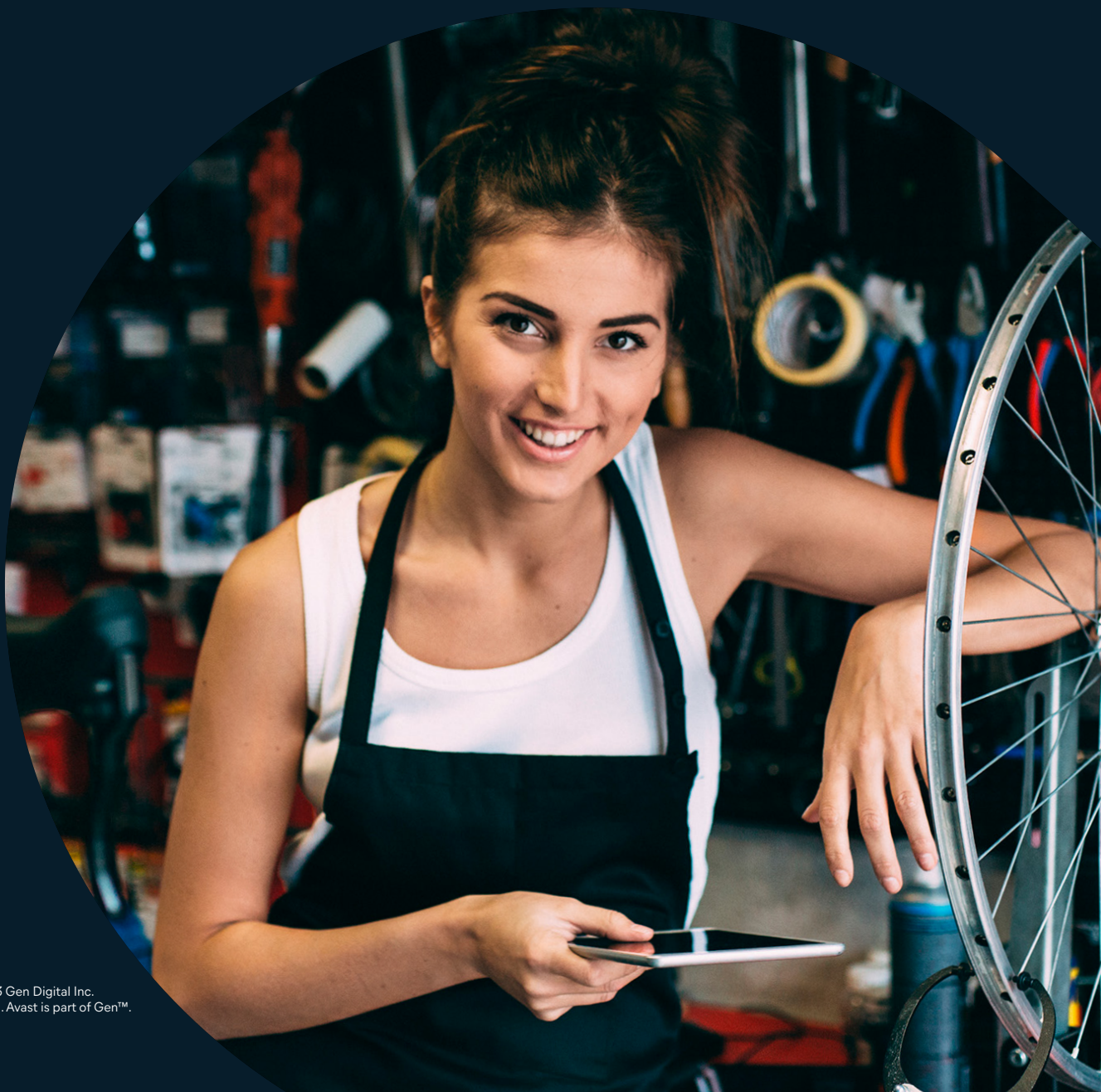
Avast Business

Your Logo Goes Here

White paper

Software patches: The seatbelt of cybersecurity

16 November 2023



Avast Business

Virtually every passenger car and commercial vehicle that has seats also has seat belts. And there is voluminous research that seat belts save lives and reduce crash-related injuries. For example, according to the U.S Centers for Disease Control and Prevention (CDC), "Seat belts reduce serious crash-related injuries and deaths by about half."

