TeamViewer
Remote Management

WHITE PAPER

Never Miss a Patch Again:

Reduce Security Risks and Keep Your IT Infrastructure Safe with Automated Patch Management

Table of **Contents**

Introduction:
What is a Patch Management Solution?

Keeping your IT infrastructure stable and secure requires regular maintenance and timely updates for all computers and devices. Neglecting to update your computers and devices can lead to significant security vulnerabilities due to outdated software.

IT organizations are faced with new challenges ensuring devices are always up to date or “patched” due to the increasing number of corporate devices, applications, and cyber vulnerabilities.

In the IT world, a “patch” is a list of changes made to a computer program specifically designed to update, optimize, or fix it. Patches are applicable to both fixing software vulnerabilities and other bugs, which are made available to users by means of software updates. Monitoring the availability of patches and installing missing patches requires an automated patch management solution.

With a patch management solution, you can detect and patch outdated, vulnerable software.

Patching is therefore an essential part of IT security. Without it, security deficiencies will never be fixed, leaving open invitations for hackers or cybercriminals to steal corporate data. According to a study by NIST, 90 percent of successful attacks against companies are due to known vulnerabilities and could have been prevented by correct, timely patching.[1]

Importance of Patch Management for Enterprises

Malware cyberattacks can cause significant damage to businesses. Data loss, image damage, or production downtime can cost organizations millions. The number of malware variants increases almost daily. And that means your IT infrastructure requires efficient security management.

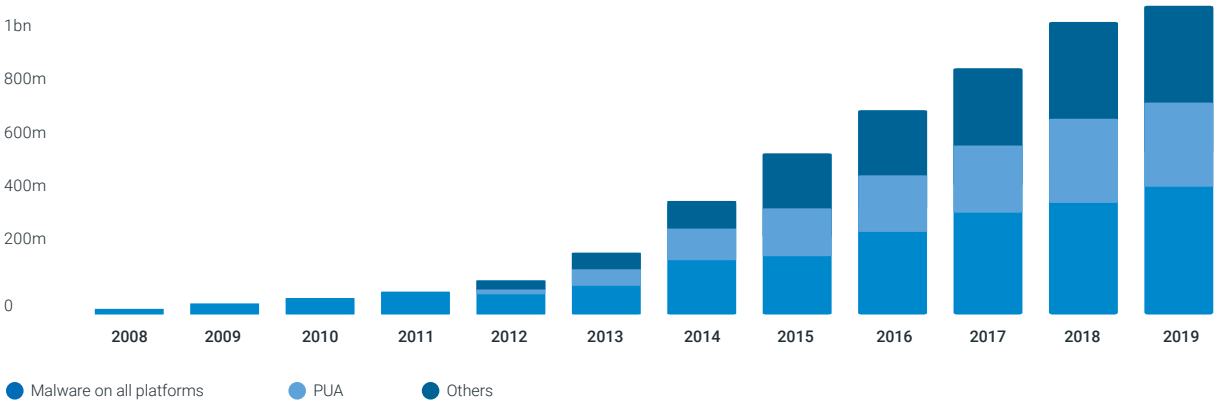

Figure 1: Total known malware variants *PUA (potentially unwanted application)[2]

Cyberattacks, such as the WannaCry ransomware attack in 2017, showed once again how important it is to protect your hardware and software from attacks. Now, most systems and applications of large companies are accessed through the internet, making it easier for criminals to gain access. Antivirus software alone is not enough to completely protect IT infrastructures. Because of the higher complexity of software, more mistakes are made in development, leaving software with vulnerabilities.

The German Federal Office for Information Security (BSI) announced that "successful attacks are often due to attacks via unknown vulnerabilities and lack of patch management."[3] This is because the number of critical vulnerabilities in standard IT products has increased sharply in recent years.

