WHITE PAPER

The Importance of Vulnerability Assessment and Patch Management with Acronis Cyber Protect

Identify and close security gaps with ease

Cybercriminals compromise home computer users and businesses in a variety of ways. One of the most popular and effective is exploiting vulnerabilities in software, either in the operating system itself or in any of the installed third-party apps. As you might expect, cybercriminals typically go after widely used applications and services, making Windows operating systems and popular third-party software (PDF readers, office suites, browsers, archivers, etc.) common targets. Of course, that doesn't mean that these attacks won't probe other applications, quite the opposite, in fact. Cybercriminals will often check what software is in use to search for rare apps with severe vulnerabilities that were never patched.

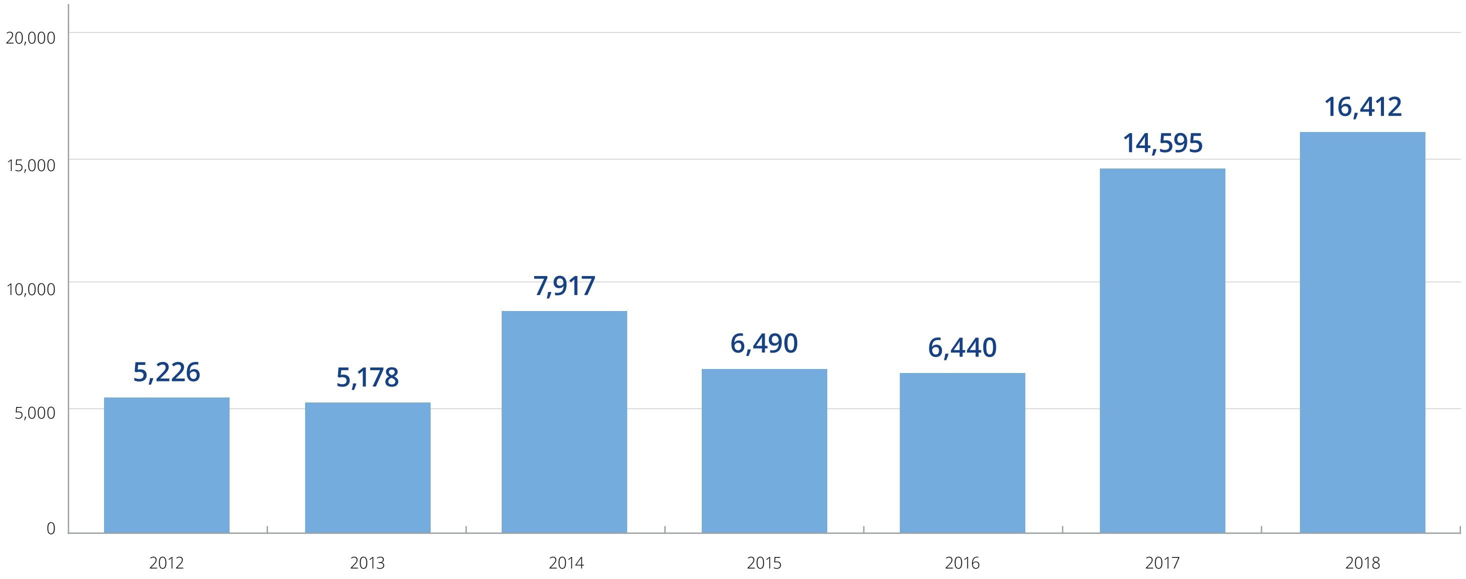
These vulnerabilities are flaws in software or service code or logic. All software has vulnerabilities because it's programmed by humans, the more concerning point is how severe those vulnerabilities are and how many of them are present in the software. To determine that, you can use the Common Vulnerability Scoring System (CVSS), an open framework for communicating the characteristics and severity of software vulnerabilities. The CVSS consists of three metric groups: base, temporal, and environmental. The base metrics produce a score ranging from 0 to 10, which can then be modified by the temporal and environmental metrics. According to the CVSS v3.0, vulnerabilities range as follows:

None	Low	Medium	High	Critical
0.0	0.1-3.9	4.0-6.9	7.0-8.9	9.0-10.0

Any vulnerabilities are dangerous, but if software vulnerabilities are determined to be High or Critical, they will require immediate action. That said, a vulnerability needs to be exploitable (i.e. used in real life) to do damage.

Vulnerabilities are not limited to software, either. They can be found in hardware and devices as well. These are much harder to fix, obviously, a good example being the relatively recent Meltdown and Spectre vulnerabilities in modern Intel, IBM Power, and some ARM-based processors. These hardware vulnerabilities allow programs to steal data that is currently processed on the running OS.

