ROBUST SECURITY PATCHING MITIGATES CYBERSECURITY RISKS

VULNERABILITY CAN LEAD TO LOSS

All software is vulnerable. It's just a fact of life. Whether the software sits on your laptop, runs on a server, resides on a chip within a firewall, or is an app on your phone, it needs to periodically be updated and patched to remain secure, function properly and protect you from outside cyberattacks.

PATCHING: YOUR FIRST DEFENSE AGAINST ATTACKS

The challenge of not patching your network is the risk of cyber attacks. In the security world, it is common knowledge that 80% of cyber attacks use vulnerabilities for which patches already exist.[1] With over 300 cyber strikes on public safety agencies in the past 24 months, ransomware and malicious malware attacks are becoming more and more common.[2] This is something your mission-critical systems can't afford. According to the Department of Homeland Security Cybersecurity Unit, as many as 85% of all targeted attacks can be prevented by applying security patches.[3]

PATCH MANAGEMENT CAN BE COMPLICATED

While it sounds simple, security patching can be a complicated process especially with mission-critical infrastructure. Your network is comprised of dozens of different software and applications. You have operating systems, server applications, firewalls, hardware-based network appliances, end-user devices and more. Do you have the expertise and tools to make certain that your systems are always updated while ensuring network availability and security?

THREE STEPS TO EFFECTIVE SECURITY PATCHING

To identify the need or gaps around system patches, all hardware and software assets, network and communication flows and dependencies are identified, mapped, classified and managed according to criticality. As new patching needs arise they are tested and deployed within the network.

1. SECURITY PATCH IDENTIFICATION

The first step is to identify all patches required to keep your system secure. This includes servers, PCs, hardware-based appliances, like firewalls and routers. Our engineers track all available anti-malware definitions and software patches. Only the applicable patches needed for your system are identified and selected for testing. This validates that no unnecessary software is introduced via the patching process.

2. SECURITY PATCH TESTING

This is a critical step. Before applying patches to your production system all potential patches are first implemented in a test environment to identify any potential risks or issues. This can be expensive for an agency to build an in-house test environment. We have a dedicated Information Assurance lab with test systems to validate patches, test interactions and identify procedures including if a reboot is required.

3. SECURITY PATCH DEPLOYMENT

Once validated as safe for deployment, we offer multiple ways to implement security patches. You can deploy patches or we can implement them for you by setting up a deployment cadence, weekly, monthly or quarterly. We work with you until the job is done. Our patch deployment reporting tool can illustrate your security patch operations and help you to better manage your cybersecurity operations.

FLEXIBLE DEPLOYMENT OPTIONS

With multiple services available we are committed to keeping your network secure from potential threats. With any of these services, you have the assurance that patches and fixes have been pretested on our lab systems to ensure they are ready to be deployed.

SECURITY UPDATE SERVICE (SUS)

This service gives you the most flexibility on when you make updates. We offer a secure extranet site where you can download pre-tested patches and fixes.

REMOTE SECURITY UPDATE SERVICE (RSUS)

Our technicians will remotely install the security updates on your radio network. Any required reboot of the system is your responsibility. As part of this service, we will do a system health check before installing patches. We will also provide reports outlining updates completed.

REBOOT SUPPORT SERVICE

In combination with our on-site install service, our technicians will schedule a reboot at a predetermined time, minimizing business disruptions.

ON-SITE PATCH DELIVERY SERVICE

Let us take care of your entire patch and reboot requirements on-site. We will address vulnerabilities from third-party software, and if a patch fails, develop a plan and then redeploy. Our robust patch deployment reporting tool keeps your team, management, auditors and regulators fully informed.

MOTOROLA SOLUTIONS - YOUR TRUSTED PARTNER

As a leading provider of mission-critical solutions, we understand your mission can only be as secure as your partners enable you to be. Our goal is to provide you with transparency, accountability and security that's built-in from the start.

We believe that our set of highly knowledgeable people with industry certifications, best-in-class organizational policies and procedures and state-of-the-art automation and analytics tools enables us to uniquely deliver enhanced cybersecurity solutions that address your needs today and in the future.

GLOBAL EXPERIENCE

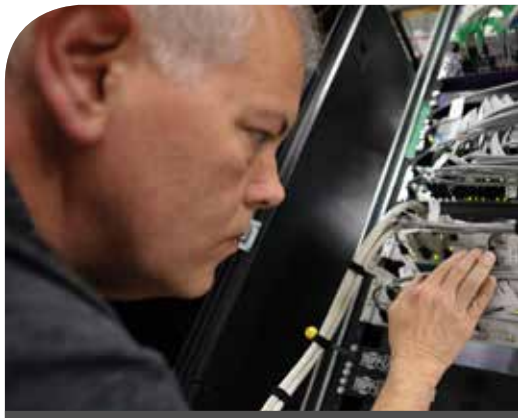
4M
USERS UNDER OUR MANAGED SERVICE

20M
EVENTS PROACTIVELY MONITORED EACH DAY

13K
SYSTEMS INSTALLED

100K
CUSTOMERS ACROSS 100 COUNTRIES

90+
YEARS OF EXPERIENCE



WAUKESHA COUNTY DEPENDS ON PATCH MANAGEMENT TO MINIMIZE CYBER THREATS

"The reason why we chose security patching was really to prevent ransomware attacks. What we try to do is make it more difficult for those people that are wearing black hats to get into our system to impact the functionality."

Chris Petterson,
Manager of the Waukesha County Radio Services[5]

For more information on our Security Patching Service contact your Motorola Solutions representative or visit us at **www.motorolasolutions.com/cybersecurity**

Resources

1 https://www.seculore.com/cyber-attack-archive
2 https://www.computerweekly.com/news/450421649/Security-Think-Tank-Patching-is-vital-and-essentially-a-risk-management-exercise
3 https://www.us-cert.gov/ncas/alerts/TA15-119A
4 https://www.nist.gov/cyberframework/framework
5 https://www.motorolasolutions.com/content/dam/msi/docs/services/waukesha-county-case-study.pdf

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**