ivanti

The Ultimate Guide to Risk-based Patch Management

A working reference for IT Ops and security for modern patch program implementations

Executive summary

With over 187,000 security vulnerabilities currently registered in the National Vulnerability Database (NVD)[1]– with an average 61 new vulnerabilities added every day[2] – **organizations can't realistically remediate every potential threat to their systems.**

Moreover, comprehensive considerations of all data available show more than 236,000 total vulnerabilities, with the true threat percentage around 12.4% weaponized by cybercriminals.[3]

Traditional patch management structures don't have this sort of visibility of the complete vulnerability landscape, leaving critical gaps in your cybersecurity coverage.

But even if you knew about every vulnerability possible, how do you decide which of those CVEs should be patched first? When should you interrupt your normal maintenance cycle for the highest priority patch rollout?

Enter: risk-based patch management.

One of the most effective approaches to risk mitigation, risk-based patch management goes beyond basic Common Vulnerability Scoring System (CVSS) scores and scanners to identify and qualify the specific vulnerabilities that pose the most significant risk to an organization's devices, data and end users.

> "Organizations can't realistically remediate every potential threat to their systems."

This extension of risk-based vulnerability management **brings real-world risk context into the patch management process** by incorporating updates with known exploited vulnerabilities that matter most to an organization's security posture.

This approach puts vulnerabilities in context, enabling patch admins to prioritize critical remediation activities and allowing operations teams to understand the urgency of their activities through the same real-world risk lens as security teams.

Risk-based patch management requires additional resources beyond the traditional linear patch prioritization structure, including:

- **Multiple data sources** – both external and internal – which can be dynamically updated and quickly synthesized to produce the information required to identify an organization's unique risks while comparing to known vulnerabilities and patches.
- **A prioritization scheme** which arranges critical vulnerabilities for the organization by their damage potential, known ransomware activity, ease of remediation and more.
- **Enough bandwidth –** either human team members or increasingly automated functionality – to identify, alert and execute on critical vulnerability remediation as they occur.

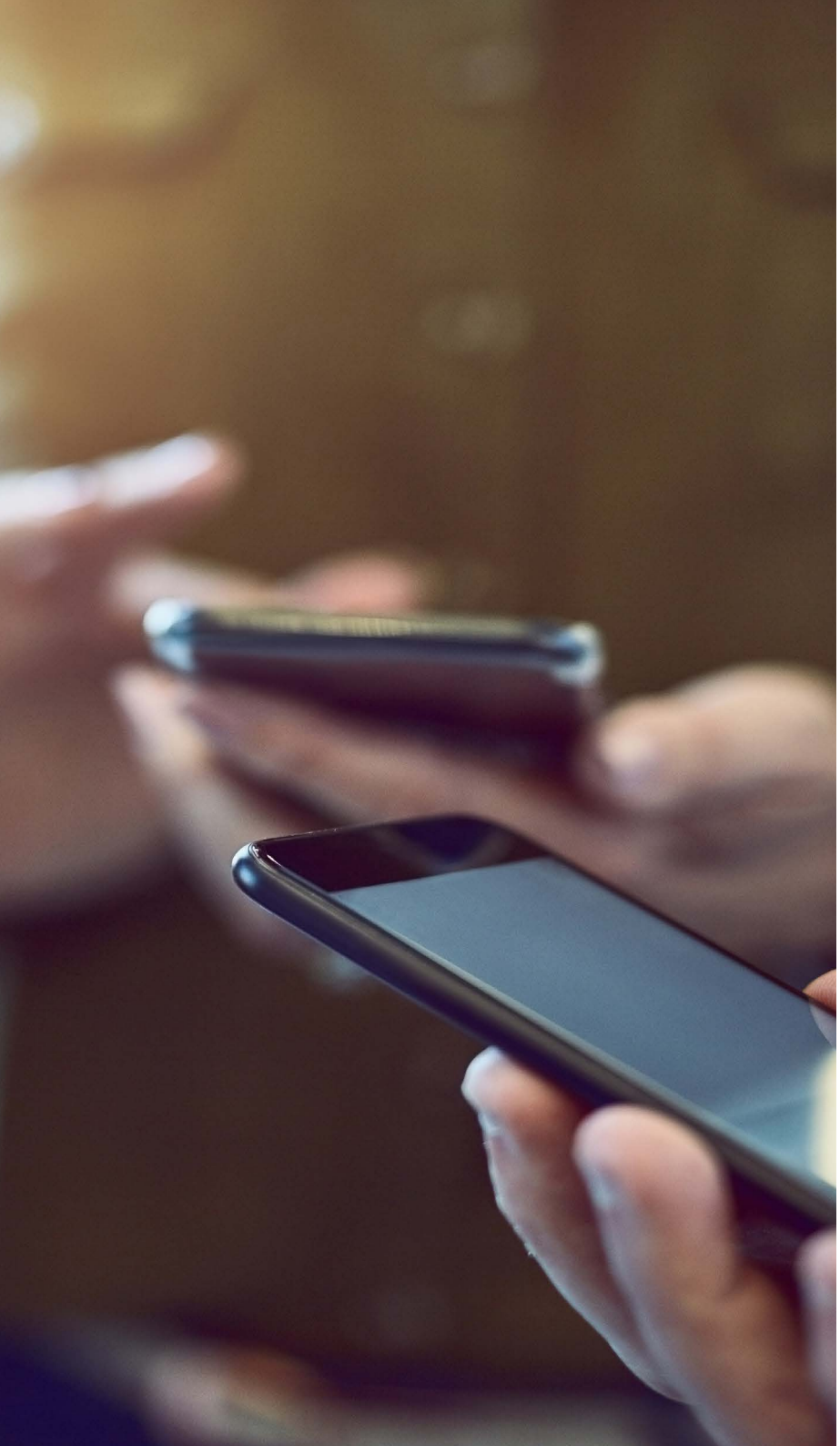


Table of Contents

Critical hours: Too many vulnerabilities, not enough time

The National Vulnerability Database lists over 187,000 vulnerabilities, each with different severity ratings glossing over specific risks to individual organizations.[4]

For those organizations able to expand their monitoring capabilities to cover all possible data sources – including the NVD and CISA databases, industry scanners, bug bounties, penetration testing and various industry research on threat trends – the true number of potential vulnerabilities is over 236,000 as of June 2022.[5]

Of those, 12.4% have known exploits for ransomware and cybercriminals.[6]

Sheer volume alone requires a proactive, prioritized approach to patch management if organizations intend on maintaining consistent security.