As shown in the graph below, the number of vulnerabilities is on the rise. BeyondTrust reports that Microsoft vulnerabilities continued to rise in 2018, with 700 vulnerabilities discovered.



A report by Skybox Security «2019 Vulnerability and Threat Trends»

Why patching is important and how it's done today

Vulnerabilities are eliminated through software patches – updates released by a manufacturer to close security loopholes, add functionality, or improve performance. Some software vendors do this well, others don't. In either case, there is always a time gap – as any patch release requires time.

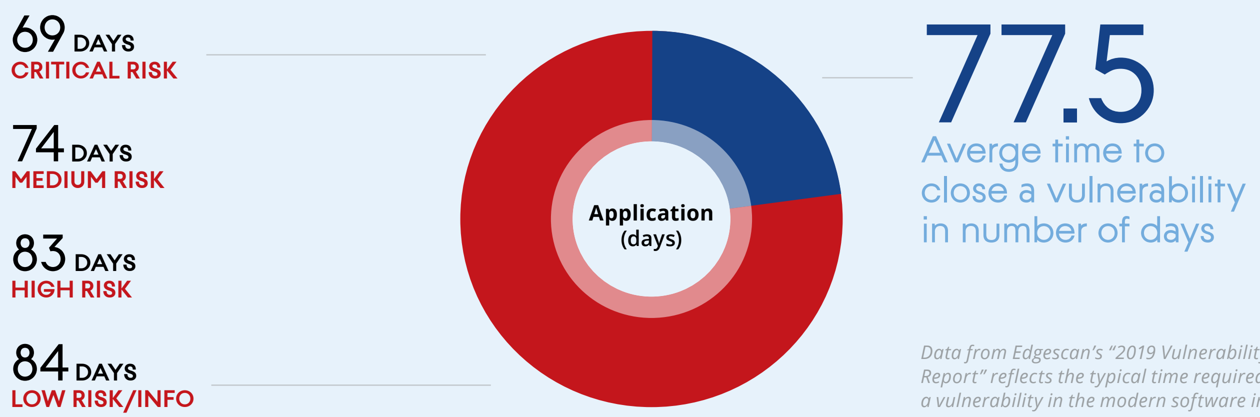
For example, the Equifax data breach, one of the biggest known data thefts to date, was done via a known "critical vulnerability" in the Apache Struts software, which was disclosed on March 7, 2017. Despite being alerted by the Department of Homeland Security on March 8, "Equifax did not fully patch its systems … leaving its systems and data exposed. On May 13, 2017, attackers began a cyberattack on Equifax which lasted for 76 days…"

Patching is typically done for supported software. As soon as support for older versions of applications stops it should not be used, as the developer is not obliged to close security holes anymore.

The problem is when patching isn't transparent and automated, both personal users and business admins aren't nearly as careful about performing them regularly. That's why software developers are continuously improving and automating update procedures for their products. Microsoft, for example, has Windows Server Update Services (WSUS) for corporate environments and Windows Update for home users and home offices. These are update mechanisms for Windows-based applications. Companies like Java, Adobe, Google, Mozilla, and others use their own update routines typically embedded into specific software that they release.

That said none of them are perfect. Microsoft can only update its own software and can't do anything about third-party software. Other software developers only update their own apps and often require user interaction, which brings it's own problems because users tend to delay updates as long as possible to avoid an operating system restart. Alternately, users will install updates but not restart their machine, leaving their system vulnerable until it's restarted.

That's why specialized solutions called patch management systems, exist. But, unfortunately, these solutions often lack required functionality and fail to meet customers' expectations.



Data from Edgescan's "2019 Vulnerability Statistics Report" reflects the typical time required to close a vulnerability in the modern software industry.

What you should expect from a good patch management system

Patch management systems function as a separate product, or as a part of a larger cybersecurity suite, aimed at managing multiple software patches and keeping your infrastructure up-to-date and protected from threats. In organizations, patch management is typically controlled by a system administrator who will configure it according to the organization's security policy, structure, and needs, including specific functionality requirements.

