DATASHEET

Patch Management Challenges

Survey Results and Insights as Organizations move to Everywhere Workplace

Introduction

Today’s work environments are no longer limited to a contained space where IT-controlled PC workstations are the center of productivity. Organizations nowadays are more distributed than ever before, leading to larger attack surfaces. In the Everywhere Workplace, employees connect with various devices to access corporate networks, data, and services as they work and collaborate from new and different locations, so patching has never been more challenging.

Meanwhile, IT and security teams are struggling to keep the constantly widening remote work landscape under control. Keeping the new online workspace safe and up to date with the latest security patches is necessary but has become increasingly challenging.

The Challenges

A new study by Ivanti revealed that 71% of IT and security professionals find patching to be overly complex and time-consuming. As threat actors are maturing their tactics and weaponizing vulnerabilities, especially those with remote code execution, organizations are struggling with attack surface risk and ways to accelerate patch and remediation actions.

IT and security professionals simply cannot respond fast enough; 53% of those surveyed said that organizing and prioritizing vulnerabilities takes up most of their time. This is alarming because the longer vulnerabilities remain unpatched, the more exposed a business is to the risk of an attack or ransomware. However, no organization can patch all its exposure points and risk-based prioritization must be done quickly to keep ahead of automated adversarial attacks. Today, unpatched vulnerabilities remain one of the most common points of infiltration for ransomware attacks, which have increased in frequency and impact to businesses of all sizes.

IT and security teams also spend a lot of their time issuing resolutions for failed patches (19%), testing patches (15%), and coordinating with other departments (10%). The myriad of challenges that IT and security teams face when it comes to patching may be why 49% of respondents believe their company's current patch management protocols fail to effectively mitigate risk.

IT and security professionals said they spend the **most** time each month on the following activities:

🟥 **53%** - Organizing and Prioritizing Vulnerabilities

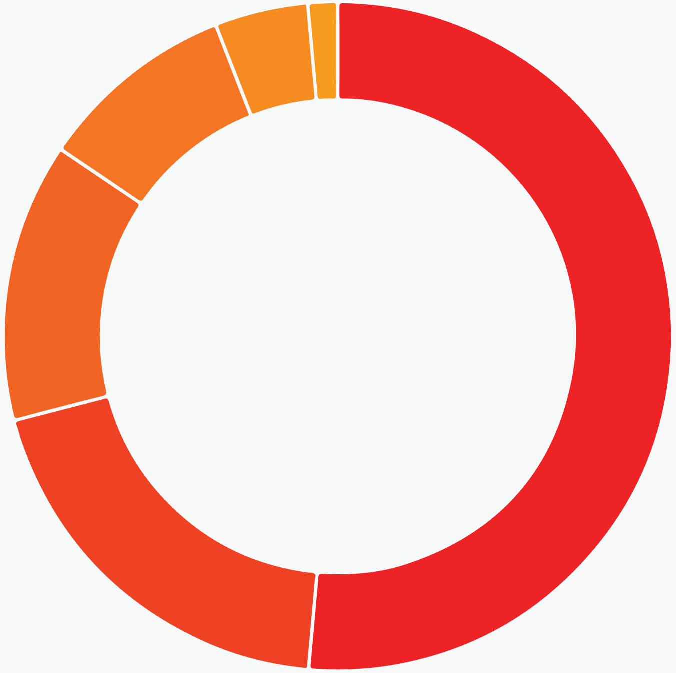
🟥 **19%** - Issue Resolution for failed patches

🟧 **15%** - Testing Patches

🟧 **10%** - Coordinating with other departments

🟧 **3%** - Compliance

🟨 **1%** - Record keeping



The Causes

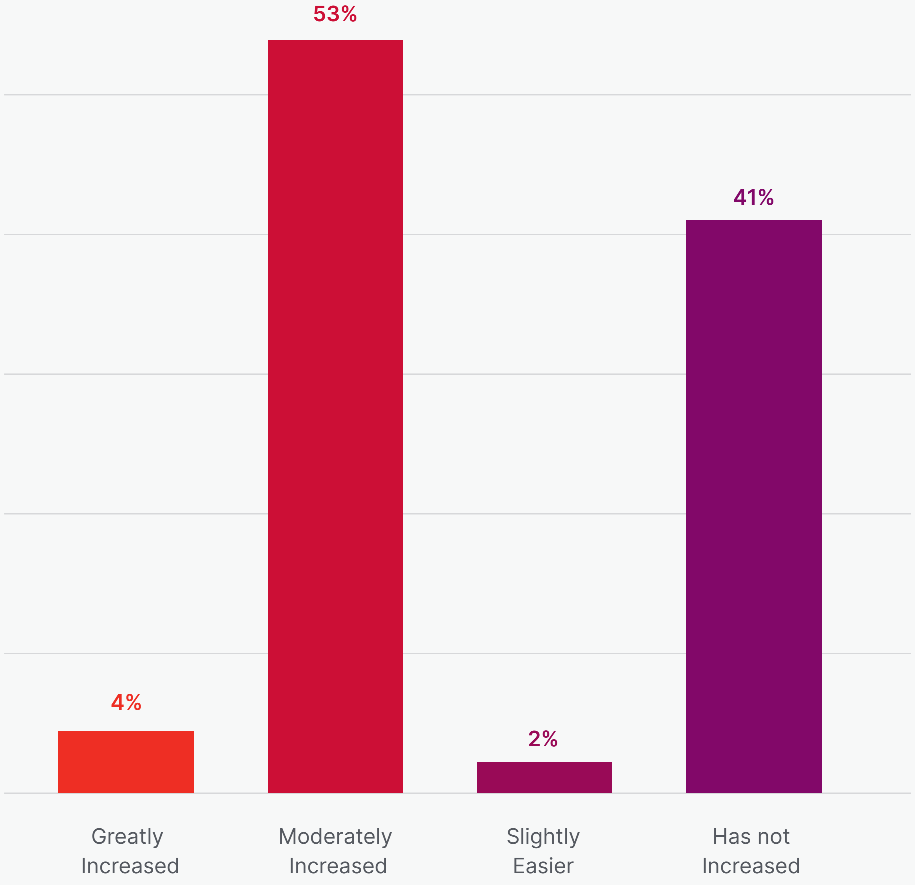
A majority (57%) of respondents believe that the global transition towards a decentralized workspace has made patch management more complex to deal with. The scale of patch management has also increased with so many different endpoints available to users and the business-critical systems that support them – from Windows to macOS, Linux to Windows Servers, and more.