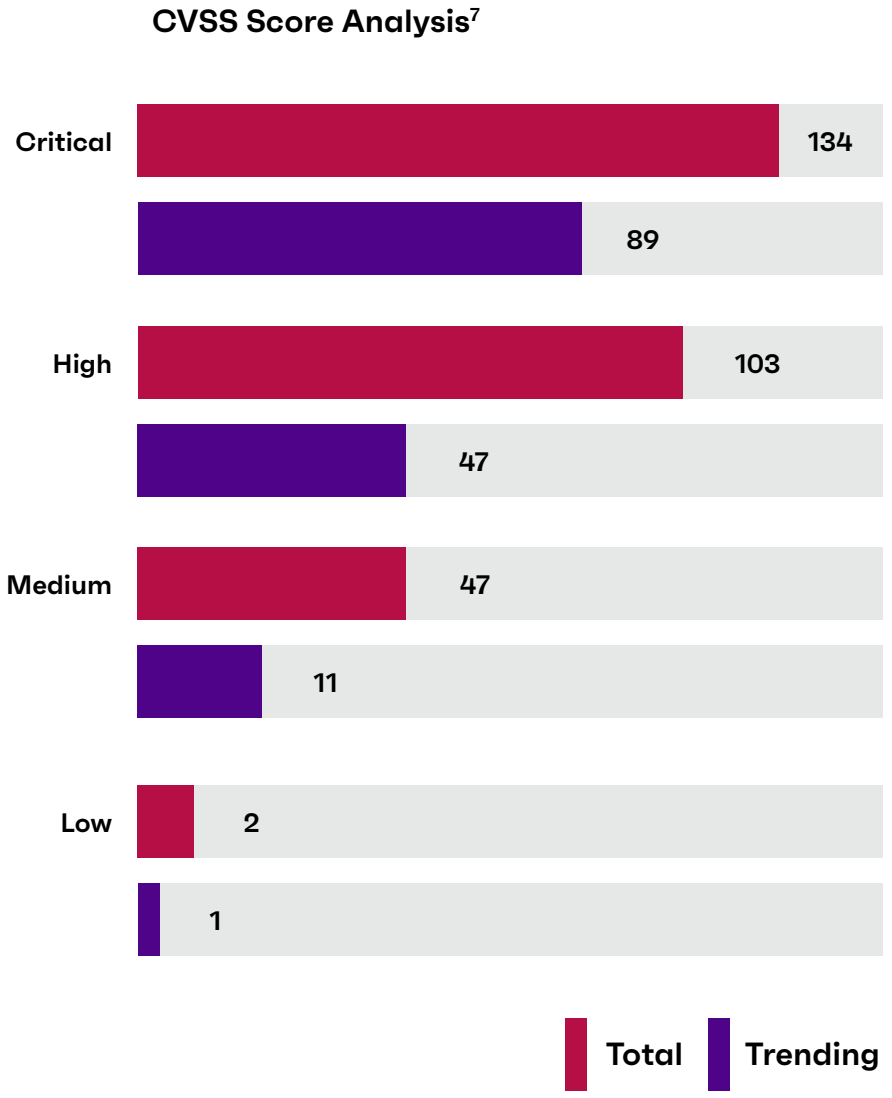
There are over 236,000 known vulnerabilities.

12.4% of those vulnerabilities are actively exploited or otherwise connected to ransomware.

Unfortunately, vendor severity ratings and the CVSS do not provide adequate context to help in-house security teams prioritize which vulnerabilities they should focus on first.

Consider the latest ransomware report from Ivanti[8] which shows:

- Organizations only patching Critical-rated CVEs miss almost 40% of trending vulnerabilities actively in use by ransomware gangs and other cybercriminals today.
- 91% of all active vulnerabilities tied to ransomware are more than a year old.



Without mapping vulnerabilities to real-world ransomware threats – as well as remote code execution (RCE) and privilege escalation (PE) susceptible exploits – it's hard for an organization to prioritize remediation effectively while guaranteeing both security and productivity.

After all, security teams must patch every relevant vulnerability to keep their organization – devices, data and end users – secure.

Cybercriminals only need to get lucky once.

Real World Repercussions:

Microsoft

In 2021, Microsoft[9] resolved 23 zero-day vulnerabilities.

15 of those were only rated as Important – not Critical – patch priorities.

100% of all 2021 zero-day Microsoft vulnerabilities were actively exploited by cybercriminals and ransomware.

The traditional patch management process

Historically, patch management followed a linear, waterfall approach:

1. **The security team's vulnerability scanner or database** detects a new vulnerability in the environment, prompting a CVSS criticality evaluation for high-scoring vulnerabilities to triage remediation.
2. **Meanwhile, patch administrators assess the environment** to find software in need of updates as part of the regular maintenance cycle, assessing critical vendor severity as part of their remediation prioritization – independent of the security team's assessment.
3. **Security teams and patch admins debate patch prioritization** for a reconciled list of critical patches for remediation.
    a. Generally, security's recommendations become prioritized above
    b. the patch admin and IT Ops' vendor-sourced recommendations.
4. **Patch admins find the relevant patches** for remediating the prioritized list of vulnerabilities – if they exist – and ideally test within a sandbox environment before rolling out the fix to the broader organization.
    a. Admins face the reality that test environments rarely encompass every nuance of the living organizational network.
5. **The patch rolls out**, possibly causing shutdowns or crashes as the patch interferes with functionality or interconnectivity with other applications – even if the patch got a clean bill of health with no projected impacts in the sandbox testing round.
6. **The rinse and repeat cleanup cycle begins**, as patch admins and security teams alike review the results of the rollout and identify machines that failed to update – or were completely overlooked in the process.

Challenges with traditional patch management

Anyone who's done patch management will be able to point out the shortcomings with the traditional linear approach. For example, ransomware gangs can exploit vulnerabilities within days of being identified from central databases, shortening the window in which patch admins can identify and remediate the vulnerability before attack.

Several major vulnerabilities last year – such as QNAP, Sonic Wall, Kaseya and Apache Log4j – were exploited before they ever reached the NVD.[11]

of exploits occur within 14-28 days of patch availability[12], with cybercriminals needing only a median of 22 days to develop functional exploits.[13]

Real World Repercussions: BlueKeep[10]

May 14, 2019
CVE-2019-0708 published with patch.

May 15, 2019
Proof of Concept research begins.

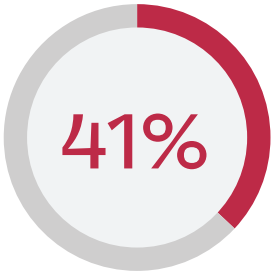
May 20, 2019
BSOD exploit confirmed by research firms.

May 28, 2019
6 independent research firms achieved RCE, with additional confirmed exploits by cybercriminals.

Just 14 days from publication to active exploits by cybercriminals

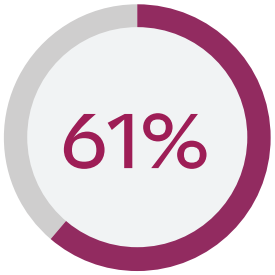
Without additional bandwidth, resources and staff,
patch admins and security teams are forced to rely exclusively on vendor severity ratings and CVSS scoring without further context for their unique risk environment.

53% of surveyed IT Ops and security teams report spending most of their time simply organizing and prioritizing vulnerabilities, not actively patching![14]



A recent international survey found that 41% of surveyed organizations lost IT Ops staff due to high workloads in an incredibly competitive job market.[15]

Misalignment between security and IT Ops goals
often leads to failed patches and lost productivity.