In 2017 alone, there were more than 450 known vulnerabilities in the 10 best-known applications. According to BSI, there aren't any signs that the situation will change in the next few years. 12,174 vulnerabilities have already been verified in 2019, in the top 50 most frequently used software products.[4]

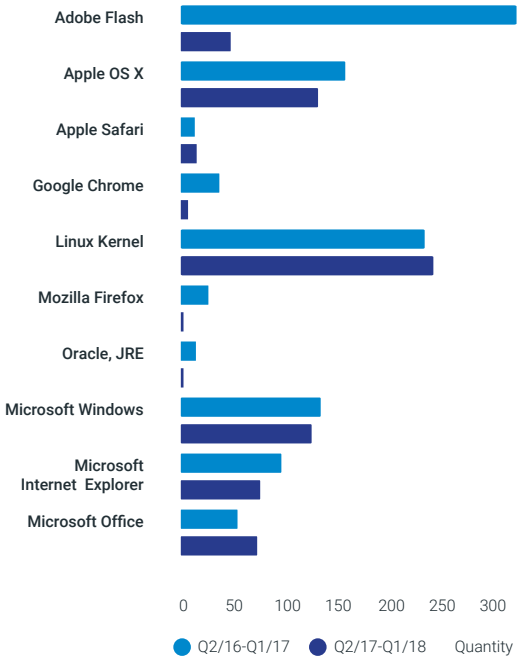

Figure 2: Critical CVE Entries, as of 31.03.2018[5]

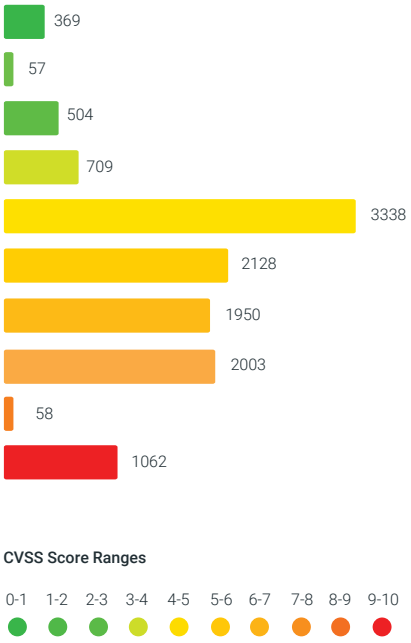

Figure 3: Distribution of vulnerabilities in 2019 as of 30.10.19. From non-critical (green) to critical (red) of the top 50[4]

90 percent of exploited software vulnerabilities occur within the first 40 – 60 days of being released. As IT administrators are held accountable, they must act quickly. Patches must be deployed, tested, and rolled out. For IT administrators, this not only takes an enormous amount of time, but also has a significant cost factor.

With the increase in volume of vulnerabilities manual patching has become more tedious and less practical to do on a regular basis with assurance that all the devices have in fact been successfully patched. Manual patching processes require manual follow-up processes as well, which increases the strain on IT administrators' time and resources.

When it comes to a manual patching processes, depending on the complexity of the system, it might be necessary to rely on end users to implement the patches. This usually impacts the successfulness of patch implementation.

Patching the server side is relatively easy because IT has full control over it, but the client side is where most of the vulnerabilities occur (~95 percent) and keeping clients up to date is hard. Logistical issues get in the way like the human factor; people delay patches because they don't want to disrupt their work. For these reasons, patching is often neglected, although patches are often available for a long time, they are never implemented due to time and cost reasons. However, if patching is not done properly, cybercriminals can exploit these vulnerabilities systematically.

These software vulnerabilities can lead to serious security vulnerabilities in an application or IT network. This is why companies face the great challenge of better organizing and managing their IT infrastructure today. Patch Management is the optimal solution to relieve IT administrators and increase the performance, efficiency, and effectiveness of the IT infrastructure. An efficient patch management solution checks which patches are best suited for the systems, automates the distribution and rollout of patches, and classifies them according to urgency. Therefore, patch management not only improves patch deployment, it also minimizes manual steps and reduces the risk of human error.

Risks of Poor Patch Management

Costly system downtime

Lost credibility with customers

Lengthy remediation time

Questionable data integrity

Negative PR

Unsecure IT environment

Benefits of Patch Management

Regular and automated patching significantly increases the security of IT systems and the integrity of networks. This is the most obvious advantage of patch management. However, an automated patch management solution brings other important benefits to businesses.

Increase IT productivity and reduce unplanned downtime

Manual patch management is very time-consuming for IT administrators. Identifying vulnerabilities, establishing which endpoints require patches, and finally rolling them out and ensuring the patches were properly applied to the affected computers and laptops takes a lot of time and resources.