- Support as many apps as possible, not just operating systems. Of course, you need to pay attention to the specific apps you use in your environment, but a simple guideline is the more apps the system can cover, the better.
- Automatic patch deployment will save admins a lot of time, especially in large organizations and enterprises. This goes along with a process called staging: the ability to install new patches into a special environment and automatically mark the installed patches as approved in a couple of days (or other trial period) if everything performs correctly. A golden rule of patch management is never to deploy a patch for a whole infrastructure. Failures are always possible and you don't want to bring your entire organization to a non-working state. To prevent that, patch test segments of your infrastructure and gather information on new patch availability automatically.
- Admins need to be able to create custom groups of machines where only specific patches should be applied. These groups are typically arranged according to department, operating system used, java apps running, etc.
- Patch statuses need to be clear and actionable in the management console. If a patch fails the admin needs to know why and be able to fix the situation remotely, if not automatically. The management console should provide visibility into all unpatched machines and on each device's compliance status (GDPR, for example).
- Patches that couldn't be applied because the machines were offline should be retried automatically. Often this will happen with mobile devices and laptops, and good patch management systems track these devices and finalize patching as soon as the device is online with minimum admin involvement.
- Detailed reports and notifications should be available. Missing patches, vulnerable systems, delayed updates, systems requiring reboot, who was notified (admins), etc. – all this information should be available for an administrator to perform his job effectively.

> **NOTE:** This is not a full list, of course, but addressing these points will justify a patch management system in a business environment. data centers. Customer and management environments are logically isolated.

Acronis vulnerability assessment and patch management

As a cyber protection company, Acronis covers all aspects of cybersecurity to provide seamless business continuity for its partners and customers. Vulnerability assessment and patch management are important parts of Acronis' cyber protection proposition, which centralizes your security posture in one management console and one agent, eliminating typical security management complexity.

Acronis vulnerability assessment and patch management functions meet all the expectations listed above and more, all while providing detailed information about devices and applications running on your network. Vulnerabilities are classified according to an internal severity scale and required updates are fetched automatically and rolled out to different groups in a variety of ways by tweaking the corresponding protection plan. Acronis distributes patches from its cloud servers around the world but also uses peer-to-peer patch distribution technology to prevent slowdowns during patch rollout for non-Windows systems and third-party apps. Updates, upgrades, and applications can contain packages with very large files. Downloading and distributing them can consume network resources on the devices receiving them. That's why Acronis uses delivery optimization to reduce bandwidth consumption by sharing the work of downloading these packages among multiple devices in a customer's deployment.

Unlike many competitive solutions, Acronis Cyber Protect's vulnerability assessment supports not only Windows-based networks but also Linux networks. Its patch management capability includes a set of client management tools to automate a wide range of IT administration functions to save time and resources. For instance, Acronis Cyber Protect's patch management feature is able to patch endpoints, which are located inside and outside the corporate network, a frequently demanded capability from customers with mobile users.

This patch management functionality can be used in unique safe restore scenarios from a full disk backup. As you may be aware, malware can be backed up, especially in full system backups. This happens when there is no anti-malware product on the backed up machine or the anti-malware solution in place wasn't good enough to catch it. Acronis Cyber Protect is able to scan backups for malware and eliminate them so admins can restore a user's machine from a "clean" disk image, free from malware. But, what is more important, in the next release Acronis Cyber Protect will be able to patch the system to the latest available updates automatically if the administrator enables this option – thus preventing live new worm epidemics. These are actual infection cases reported by our partners where the company network was compromised, the admin tried to restore machines from a full disk image, and they got infected all over again because net worm malware was using an unpatched vulnerability in the operating system.

Acronis Cyber Protect's safe restore feature guarantees you're protected by updating anti-malware bases of the Acronis Cyber Protect agent in this full disk backup to the latest definitions and AI-models, so you can detect malware and prevent it from attacking already patched systems.

> **To summarize:** with Acronis Cyber Protect you gain top-level vulnerability assessment and patch management functionality that provides a number of useful, unique features due to close integration between exceptional cybersecurity and an award-winning backup solution.

Patch management is crucial to business continuity

Vulnerability assessment and patch management are important parts of a proactive, multilayered cyber protection strategy. While enrolling new machines into the network, they need to be checked for any known security flaws and patched whenever possible. This will ultimately increase:

- **Security:** Patches are often created after a vulnerability is found either by security researchers or when customers have experienced a data breach, to ensure other businesses' data, applications, and systems remain safe. Critical patches should be applied as soon as possible to avoid data theft and lasting reputation damage that often follows a security breach.
- **Compliance:** Patch management plays a significant role in compliance, minimizing potential data leaks and adding to your data protection. This is especially important for government institutions, healthcare services, and organizations in the financial sectors who face huge losses due to legal penalties, alone, following a data leak through an unpatched vulnerability.
- **Productivity:** If a machine was hacked and rendered useless through an unpatched vulnerability, or after a bad patch you can't restore a user's machine to a working state, that's obviously a detriment to business continuity and productivity. A good patch management solution will take care of that.

For more information visit **www.acronis.com**