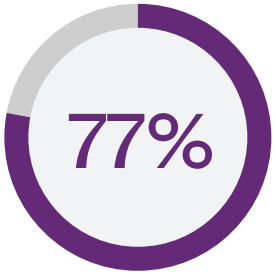
61% of surveyed IT and security professionals receive requests to postpone maintenance windows once a quarter – 28% every month – leaving organizations vulnerable to cyberattacks for perceived "gains" in productivity.[16]

When cyberattacks do hit companies – as they did for 63% of surveyed organizations in 2021 – 38% of those victims lost a week's worth of productivity across the organization; 24% of organizations lost an entire month of work.[17]

Most departments don't have time to test updates or coordinate with other departments before deploying patches.

Only 15% of IT Ops and security teams report spending most of their time testing patches, while just 10% said they spend the most time coordinating with other departments.[18]

Scanners and databases don't catch and publicize all exploitable vulnerabilities.

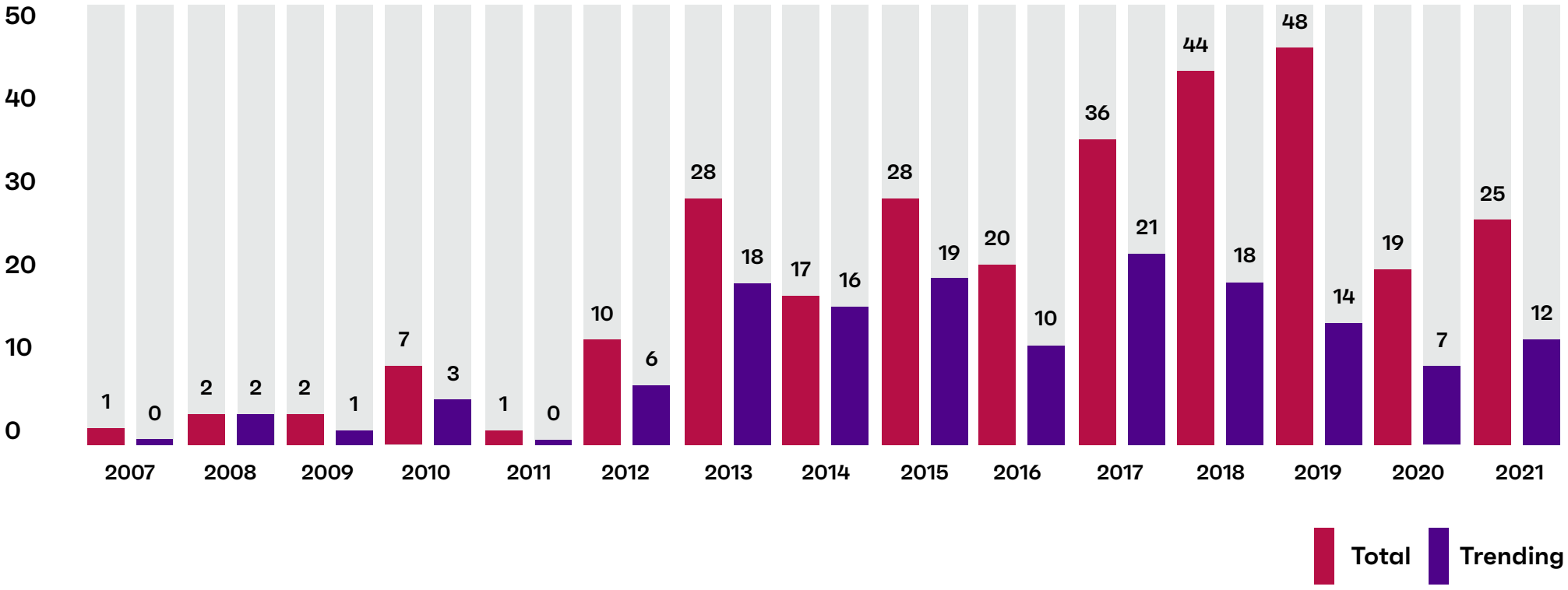


Three of the most popular vulnerability scanners – Nessus, Qualys and Nexpose – detected just 77% of all exploitable vulnerabilities last year.[19]

Cybercriminals and ransomware gangs can still use non-critical or older vulnerabilities in their attacks.

- Organizations only patching Critical-rated CVEs per the CVSS would miss 53% of all exploitable vulnerabilities tied to ransomware.[20]
- 92% of all actively trending vulnerabilities were publicly disclosed before 2021 – with two recently active vulnerabilities first disclosed in 2008![21]
- According to research from the Rand Consulting Group, vulnerabilities continue to be actively exploited by cybercriminals up to 7 years after their initial publication.[22]

Vulnerabilities Tied to Ransomware and Trending by Year of NVD Publication



38%

of victim organizations of cybercrimes lose a week of productivity.

24%

lost an entire month.

Unpatched vulnerabilities continue to be the primary attack vector for ransomware groups. The absence of a swift response can quickly compromise an organization's security environment, significantly impacting its productivity and profitability.

And, with the average total cost of a ransomware breach estimated at $4.62 million[24], an effective vulnerability remediation strategy is crucial for security and IT Ops teams to patch those loopholes and vulnerabilities.

But, patching every vulnerability out there simply isn't a feasible solution for any IT Ops or security team, let alone overworked and understaffed departments.

Patch admins need a strategic plan of attack that maximizes those often-limited resources of time, staff and internal bandwidth while staying ahead of cybercriminals and other threat actors.

Enter risk-based patch management (RBPM).

The average ransomware breach costs an estimated

$4.62m

Risk-based patch management: an overview

A risk-based patch management strategy takes a niched-down approach to patching, rather than attempting to cram an organization's unique risk profile into the "one size fits all" linear patching approach traditionally used.

First, admins collect information from external sources: network scanners, databases like the NVD and CISA, and vulnerability findings from manual research and penetration tests.

They also collect internal datapoints to map out the exact risk profile of the organization's entire IT footprint.

This dataset includes:

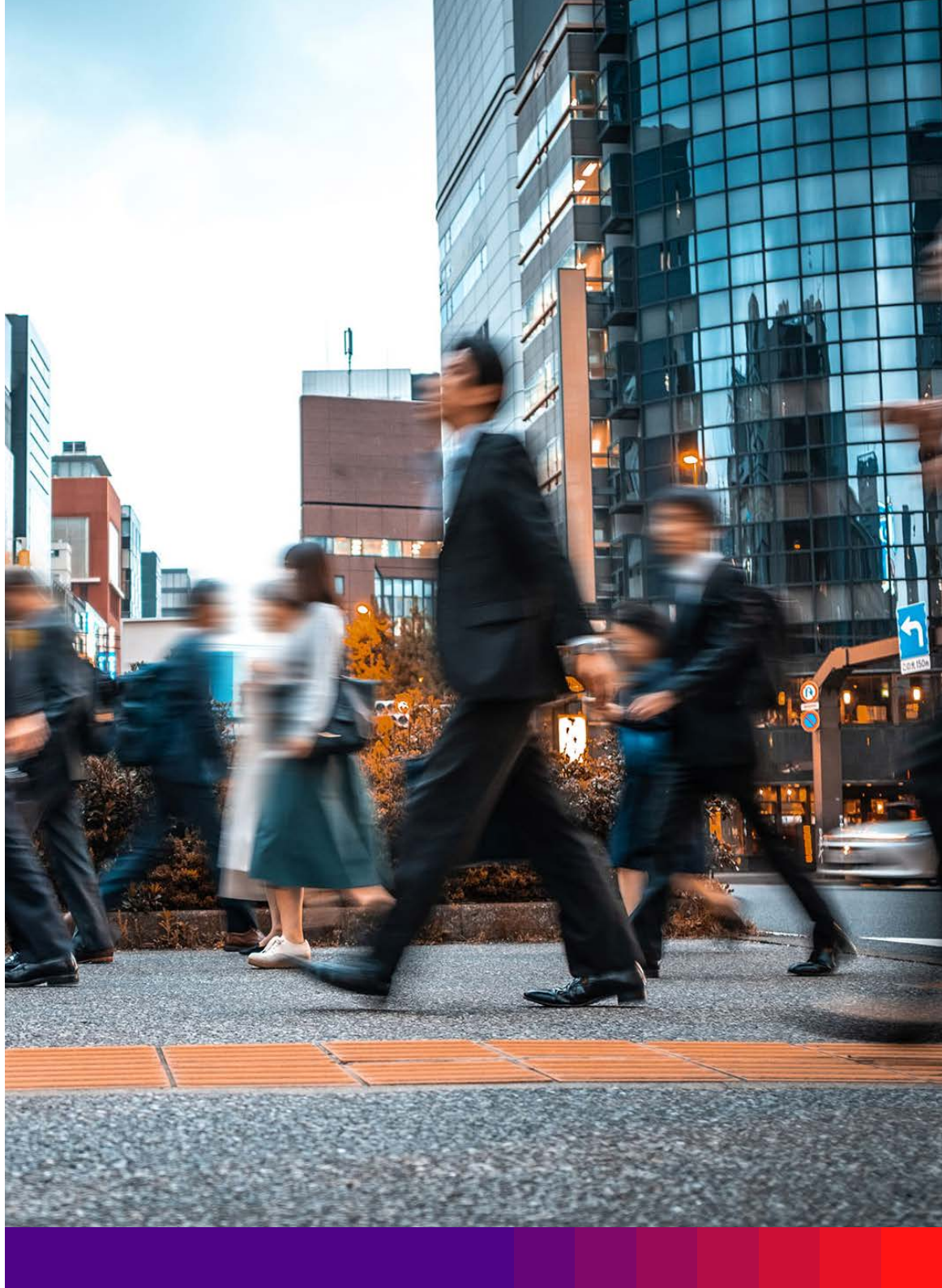
- A list of in-use devices and OS supported by the organization's IT and operations teams.
- Any applications and software currently used by the organization's end users – including both officially installed software *and* user-sourced applications, either downloaded or cloud-based.
- An understanding of how data – both proprietary and customer – is retrieved, where it's stored and how it's used.

By reconciling the external vulnerability and threat information with the internal organization's unique security environment, patch admins can contextualize threat information and prioritize which patches are most mission-critical to the organization, instead of how an external source perceives the threat.

Through RBPM, a small team can handle a continuously growing number of vulnerabilities and keep the organization, its end users and its clients safe without overburdening already stretched IT Ops and security teams.

4 business benefits of a risk-based patch management approach

- RBPM reflects the **pragmatic middle ground** between “patch everything” and “why bother.”
- RBPM offers a **“reality-based” prioritization** for vulnerabilities that’s customized to your organization, contextualized with real-world attack information to determine what truly matters.
- RBPM can be **faster** than a traditional patch management approach.
- RBPM forms a **bridge across departments** for security and IT Ops.



ivanti

1. RBPM encourages a pragmatic – not idealized – approach to patching.

The risk-based method to patch management acknowledges and accommodates the reality in which all admins operate: there are simply too many vulnerabilities and too few resources to keep up with everything.

In 2021, vulnerabilities tied to ransomware increased by 29% YOY.

On the other hand, doing nothing isn't an option, either: unpatched vulnerabilities are the most prominent attack vectors exploited by ransomware groups and threat actors. Last year, vulnerabilities tied to ransomware increased by a staggering 29% YOY.[25]

The optimal middle ground between "patch everything" and "why bother" is RBPM.

The sooner organizations understand that indiscriminately patching everything – even every "critical" CVSS-rated or vendor-rated CVE – is no longer a realistic goal, the faster they can shift to a proactive, updated patch management strategy that will better protect their users, systems and assets.

A proactive risk-based vulnerability program can reduce an organization's data breach incidents by 80%.

And, according to Gartner Research, even if an organization doesn't patch everything, a comprehensive risk-based *vulnerability* management program – which includes RBPM – can reduce an organization's data breach incidents by 80%.[26]

It's a remarkable business improvement for a relatively small philosophical shift.

2. RBPM is a “reality-based” prioritization process that ranks risks through organizational context.

By ranking issues based on ransomware gang behavior and which vulnerabilities they exploit – among other priorities, including RCE and PE potential – organizations’ patch admins can make more realistic evaluations of the possible impact of a vulnerability.

These evaluations consider vulnerabilities not just as an isolated threat, but also in combinations of several exploited together through “vulnerability chaining.”

Vulnerability chaining occurs when ransomware exploits several vulnerabilities at once – often vulnerabilities with mixed severity ratings and ages – to stage a comprehensive attack on an organization.

For example, the 2021 LockFile ransomware attacks chained four total vulnerabilities from Microsoft Exchange and Windows OS:

The “ProxyShell” vulnerabilities

allow cybercriminals to enter an organization’s network and trigger remote code that further additional exploits, as well as install backdoors for later access.

The “PetitPotam” vulnerability

lets attacks burrow even further into an organization’s systems to gain deeper access into more valuable and mission-critical systems.

Organizations that followed only a traditional, linear patch management process would not have patched all vulnerabilities involved in this and similar attacks.

Of the four vulnerabilities chained in the LockFile ransomware, only one was rated as a critical vulnerability for patching – two were simply rated a "medium" importance to patch.[30]

The LockFile Vulnerabilities

Vulnerability	CVSS Score	CVSS Severity	Product
CVE-2021-31207	7.2	High	Microsoft Exchange Server
CVE-2021-34473	9.8	Critical	Microsoft Exchange Server
CVE-2021-34523	9.8	Medium	Microsoft Exchange Server
CVE-2021-36942	5.3	Medium	Microsoft Windows Windows Server 2008, 2012, 2016 and 2019

And, even though the LockFile ransomware attacks first happened in 2021, research reports that over 34,000 ProxyShell exposures still exist online – waiting for a new batch of bad actors to exploit the vulnerabilities.

3. RBPM decreases time to patch vulnerabilities.

The longer a critical exposure remains unpatched,the more exposed a business is to a data breach or ransomware attack.

In 2021, the Department of Homeland Security – via the Cybersecurity and Infrastructure Security Agency (CISA) – issued Binding Operational Directive 22-01.