Moreover, this causes unplanned downtime for employees who need access to their devices. An automated patch management solution therefore not only helps IT staff increase their efficiency, but also minimizes unplanned downtime for employees.

Enables security and data compliance to mitigate risks

Security compliance guidelines in IT departments are critical and should not be overlooked. IT compliance protects companies from penalties or potential damage to their brand. For example, software vulnerabilities are major security risks that can lead to serious data breaches.

If sensitive employee or customer data are exposed, companies may incur penalties for violating data protection regulations. This could result in customer churn or negative publicity. An effective patch management solution detects security vulnerabilities and can help mitigate these risks.

Key **Benefits**

Save time with fast, comprehensive IT system updates

Automatically apply patches to fix software vulnerabilities

Manage computers centrally

Boost employee productivity

Leverage insights from detailed cross-network reporting

Understand your infrastructure with system status overviews

Reduce unplanned device downtime

Mitigate security and compliance risks

Key **Features**

Identify Vulnerabilities

Get total visibility across your network by automatically detecting vulnerabilities due to outdated software.

Fast Rollout, Integrated with TeamViewer

Deploy Patch Management to your entire network with just a few clicks.

Automatic Patch Deployment

Automatically detect and deploy policy-based patches for outdated, vulnerable software, operating systems, and third-party applications to keep your IT infrastructure secure and updated.

TeamViewer Patch Management Solution

Patching endpoints can protect your entire network from cyber attackers. But did you know just one unpatched device puts your entire IT infrastructure at risk?

With the Patch Management solution from TeamViewer Remote Management, **vulnerabilities are automatically detected**, making it easy to keep every device updated and safely patched.

Protect your IT networks with Patch Management by TeamViewer

Stay on top of critical patches with automated patch management. Instantly see if updates are available and mass deploy them from a centralized platform.

Manage and deploy Windows updates from a centralized dashboard, ensuring all your Windows devices are up to date.

Reduce risks, automatically monitor and deploy patches for third-party applications and operating system updates.

See the patch status of your devices and all available patches in a single dashboard.

Define individual policies for different departments or customers to customize and automate patching tasks.

Prioritize patches, see which patches are critical, urgent, or can be postponed by sorting them by priority.

Manage and check your patches remotely, from anywhere. The seamless integration between TeamViewer Remote Management and TeamViewer Remote Access allows you to access devices as needed with only a few clicks.

Conclusion

IT organizations know they must continuously protect their companies from cyber criminals and that an automated patch management solution is key to improving endpoint security. While patch management is critical, it doesn't have to be complicated.

With easy-to-use features, Patch Management by TeamViewer enables you to proactively protect your IT infrastructure, and eliminate tedious manual patching tasks, while increasing the security, stability, and integrity of your network.

Resources

Request a free demo of TeamViewer Remote Management (includes Patch Management)

Learn more at teamviewer.com/patchmanagement

Get started with a free trial of Patch Management

References

1. National Institute of Standards and Technology (November 2019): Automation Support for Security Control Assessments: Software Vulnerability Management, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8011-4-draft.pdf
2. Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit in Deutschland 2018, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf
3. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf;jsessionid=F64FE0EE50A281C976D952B395DCD531.2_cid369?__blob=publicationFile&v=5 S.11
4. CVE Details (2019): Current CVSS Score Distribution for all Vulnerabilities, https://www.cvedetails.com/cvss-score-distribution.php
5. Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit in Deutschland 2018. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3 page. 43
6. CVE Details (2019): Vulnerabilities by Date, https://www.cvedetails.com/browse-by-date.php

About TeamViewer

As a leading global remote connectivity platform, TeamViewer empowers users to connect anyone, anything, anywhere, anytime. TeamViewer offers secure remote access, support, control, and collaboration capabilities for online endpoints of any kind and supports businesses of all sizes to tap into their full digital potential. TeamViewer has been activated on approximately 2 billion devices; up to 45 million devices are online at the same time. Founded in 2005 in Göppingen, Germany, TeamViewer is a publicly held company listed on the Frankfurt Stock Exchange, employing about 800 people in offices across Europe, the US, and Asia Pacific.

www.teamviewer.com