AVTEC PROTECT

PUTTING OFF SECURITY UPDATES: IS IT WORTH THE RISK?

CURRENT CUSTOMER ENVIRONMENT

Dispatch operation centers today typically require IT managers and system maintainers to regularly update computer operating systems to apply the latest features and security patches.

While this is a necessary requirement to maintain the highest level of performance and protection for control center software systems, the update process can be tedious, time consuming and straining on an organization's resources. As a result, routine system updates can be neglected, potentially degrading performance and exposing security vulnerabilities that could lead to a costly attack.

CUSTOMER CHALLENGES:

COMPATIBILITY

“If it’s not broken, don’t fix it. Our mission critical software applications may not be compatible with the latest security update.”

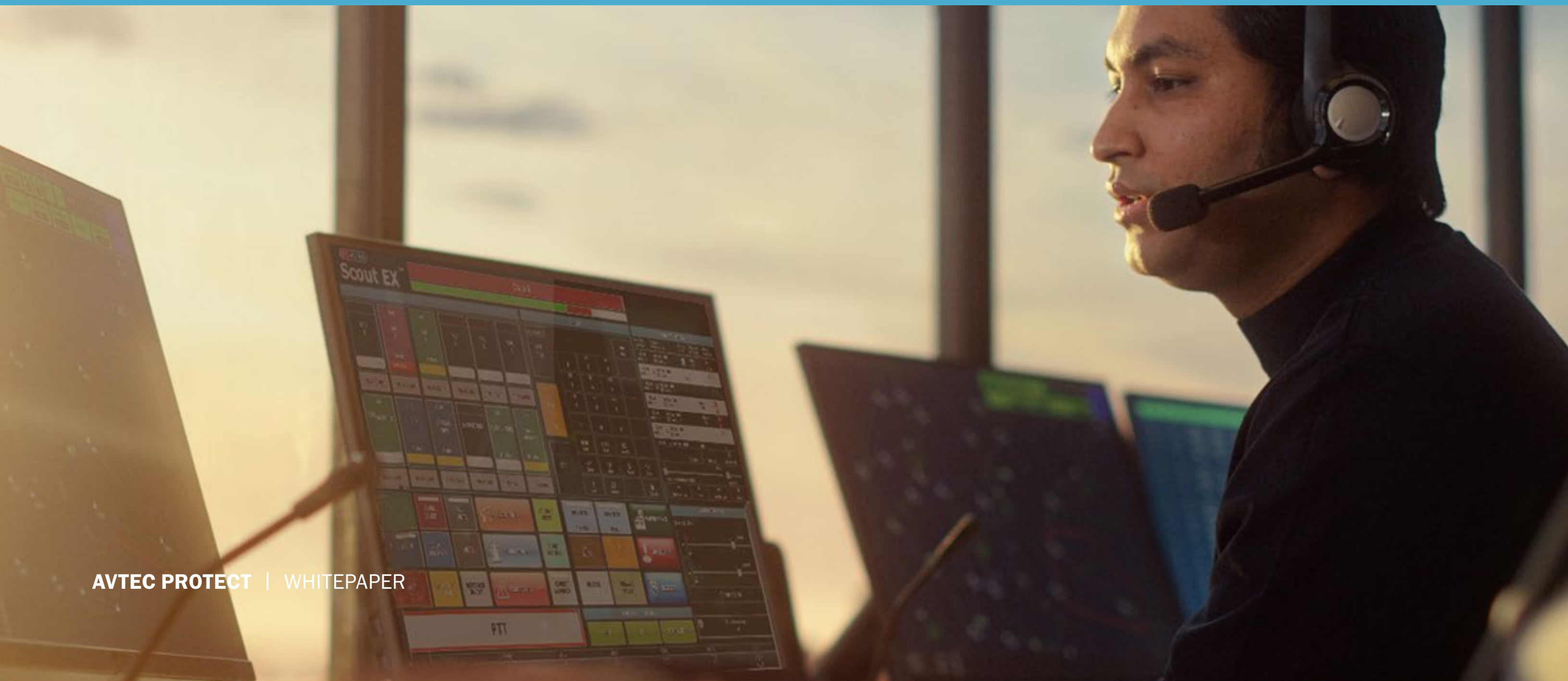
Over 80% of security professionals claim they’ve postponed a patch to avoid disrupting the workplace.[1]

TIME AND RESOURCES

“We don’t have time to keep up with security updates. Our IT team is swamped with other projects.”

LIMITED EXPERTISE

“We share IT resources with other agencies. We don’t have someone on our team that has the expertise to implement security patches.”



COST VS. BENEFIT:

WHY BEING PROACTIVE SAVES IN THE LONG TERM

Putting off security updates may provide savings now, but can result in significant costs in the future. A cyber attack can be devastating to an organization with serious ramifications including revenue loss, downtime and reputational damage.