These new requirements for public-sector organizations reduced patching time for critical vulnerabilities to two weeks and suggested additional adjusted timelines in the case of "grave risk" to an organization's infrastructure.[32]

Incidentally, this CISA vulnerability list of required vulnerability patches feature 20% of all the CVEs currently identified as actively exploited by ransomware families.[33]

So, even for security teams taking advantage of a vulnerability prioritization system to determine the most important patches needed, there are still a ton of vulnerabilities to patch, and not a lot of time in which to patch them.

With traditional patch management methodologies, admins often spend hours researching and determining what actions to take each time they receive a vulnerability report.

The CISA vulnerability list of required patches only covers 20% of all actively exploited vulnerabilities.

By contrast, some modern patch management systems can automatically reconcile vulnerability information with patch data and organizational context. These reconciliations increase visibility into organization-specific risks, speed up the overall remediation process and reduce the remaining cleanup after each maintenance cycle.

In addition, a comprehensive risk-based approach to patch management is also most likely to counter or limit the impact of zero-day vulnerabilities by:

- Simply knowing that the vulnerability does exist, so that a patch – when available – can get prioritized release and rollout on organization systems.
- Developing ad hoc strategies which mitigates impact to potentially vulnerable systems without impeding day-to-day operations.
- Setting up an internal alert system to know the instant a cybercriminal may be leveraging that vulnerability.

By discovering and prioritizing updates to protect the most vulnerable systems within the organization, patch admins make the best use of their resources and protect systems against external cybercriminals and ransomware gangs. Identified by the vendor – often after an exploit attack occurs.

What is a zero-day vulnerability?

A zero-day vulnerability is a vulnerability that is:

- Identified by the vendor – often after an exploit attack occurs.
- Actively exploited by cybercriminals.
- Unable to be patched (or with no patch available).

4. RBPM reduces the natural friction between IT Ops and security teams.

Risk-based patch management creates space for empathy:

The IT Ops team

better understands the security team's priorities and rationale for truly important patches of critical vulnerabilities.

The security team

better appreciates how a bad patch impacts the business, breaks critical applications and causes a surge of user tickets.

When the IT Ops team trusts that the security team is properly prioritizing patches – so they don't waste their or end users' time on every possible vulnerability – IT Ops is more likely to cooperate and proactively find time for security's most important risks.

More broadly speaking, a risk-based vulnerability management process can also educate these teams on what they risk losing if a given vulnerability isn't patched.[34]

Suddenly, the requested patch is no longer resolving just one of many vulnerabilities; the risk is contextualized in terms of department and business outcomes, with end user experience and revenue impacted by a possible breach if not addressed.

The average ransomware breach cost $4.62 million in 2021.[34]

The immediate, short-term inconvenience of finding a few hours to update is outweighed by the longer-term risk of losing a week or more of time due to a ransomware attack.

Likewise, when security isn't trying to cover every loose end at once – just the most important ones – they can be more flexible with their partners in IT Ops to *not* reconcile patches during critical hours, shrink the maintenance cycle and avoid crashing systems with unplanned updates.

Moreover, a modern RBPM platform centralizes data analysis and prioritization in a single accessible location or dashboard, which has several benefits:

IT Ops teams

don't have to wait for security to hand over vulnerability reports. They can see what's most important to their organization from the dashboard and immediately start testing updates in a clean environment to improve response time, including mapping relevant CVEs to internal environments.

Security

can see at a glance patch rollout status, possible bottlenecks and patches still in the backlog to address in a future sprint or maintenance cycle.

In RBPM, the process becomes one of mutual reconciliation – not constant interruption.

ivanti

Can you run a manual risk-based patch management program?

Risk-based patch management is the natural alternative to trying to patch everything, but it's far from being a straight forward process.

(After all, if it were easy to implement, this guide wouldn't need to exist.)

Setting risk-based priorities and tracking vulnerability shifts in real-time – not to mention proper testing and patch rollout – quickly overwhelms unprepared teams trying to tackle RBPM manually, rather than through explicit tools or automated processes.

For example, let's say an organization wants to implement an RBPM strategy. To avoid getting overwhelmed by too many data sources, they choose to only focus on the NVD, which added an average of 61 new vulnerabilities every day last year.[35]

As part of their RBPM philosophy – which requires new vulnerabilities to be contextualized with the possible attack surface internally, and not simply leaning on an external assessment of criticality – the team must manually review all 61 new NVD vulnerabilities daily to make 61 separate prioritization calls.

(The Monday backlog would be *terrible* on that team.)

And, our hypothetical company is just referencing a single, albeit comprehensive, data source.

That's to say nothing of the flood of raw vulnerability information that could be available to them from other databases, research and reports.

Real World Repercussions:

Vulnerability & Patch Reconciliation

In conversations with Ivanti experts, IT Ops and security teams at companies around the world anecdotally report that their traditional vulnerability and **patch reconciliation reports take at least 8 hours to complete by hand.** Professionals working on these manual reports admitted that they knew the final document – while critical! – would not be 100% accurate.

However, for the sake of argument, let's say that our organization has enough security and IT Ops staff to directly monitor large vendors such as Microsoft, Apple, Linux and other app providers regularly to find vulnerabilitiesand exploits as soon as they're disclosed.

There are even places online – such as PatchMangement.org, Reddit and the Ivanti Patch Tuesday Webinar – which curate particularly relevant vulnerabilities. These and other industry websites are certainly great resources to help teams navigate this portion of the RBPM process for free!

However, monitoring is just one of multiple tasks that need to be completed before the end of the patching cycle.

As part of the RBPM process, our hypothetical organization's security & IT Ops teams still need to:

- Identify all internal devices and applications – IT-sanctioned and user-installed.
- Determine which end users and use cases get patches first.
- Test the patch across all variations and variables – or as many as is practical for the specific vulnerability.
- Schedule and execute the patch rollout.

Especially for hybrid or fully remote workplaces, these procedures can escalate into never-ending processes that can't keep up with the speed of reality.

Last but not least, many manual systems use spreadsheet-type documentation and database reconciliation.

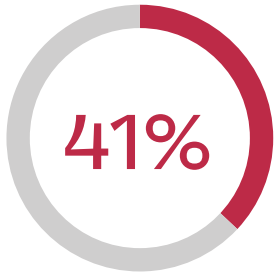
However, reliance on spreadsheets simply opens the door to mistakes. The more people you have frequently adjusting the same report, the more likely you'll end up with errors that snowball into costly delays and corrections.

In fact, one study found that 88% of all spreadsheets have "significant" errors – the majority caused by the very people working on them![36]

of all spreadsheets have "significant" human-caused errors.