A significant figure, given that CDC estimates that "More than 2.2 million adult drivers and passengers were treated in emergency departments as the result of being injured in motor vehicle crashes in 2012" and that "Non-fatal crash injuries resulted in more than $50 billion in lifetime medical and work loss costs" in that same year.

Yet, every year, a saddening percentage of people in vehicle accidents die or are critically injured because they weren't wearing a seat belt.

Imagine how much higher that percentage of deaths and injuries would be if seat belts didn't come with every vehicle. What if every vehicle owner had to research and compare seat belt solutions, select them, buy them, install them, and then ensure that they kept functioning and were up to date?

In the face of such challenges, would most vehicle owners decide to skip the expense and hassle, and do without seat belts? That seems highly unlikely, given what is known about the increased risks of driving or riding without them.

But for a variety of reasons, none of which make logical or financial sense, many organizations still don't invest in patching automation and processes. Somehow, leaders at those organizations decide that it's easier, cheaper, or both to continue doing business on systems that they know are unprotected or under-protected, rather than protect those systems adequately. This is true even when they know the magnitude of the risk and have witnessed peer companies suffer significantly (and publicly) from taking similar risks.

Avast Business

Patching: clearly valuable, yet inconsistently deployed

Where effective IT security is concerned, the power of proactive patching processes (and the tools that support them) is difficult to overstate. The Australian Signals Directorate, that country's analog to the U.S National Security Agency, estimates that at least 85 percent of targeted cyberattacks can be prevented by four simple steps:

- Application whitelisting
- Patching of applications
- Patching of operating systems
- Restricting of administrative privileges

And the value of patching is apparently widely known among those who identify themselves as security experts. In July 2015, the good folks at Google published research based on surveys of 231 cybersecurity experts and 294 "typical Internet users" about how they protect the data that matters to them. Among the experts, installing software updates was the top protection measure cited, ahead of strong passwords and two-factor authentication. Some 35 percent of the expert respondents listed software updates as important, compared with only two percent of the non-experts, who focused instead on antivirus software and strong passwords.

In many cases, effective patching is not only valuable, but essential for doing business. As HP points out in a June 2015 Security Briefing entitled The Hidden Dangers of Inadequate Patching, "Compliance with industry standards as well as various government regulations also requires a robust servicing and patching strategy." Examples of regulations that require patch management include the Payment Card Industry Data Security Standard (PCI DSS) and the European Network and Information Security (NIS) Directive.

Yet despite its obvious value to security efforts, patching remains largely an unsolved problem. The 2015 Verizon Data Breach Investigations Report (DBIR) found that "99.9% of the exploited vulnerabilities were compromised more than a year after the common vulnerabilities and exposures (CVE) was published." Even more troubling, the same report found that "M any existing vulnerabilities remain open, primarily because security patches that have long been available were never implemented. In fact, many of the vulnerabilities are traced to 2007 – a gap of almost eight years."

85% of targeted cyberattacks can be prevented by 4 simple steps*:

1. Application whitelisting
2. Patching of applications
3. Patching of operating systems
4. Restricting of administrative privileges

*Australian Signals Directorate

An April 2015 alert published by the U.S Computer Emergency Readiness Team (US-CERT) lists what US-CERT found to be the "Top 30 Targeted High Risk Vulnerabilities." The oldest of the CVEs and security bulletins related to those top 30 vulnerabilities dates back to 2006.

Why patching remains broken – and how to fix it

As Google said in its research mentioned previously, "Software updates...are the seatbelts of online security; they make you safer, period. And yet, many non-experts not only overlook these as a best practice, but also mistakenly worry that software updates are a security risk."

Mistaken or not, that worry is one of several also shared by some experts. HP's research highlights several reasons why otherwise security-conscious business people don't patch or trust patches.