66%

of organizations were hit with a ransomware attack in 2023[2]

$4.45

Million - The global average cost of a data breach in 2023[3]

20 days

The average downtime a business will experience due to a ransomware attack[4]

FACTORS TO CONSIDER

Delaying security updates can be detrimental to your mission critical environment and workflows. When deciding how and when to prioritize your investment in security updates, consider these factors:

Reliability and Performance:

In a mission critical environment, it is imperative that devices are operating efficiently. Skipping updates can put your organization at risk for reliability and performance related issues. Outdated software often runs slower and can cause crashes, decreasing the productivity of your staff and potentially disrupting operations. In addition to maintaining security, software updates can target bugs and performance related issues to help make your devices run smoother. Operating system updates help increase the stability of your PCs and often offer new features that can improve user experience.

Security Incidents:

Between the financial losses and disruption to operations, the cost of a cyber attack can be significant. The threat landscape is changing rapidly with cybercriminals constantly looking to exploit software vulnerabilities and security flaws. Using outdated software can leave your system exposed and unprotected. System updates provide patches for vulnerabilities found in the current operating system. By completing software updates regularly, you ensure these essential patches are applied to keep your system protected from malware and ransomware.

Compliance Violations:

For some industries regular system updates are mandatory, and failing to comply can come with a hefty price tag. If a healthcare provider fails to keep up with security updates and a data breach occurs, the cost of the attack could include serious fines for violating HIPAA. In the energy and utilities industry, system owners must perform security updates to meet the required compliance with NER-CIP. Using an outdated system can also make you legally liable for damages, should customer data be compromised. Failing to regularly perform security patches can also put you at risk of breach of contract with customers and partners who require you to adhere to security best practices.

Incompatible Software:

Software developers design applications to work with the latest OS and utilize its newest features and functions. Using an outdated OS may cause compatibility issues with your software applications or block you from installing new technology or applications that require a newer OS.

Sources

Inc., Tanium. “Tanium Study: 81% of CIOs and CISOs Hold Back From Making Critical Updates to Keep the Business Running.” Tanium, 3 Apr. 2019, www.tanium.com/press-releases/tanium-study-81-of-cios-and-cisos-hold-back-from-making-critical-updates-to-keep-the-business-running/.

Adam, S. (2023) The State of Ransomware 2023, Sophos News. Available at: https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/ (Accessed: 16 January 2024).

Security, IBM. “Cost of a Data Breach 2023.” IBM, July 2023, www.ibm.com/reports/data-breach.

Holmes, Rachel. “Evidence-Based Strategies for Ransomware Prevention.” Bitsight, 20 June 2023, www.bitsight.com/blog/ransomware-prevention. Accessed 8 Jan. 2024.

PRIORITIZING UPDATES: CRITICAL FIRST STEPS

Once you've recognized the importance of prioritizing security updates, the process may seem daunting. Updating your system can be a complex challenge when you have mission critical applications involved. Changes to your operating system or STIG settings could cause incompatibility issues and disrupt your operations, so it's important to plan ahead. When it comes to mission critical software, be sure to check with the manufacturer to ensure compatibility. They may offer guidance or services to assist with security updates. At Avtec, we test security updates in our own lab before deploying them to a customer site to ensure compatibility.

HOW AVTEC CAN HELP

Keeping up with security updates can be a daunting task and it gets even more complex when mission critical applications are involved. For Scout customers looking to safeguard their systems and ensure compatibility, Avtec offers Avtec Protect™, a comprehensive security update service designed to ensure that Scout customers keep their equipment up-to-date and fully protected with the latest OS patches and STIG settings, all while maintaining the full functionality of Scout. With Avtec Protect, your technical team can confidently shift their focus to other critical priorities and know that Avtec will help to secure your system and strengthen your cybersecurity posture as a trusted partner.

WHAT'S INCLUDED:

Routine Data Backup

Avtec backs up your Scout files to ensure the safety of your assets in the event of an attack.

Windows OS Patches Updates

Apply the latest qualified Windows OS patches. This includes feature and cumulative updates and antivirus signatures.

STIG Settings Updates

Update to the latest qualified STIG configurations for your release. These include Windows Firewall, MS Defender, MS .NET Framework, and MS Edge.

Updates Qualified by Avtec

Ensure your system continues running smoothly with the latest patches and STIG setting— all tested and qualified by Avtec.

ONE PLATFORM.
UNLIMITED POSSIBILITIES.

The Avtec Scout family of solutions integrates all your communication center needs, whether simple, highly complex or somewhere in between. Discover how our solutions can adapt and scale to any environment. Feel confident in your ability to protect people, assets and livelihoods with the most efficient communications system.

Don’t skip another security update! For more information regarding Avtec Protect, reach out to us at is@avtecinc.com or call us at 1-803-358-3600.