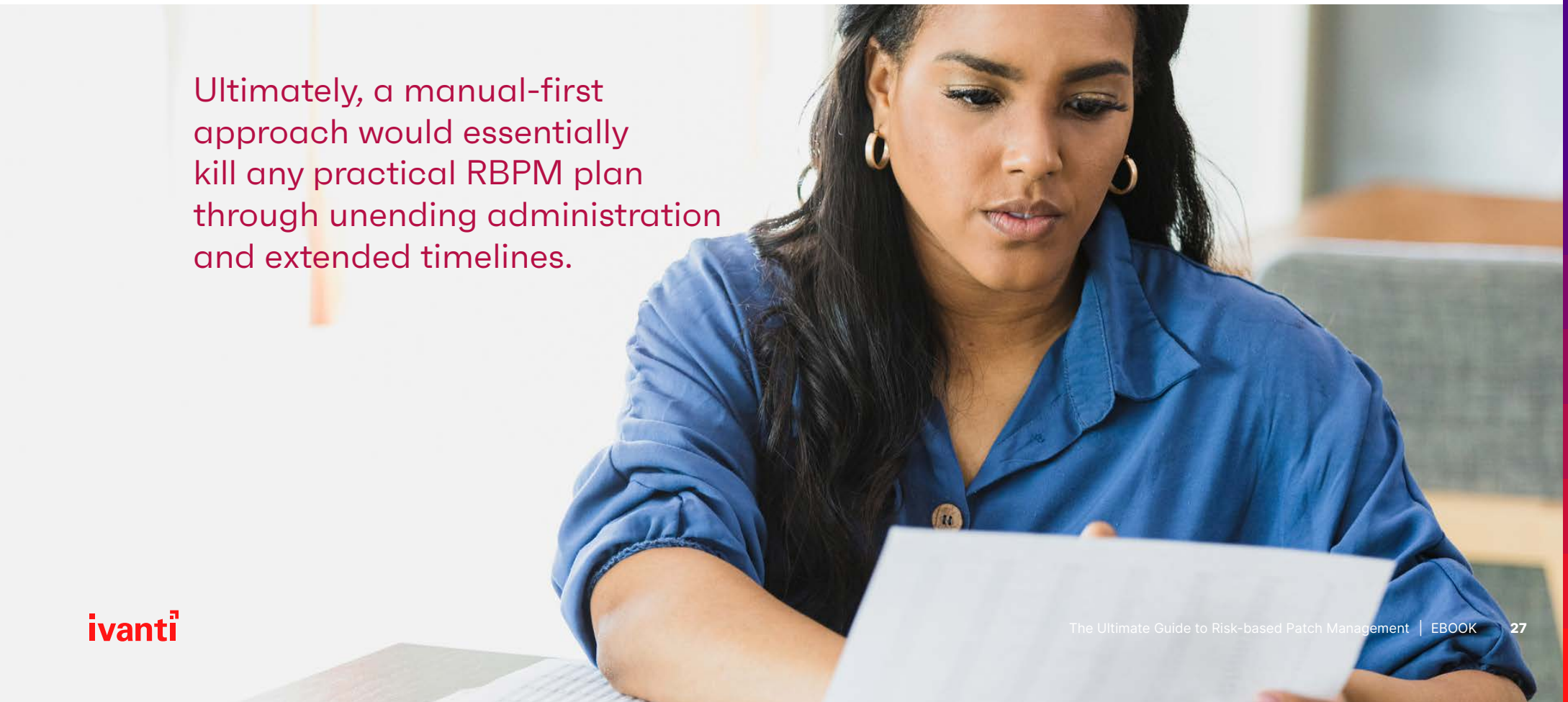
So, while manually executing a risk-based patch management strategy is certainly possible – particularly at the start, to get a feel for the approach and before purchasing dedicated tools – it wouldn't be the optimal configuration for teams who truly wish to embrace the RBPM philosophy.

Adding more manual labor at a time when 41% of surveyed organizations report losing IT staff due to high workloads seems unwise, too.[37]



of surveyed organizations report losing critical IT staff due to high workloads.

Ultimately, a manual-first approach would essentially kill any practical RBPM plan through unending administration and extended timelines.



5 best practices for your risk-based patch management program

1. You can’t patch what you don’t know about.
2. Get IT Ops and security reading off the same sheet of music.
3. Work in parallel through an internal SLA.
4. Set up pilot groups.
5. Use automation!

ivanti

1. Figure out what you currently have and how you use it.

You can't protect or patch something you don't know exists. Therefore, asset discovery – finding out what you have, with which end user profiles – plays a critical role in any vulnerability management initiative.

Asset management for RBPM

Modern asset management tools can help organizations understand and track their current tech stack. It starts with identifying all the devices – laptops, desktops, phones, tablets, servers and network devices – and software operating within the organization.

Just like with the broader patch management program, information about your assets will come from multiple sources, such as:[38]

- ☐ Microsoft Endpoint Configuration Manager (SCCM) and Microsoft Intune
- ☐ CSV files or spreadsheets
- ☐ Microsoft Active Directory
- ☐ Workspace One (AirWatch)
- ☐ Ivanti Neurons for Discovery

After listing all the assets, you'll need to eliminate duplicates and ensure all data is consistent within the database.

Last but not least, asset managers in IT Ops will organize the records, enabling patch admins to find the most critical terminals and any potential weaknesses – information that will help prioritize your patches.

Service mapping for RBPM

As an extension of the discovery process, service mapping can help you find the systems which need to be managed and secured, highlighting how they – and the data they use – are interconnected and accessed.

Service maps may contain:

- The infrastructure and hardware inventory.
- Applications, configuration documentation and a software library that lists the most recent versions of used software.
- Settings and network diagrams, which will highlight information flows and how devices connect throughout the organization.
- End users, user profiles and any high-risk terminals, as well as the level of impact each can have on the organization's critical system if compromised.

Security teams can then map the path an attacker might take through a vulnerability to reach a critical system by the connected user systems or applications.

Simultaneously, the IT Ops team gets an understanding of how many systems may connect to a mission-critical application, providing essential information on how to best configure and implement patch tests.

2. Ensure everyone can access the same information.

Risk-based patch management efficiency depends on how well your IT Ops and security teams all work together to synchronize their interventions. To do so, they'll probably need help aligning cross-functionally to achieve all their goals.

Theoretically, all teams should be working towards the same goal: a secure organization that can do its work without interruption from cyberattacks.

Practically, their objectives seem diametrically opposed: security seeks to mitigate risk, while IT Ops wants to optimize end user performance and experience.

The security team

used to treat everything as a risk, often with no practical way of identifying the relevant threats to the organization and with little awareness of how patch rollouts impact day-to-day work.

The IT Ops team

must balance their end user service-level agreements (SLAs) to keep regular work proceeding as scheduled against a theoretical threat of potential ransomware that never seems to let up.

A great RBPM system will seek to ease this natural point of friction through shared information and mutually understood risk analysis:

Security

will only prioritize those vulnerabilities that truly matter to the organization's cybersecurity posture.

IT Ops

can see for themselves how the vulnerabilities might impact their end users in real-time, and so are more willing to make time for rollouts.

3. Work in parallel to reduce time to patch through an RBPM SLA.

In a best-case scenario, a risk-based patch management solution makes all involved parties aware of vulnerabilities and how to counter them in real-time.

IT Ops and security teams would use and understand the same methodology to prioritize risk, so they can run in parallel and sync at multiple points during the remediation process to ensure they stay in agreement on what needs resolution.