And then, some IT systems are difficult to patch because they cause outages. A daunting 61% of the IT and security professionals said that they receive requests from line of business owners to postpone maintenance windows once a quarter. Another 28% said that they get such requests once every month.

At the same time, the speed of vulnerability weaponization continues to increase, especially for those with the capability of allowing for remote code execution (RCE). It's the perfect storm of poor visibility due to the recent switch to a work from anywhere and the growth of threat actors quick to find and use exploitable vulnerabilities.

Additionally, many organizations lack the security expertise or time to allow their resources to collect threat intelligence and map active exploit threats with the open vulnerabilities in their organization to achieve risk-based threat context. A shortage of IT staff has reduced the ability to mitigate security issues promptly for many companies. And for organizations such as these, cyberattacks, especially ransomware, have proved to be the most devastating.

To what extent has remote work increased the complexity and scale of patch management at your organization?



The Threat Landscape

As IT teams struggle to cope with an increased attack surface, hackers are maturing their tactics and monitoring where enterprises have vulnerability exposure risk. They are balancing dogged persistence and patience with sophisticated use of exploits, tools, and emerging technology. Their main goal is to disrupt, steal and act to make monetary gains by exploiting enterprise business.

Another survey by Ivanti revealed that 63% of those surveyed said their organizations have suffered a ransomware attack in the past year. And 89% of respondents described laptops, desktops, and mobile devices as the most targeted devices.

Hackers are always on the lookout for vulnerabilities and IT and security teams are struggling with prioritizing their patch management efforts so they can quickly resolve vulnerability risk exposure.

The WannaCry ransomware attack, which encrypted an estimated 200,000 computers in 150 countries, remains a prime example, even after four years, of the severe repercussions that can occur when patches are not promptly applied. A patch for the vulnerability exploited had existed for several months before the initial attack, yet many organizations failed to implement it. And even today, two-thirds of companies still haven't patched their systems. Yet organizations around the world are still being targeted by WannaCry ransomware attacks; there was a 53% increase in the number of organizations affected with WannaCry ransomware from January to March 2021.

Building Trust-Context for Security and Risk Management

The expanding work landscape and digital transformation will continue. However, there needs to be a way to expand the trust-context for security and risk management.

Implementing a Zero Trust framework is paramount for securing sensitive enterprise data from unauthorized access and cyber breaches from attacks. At its simplest, Zero Trust provides organizations continuous evaluation of their employee devices, endpoints, assets, and networks that business relies on.

President Biden signed an Executive Order in May 2021 stating that federal agencies must develop plans to implement a Zero Trust security strategy. Zero Trust security is also a top priority for IT and cybersecurity professionals: according to a recent study conducted by Ivanti, 98% of North American IT and security practitioners said that their security practices will become more aligned with the Zero Trust strategy over the next year.

Trust-context will look at the risk aspect for the devices, endpoints, and assets that are used in the Everywhere Workplace. Understanding what level of vulnerability risk is acceptable and what patches need to be implemented to meet the business-set requirements for trust is expected to increase the value of risk-based patch management.

Top industry leaders, practitioners, and analyst firms recommend a risk-based approach to identify and prioritize vulnerability weaknesses and to accelerate remediation effectiveness. The White House recently released a memo encouraging organizations to use a risk-based assessment strategy to drive patch management and bolster cybersecurity against ransomware attacks. Furthermore, Gartner® listed risk-based vulnerability management amongst top security project that security and risk management professionals should focus on in 2021 to drive business value and reduce risk.

Conclusion

While productivity has increased in the Everywhere Workplace, threats have also skyrocketed. In this scattered ecosystem, employees use various devices to access enterprise data, networks, and applications to keep working from anywhere, anytime. These decentralized workstations are more prone to significant threats from bad actors, who are capitalizing on the sudden shift to a perimeter-less workspace and as a conduit to infiltrate organizations.

The Everywhere Workplace demands an approach to security and risk management that continually evaluates the current context for establishing trust that is based on active risk-based analysis. With access to the best vulnerability and patch intelligence that includes active vulnerability exploits in the wild, vulnerabilities with ties to ransomware, sentiment data on patch reliability, Ivanti is expanding the tools that IT and security teams can seamlessly deploy and improve the effectiveness of the security and risk management of their organization.

For more information, check out our blog and register for the Ivanti Patch Tuesday webinar series. And listen to the Ivanti Insights podcast, "The Next Evolution of Patch Management: Don't Try to Patch Everything!"

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. i. Smarter with Gartner, Gartner Top 10 Security Projects for 2020-2021, February 22, 2021
2. ii. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.