCR) is a leader in omni-channel solutions, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables nearly 700 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Atlanta, Ga., with over 30,000 employees and does business in 180 countries.

For an in-depth conversation about your network security needs, call your NCR representative or visit **www.ncr.com/360-security**