SECURITY PATCHING MITIGATES CYBERSECURITY VULNERABILITIES AND RISKS

Security patches are one of the most important digital security tools that every public safety agency needs. Regardless of where system software resides, it needs to be periodically updated to remain secure, function properly and protect you from cyberattacks.

PATCHING: YOUR FIRST DEFENSE AGAINST CYBERATTACKS

In 2021, 58 percent of local government organizations were hit by ransomware, up from 34 percent in 2020. This is a 70 percent rise over the course of a year, demonstrating that adversaries have become considerably more capable of executing the most significant attacks at scale.[1]

This is something your mission-critical systems can't afford. According to the Department of Homeland Security Cybersecurity Unit, as many as 85 percent of all targeted attacks can be prevented by applying security patches.[2]

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?

85%

OF TARGETED ATTACKS CAN BE PREVENTED WITH PATCHING[2]

MOTOROLA SOLUTIONS
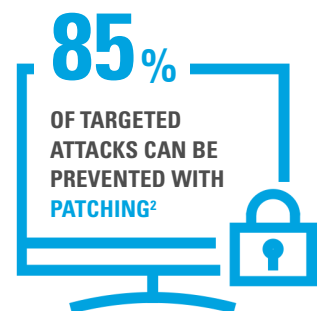
FOUR STEPS TO EFFECTIVE SECURITY PATCHING

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 and 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 test. 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.

4. GOING FORWARD

Per CISA Guidelines, implement regular security patching and updates on all operating systems and software to ensure physical and virtual assets are secure. Remove any unauthorized or outdated component from your system that could enable insecure access. Maintain proper encryption protocols and key management policies.[3]

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

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 SCALE & EXPERIENCE

300+
SECURITY EXPERTS FOCUSED ON 24/7 MONITORING & RESPONSE

9B
SECURITY EVENTS PROACTIVELY MONITORED EACH DAY

100%
CO-MANAGED APPROACH FOR VISIBILITY AND CONTROL

20+
YEARS OF EXPERIENCE DEVELOPING CYBERSECURITY SOLUTIONS

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

Resources
1 https://news.sophos.com/en-us/2022/09/28/the-state-of-ransomware-in-state-and-local-government-2022/
2 https://www.us-cert.gov/ncas/alerts/TA15-119A