SECURITY PATCHING AND SYSTEM UPGRADES

CYBER THREATS ARE A REALITY

For agencies tasked with mission-critical operations, system downtime endangers lives and failure is simply not an option. But cyber attacks continue to accelerate in number, frequency and impact. In fact, the annual cost of global cybercrime damage is expected to hit $5 trillion in 2020[1]. There have been over 300 cyber strikes on public safety agencies in the past 24 months[2]. You could be next and this is something your mission-critical systems can't afford.

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[3]. According to the Department of Homeland Security Cybersecurity Unit, as many as 85% of all targeted attacks can be prevented by applying security patches[4].

PATCH MANAGEMENT CAN BE COMPLICATED

While it sounds simple, security patching can be a complicated process especially with mission-critical infrastructure. Your network consists of dozens of different software and applications. You have operating systems, server applications, firewalls, hardware-based network appliances, end-user devices and more. You need the expertise and tools to make certain that your systems are always updated with the latest antivirus software on a monthly basis.

SYSTEM PATCHING REQUIRES YOUR SYSTEM TO BE CURRENT

You cannot patch aging systems. Today's IP-based, mission-critical networks require periodic upgrades to stay current. You need system upgrades to enable both software and hardware technology refresh. These large implementations can be complex - a change or upgrade to one component may adversely impact another. Managing all of these functionalities, each on a different timeline, can be a challenge and requires specialized mission-critical skill sets and industry-leading tools.

SO ARE YOUR SYSTEMS CURRENT? AND ARE YOU PATCHING REGULARLY?

If not, Motorola Solutions can help you with both. Contact your Customer Support Manager or Account Executive today.

NOTES

[1] Cyber Defense Magazine
[2] www.seculore.com/cyber-attack-archive
[3] www.computerweekly.com/news/450421649/Security-Think-Tank-Patching-is-vital-and-essentially-a-risk-management-exercise
[4] www.us-cert.gov/ncas/alerts/TA15-119A

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. 800-367-2346 **motorolasolutions.com**