This approach can reduce the maintenance cycle from weeks to days or hours, depending on how critical the vulnerabilities are – and how in sync each team is with their cross-department partners.

The IT Ops and security teams all must establish internal best practices and together agree on maintenance windows which consider the goals of each team, as well as overall organizational goals.

To that end, consider creating a service-level agreement for patch management between the IT Ops and security teams.

Creating your SLA

This SLA should define collaboration expectations and timeframes for each step, so everyone knows what will happen, when and from whom.

The SLA should incorporate:

- **All definitions** – even for something as basic as what a "vulnerability" means!
- **Necessary specifications** and deployed tech stacks for each stage.
- **Vulnerability prioritization criteria.**
- **Communication frequency** during the patching cycle.
- **Explicit exceptions** for when vulnerabilities must be remediated out-of-band and/or out of the regular maintenance cycle.

Particular attention should be paid to setting achievable and realistic key performance indicators (KPIs) for all involved departments, with shared KPIs wherever possible.

Real World Repercussions:

Patch and Vulnerability SLAs

One large global manufacturer with over 100,000 devices told Ivanti they implemented a vulnerability SLA between their IT Ops and security teams.

Their organization has since attained a 95% vulnerability remediation compliance rate within their SLA-dictated 2-week timeframe.

4. Set up pilot groups with key stakeholders for patch prioritization and testing.

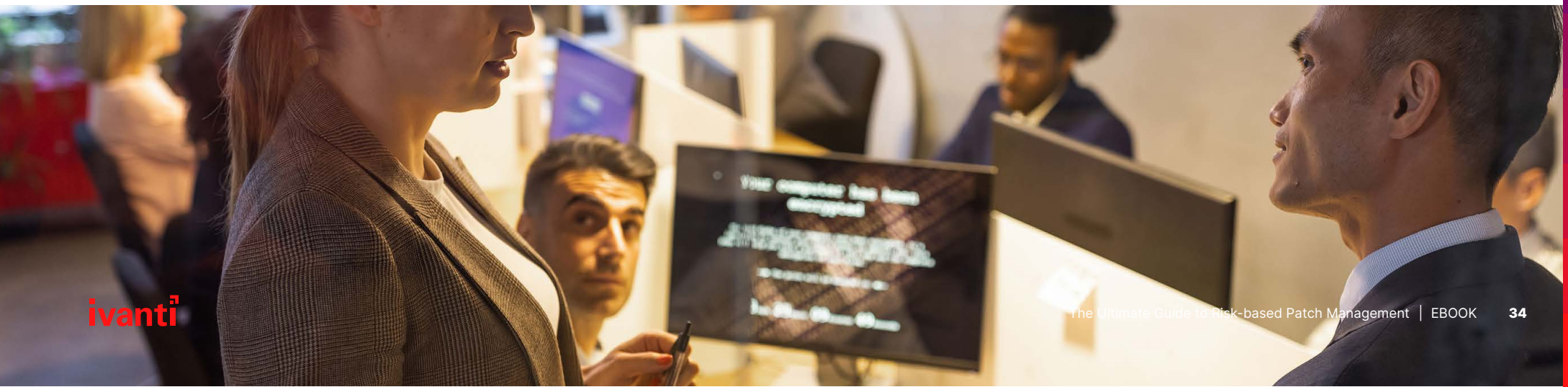
Pilot groups are predetermined (and pretrained) groups of representative user roles and device configurations that can test vulnerability patches in a live environment before they're rolled out to the organization at large.

After all, if a patch is going to crash mission-critical software, then it's better to know on a few machines rather than shutting down the entire organization.

Pilot groups supplement controlled test lab environments to better predict how patches may impact business activities.

Since test systems rarely determine downstream impacts, having one or more pilot groups for a patch rollout is critical to reducing the potential for negative operational effects.

"After all, if a patch is going to crash mission-critical software, then it's better to know on a few machines rather than shutting down the entire organization."



Winning buy-in for pilot groups

This best practice requires your patch admins to have buy-in from the entire organization – beyond just IT Ops – as relevant pilot groups should include any crucial application group or department where mission-critical systems may be in place.

To that end, **go beyond IT's service map and ask target user groups directly** about how their devices and data interact with each other,as well as how each update could impact their usual processes.

You'll win reputational points for asking *before* another patch accidentally shuts down their applications during business hours again. Plus, the connections you make will form the basis of future pilot groups, including invested stakeholders who will proactively offer help and insights you wouldn't have otherwise.

ivanti

Creating your patch pilot groups

Pilot groups should:

- **Be organized** into at least one initial “primary” pilot group – to make sure nothing major is broken – with extended pilot groups to identify rarer or application-specific issues.
- **Consider the organization’s objectives** and the specific goals that all involved departments – that is, IT Ops and security – target.
- Communicate feedback at any time.
- **Represent** all devices used within the organization to identify any patch compatibility issues.
- **Consider all user profiles** (also known as “user personas”) in the organization’s environment.

Employees and stakeholders – regardless of their participation in pilot groups – must understand why patching vulnerabilities is critical to reducing the risk of ransomware and other cyberattacks.

The message should be clear: testing is vital to keep the organization and your work safe. Putting up with a little inconvenience on your assigned device as a pilot group test subject means that you’ve saved the entire department from a critical outage.

Real World Repercussions:

PrintNightmare[39]

In June 2021, a researcher discovered an RCE vulnerability within the Windows print spooler.

- When Windows released a print spooler vulnerability patch that June, the researcher thought their specific exploit had been resolved and published their findings… only to discover Windows had patched a different vulnerability.
- Cybercriminals quickly leveraged that research, with active exploits allowing threat actors to remotely take over a victim system at admin-level permissions.
- The first PrintNightmare exploit was patched on July 1, 2021, with a quick re-release on July 16, 2021.
- Since then, several more print spooler patches have released – May 2022 saw another four.

Many organizations now prioritize these patches for remediation and pilot group testing, due to excessive operational impact.

June 2021
Research discovers Windows print spooler vulnerability.

July 2021
Windows releases first PrintNightmare patches.

June 2021
Windows patches different vulnerability; researcher publishes findings.

May 2022
4 more print spooler patches released.

5. Use automation – especially for rollouts.

Automation offers a great advantage to risk-based patch management programs, particularly when it comes to the collection, contextualization and prioritization of external vulnerability reports.

As we touched on earlier, trying to pull off an RBPM program manually would be difficult to maintain, to say the least – not to mention damning on your staff retention metrics.

However, **automation can also help segment a patch rollout** to ensure the project runs smoothly while patching at scale.

Best practices for automated patch rollouts

Automation rules and gates can enforce best practices around test systems, pilot groups and expanding rings of production groups to create a patch management experience that speeds execution while minimizing business impact.

Consider starting your automated patch rollout with your smaller primary test group. Then, expand to:

1. **An initial pilot group** of your active environment.
2. **Early adopters,** who make up about 10% of your environment.
3. **The remaining majority** organization end users.