- Patches break things
- Patches introduce security problems
- Patches don't work as promised
- Patches include undocumented/unwanted "bonus features"
- "Silent" patch deployments often disrupt users or confuse troubleshooting efforts

Beyond these concerns, discovery and prioritization of all systems that need or may need patching can be challenging. Those challenges can be exacerbated by support for mobile, remote, or itinerant IT users.

Fortunately, modern patch management solutions address all of the concerns listed above. For example, patches that are thoroughly tested and inspected before being delivered to your organization are unlikely to break things, introduce security problems, not work as promised, or include unwanted features. Patch management solutions that are sufficiently configurable can deliver patches without disturbing users or disrupting business operations. And modern solutions can deploy and manage patches for all of your organization's most critical operating systems and third-party applications.

For those who are seeking to secure larger, more complex environments, a consistent methodology for establishing business-driven patching priorities can be helpful. Development and execution of that methodology must be based on specific business requirements and goals. However, they need not be created from scratch. Forrester Research, for example, offers its clients what it calls its "prioritized patching process" ("P3").

ISACA is a non-profit IT trade association, formerly known as the Information Systems Audit and Control Association. In its February 2014 newsletter, ISACA offers a summary of the process in the article "4 Considerations During the Patch Management Process."

1. Estimate attack difficulty by using predictive threat modeling to identify your most vulnerable assets and predict how difficult it would be to compromise them.

2. Measure the potential effects of an exploit on each asset, based in part on the type and sensitivity of data residing upon and accessed by that asset.
3. Measure the so-called "intrinsic risk" of each vulnerability, based on factors such as whether an exploit of that vulnerability already exists and the maliciousness of the behavior of that exploit.
4. Assign patch priority based upon risk classification and assessment, guided by the three recommended estimates and measurements.

All of this is an essential part of effective patch management, but is only a part of the entire process. HP's research identifies several other required steps.

1. Accurate, complete discovery of all assets
2. Determination of what assets need protecting, and what process to use to protect each asset
3. Identification of and constant engagement with reliable providers of the patches needed (which can require subscriptions to email lists or following vendors on social media)
4. Determination of how best to install and manage the patches needed, based on factors such as staffing and automated solution costs, patch failure rates, and time to deploy

Other examples of patch prioritization strategies and execution recommendations are available from numerous sources – from research firms to patch management solution vendors and their integrator partners. However, it is very likely that you can improve patch management significantly at your company without any such resources. A strong start toward better patching begins by committing to identify, evaluate, deploy, and manage the patches for your most critical systems and applications more consistently than is being done today.

Yes, patches can break things or disrupt user productivity. Yes, sometimes patches even introduce new security vulnerabilities. But none of these justifies not patching in a timely, comprehensive manner. Indeed, these challenges and others argue strongly for a proactive, strategic, operational approach to patch management specifically and to improve cybersecurity more generally. That approach begins with developing and refining processes for prioritizing and implementing patches consistently and effectively, then selecting the tools that are best suited to implementing those processes.

Comprehensive, effective assets, systems, and service management require assets, systems, and services that are completely, reliably secure. And comprehensive, effective, user-centric security begins with comprehensive, effective patch management.

Comprehensive, effective assets, systems, and service management require assets, systems, and services that are completely, reliably secure. And comprehensive, effective, user-centric security begins with comprehensive, effective patch management.

Avast Business

How Avast Business can help

Seat belts combine protection with the ability for you to reach what you need. Avast Business has the tools and talent you need to enable comprehensive, consolidated, and automated patch management across your organization.

Avast Business offers multi-layered protection to safeguard your users and IT resources against the most sophisticated threats. Solutions include next-gen antivirus, automated patch testing, deployment, and management for Microsoft Windows systems and third-party applications, cloud backup, secure web gateways, zero trust network access, and more.

Our solutions are integrated in a single security platform. This enables rapid automation of both security and IT management policies, and delivers unequaled visibility across IT security and management activities.

Avast Business' security platform also delivers comprehensive, configurable reports and dashboard options. These help to sharpen risk and threat visibility, ease compliance with regulations and policies, and improve your overall security posture. For more information contact your Avast Business Account Manager or visit **avast.com/business.**