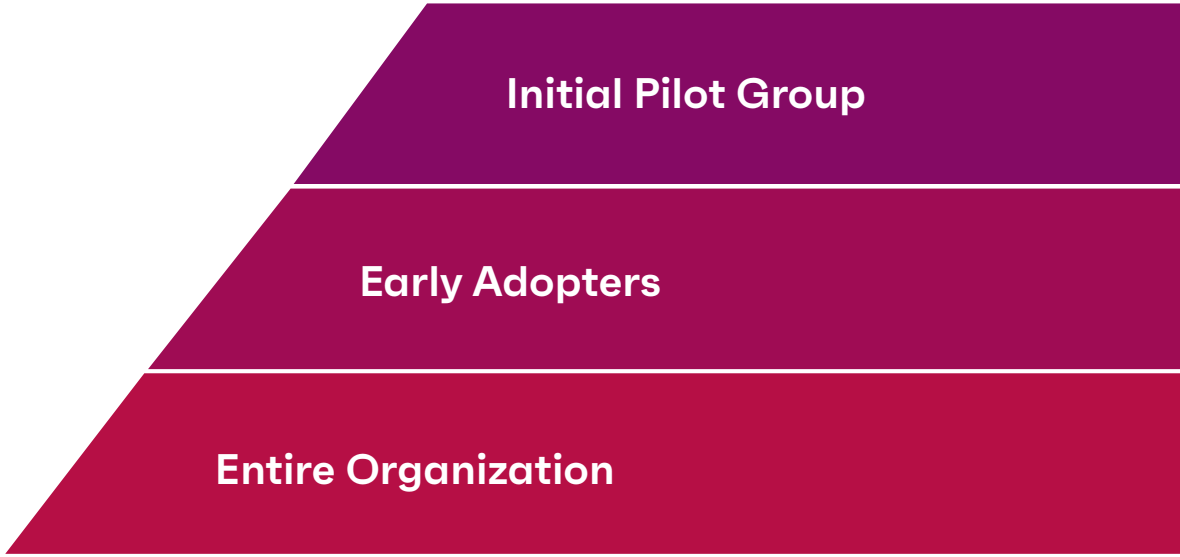
For this use case, patch admins can set up criteria and assign each end user a specific role in each separate group as part of a complete patch rollout. Automation will then govern who gets the patch and when they'll get it.

Patch admins can program the automated process to operate with complex rules and acceptance criteria, such as requiring a specific success response rate or direct user feedback to trigger a new rollout stage.

Advantages of automated maintenance

Automation can handle regular maintenance, leaving staff from all departments with more time to improve collaboration, support a consistent reconciliation process and address exceptional threats when they arrive.

IT Ops and security can even co-develop and configure automated security controls, allowing the security team to run and oversee smaller containment activities which activate on predetermined triggers without relying on the IT Ops team for every task.

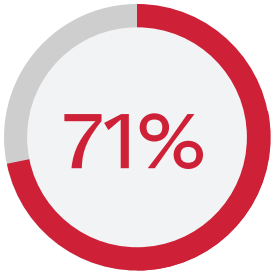


Choosing a risk-based patch management provider

71% of IT and security professionals find patching overly complex and time-consuming[40], primarily due to a lack of adequate tools to support their patch management strategy.

Before implementing a risk-based approach, evaluate your current vulnerability and patch management processes. Security and IT Ops teams must align on goals for the project and agree on the metrics to use.

Specifically, both teams must agree to use the same risk-based approach and ranking system that employs more than vendor severity and CVSS scores to prioritize updates.



of surveyed IT and security professionals consider patching to be complicated and time-consuming.[41]

Your next risk-based patch management platform should include:

- ☐ **Data** from network scanners, endpoints, databases, manual findings, IoT devices and other independent sources to provide a deep level of insight.
- ☐ **Heterogenous support** that covers all internally supported operating systems.
- ☐ **Threat insights** around what vulnerabilities are tied to ransomware or are exploitable RCE or PEs, coming from both human-generated sources and other threat intelligence.
- ☐ **A clear risk rating system** – either automatic or customizable on set-up – that considers the intrinsic attributes of the vulnerability and real-world threat context for accuracy and relevance.
- ☐ **Consideration for unique risk factors** based on your organization's assets, multiple threat intelligence sources and external accessibility.
- ☐ **Automation capabilities** – or integration with automation networks – for remediation and risk monitoring.
- ☐ Alerts and notifications that can be sent to specific user profiles, based on user need and urgency.
- ☐ **Ready-made and / or customizable dashboards** to quickly share the relevant information with the correct stakeholder without waiting for email forwards or chain reminders.
- ☐ **Threat-based, customizable filters**, showing how exploited vulnerabilities manifest themselves in an organization's specific environment.

Referenced Sources

1. The National Vulnerability Database, accessed in May 2022
2. The Ransomware 2022 Spotlight Report
3. 48,285+ Vulnerabilities Beyond the NVD: An Ivanti Research Update
4. The National Vulnerability Database, accessed in May 2022
5. 48,285+ Vulnerabilities Beyond the NVD: An Ivanti Research Update
6. 48,285+ Vulnerabilities Beyond the NVD: An Ivanti Research Update
7. The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
8. The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
9. The Problem With Patching Only Critical Vulnerabilities: A Microsoft Zero-Day Vulnerability Case Study
10. Everything You Need to Know About BlueKeep
11. The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
12. 2016 Data Breach Investigations Report
13. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits
14. Patch Management Challenges: Survey Results and Insights as Organizations move to the Everywhere Workplace (2021)
15. Top IT Trends for the Everywhere Workplace (2021)
16. Patch Management Challenges: Survey Results and Insights as Organizations move to the Everywhere Workplace (2021)
17. 7 Ransomware Trends You Need to Know About (2021)
18. Patch Management Challenges: Survey Results and Insights as Organizations move to the Everywhere Workplace (2021)
19. The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
20. Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
21. Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
22. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits
23. Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
24. IBM Security: Cost of a Data Breach Report 2021
25. Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
26. Implement a Risk-Based Approach to Vulnerability Management
27. Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
28. Microsoft Exchange ProxyShell and Windows PetitPotam vulnerabilities chained in New Attack
29. Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
30. Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
31. Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
32. Binding Operational Directive 22-01- Reducing the Significant Risk of Known Exploited Vulnerabilities
33. Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
34. IBM Security: Cost of a Data Breach Report 2021
35. Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
36. Pank, Raymond R. "What We Know About Spreadsheet Errors." Journal of Organizational and End User Computing (JOEUC) 10, no.2: 15-21. http://doi.org/10.4018/joeuc.1998040102
37. Top IT Trends for the Everywhere Workplace (2021)
38. Why IT Asset Management is Like Building a Jigsaw Puzzle
39. May 2022 Patch Tuesday
40. Patch Management Challenges: Survey Results and Insights as Organizations move to the Everywhere Workplace
41. Patch Management Challenges: Survey Results and Insights as Organizations move to the Everywhere Workplace

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com

About Ivanti Neurons for Patch Management

Ivanti Neurons for Patch Management is a cloud-native patch management solution with actionable intelligence on active risk exposure, patch reliability and device compliance, health and risk that helps organizations better protect against threats, including ransomware.

ivanti

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