tines

Essential Guide

Unlocking IT agility with automation

Vol 1: Patch management

Contents

Foreword
Alexis Perry
Senior IT Systems Engineer, Tines

Readers will likely remember when a key software supplier to the UK's National Health Service (NHS) was struck by ransomware. Critical healthcare and triage services were disrupted, doctors were unable to access medical records, and personal information on tens of thousands of people was stolen. The supplier in question was **subsequently fined**[1] over £3m ($4m) by the data protection regulator.

Among several contributory factors identified by the regulator was a failure to patch a two-year-old Microsoft vulnerability.

Unfortunately, this tale is not uncommon. But while it highlights the serious financial, reputational, and compliance risks that can stem from insufficient patch management, it also doesn't tell the whole story.

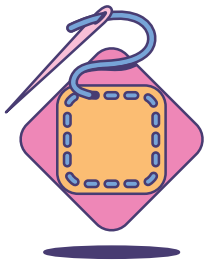
The number of CVEs (common vulnerabilities and exposures) IT teams face can be truly overwhelming. Microsoft alone released 1,360 in 2024; **a record high**[2]. Manual processes, testing and compatibility issues, and the ramifications of system downtime combine to create a formidable roadblock to consistent, streamlined patching.

The good news is that patch management doesn't have to keep IT teams up at night. By automating and orchestrating patching workflows, teams can achieve greater efficiency, consistency, and control. The right tooling and processes can also bring your security and IT teams closer together to manage and patch vulnerabilities in a way that significantly reduces risk and improves the end-user experience.

It's possible to take pain out of patch management – and replace it with a more thoughtful and sustainable approach that strengthens both IT operations and your organization's security posture.

Patch

management



A growing challenge with growing consequences

Patch management is critical to the smooth and secure running of your organization. At a very high level, it helps to keep threat actors at bay and employees focused on their work. Unfortunately, though, it's not getting easier.

Today's IT environments are more complex than ever, thanks to wave upon wave of digital investments and M&A activity. This has created an untidy mix of legacy and next-gen tech sitting side by side. One study[3] suggests that almost three-quarters (70%) of global organizations now follow a hybrid cloud model, and even more (86%) use multiple cloud providers.

The services they support are also under tremendous pressure to deliver. Consumers exited the pandemic with heightened expectations of their digital experiences. And they demand the same of enterprise IT.

At the same time, regulators are increasingly turning up the heat on IT and compliance teams. Some, like PCI DSS 4.0 and NIS 2, are more prescriptive about their patch management demands. Others, like the GDPR, specify "appropriate technical and organizational measures" to keep personal data and systems secure.

The bottom line is this: fail to take control of patch and configuration management, and you could expose the organization to vulnerabilities, system outages, and regulatory compliance violations. Just one missing update can lead to a catastrophic security breach.

For most IT teams, this means that automation and orchestration are no longer optional. As CVE volumes and the number of IT assets continue to rise, teams of all sizes struggle to handle patch management manually. This guide highlights where current approaches fail and how an automated approach that enables an IT team to shift left can help.

We'll share real-world success stories and pre-built workflows from Tines customers to help you move toward a more efficient, secure, and scalable patch management strategy. Let's dive in.

The problem

Fragmented tools, manual effort, and inconsistent patching

Why is patch management so painful? Several root causes stand out:

Inconsistent patching across environments:

The UK ICO regulatory report cited above bemoans the healthcare supplier's "ad hoc" approach to patching. Inconsistency creates risk, especially when threat actors are getting better at automatically scanning for unprotected and exposed IT assets.

Reliance on manual processes:

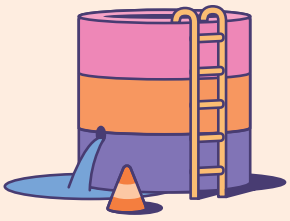
The volume of CVEs and IT assets in modern organizations makes manual tracking and intervention almost impossible to carry out effectively. It increases the chances of mistakes, inconsistencies, and delays, as well as making it more challenging for your IT team to prioritize patches.

Tool fragmentation:

Multiply the number of tools involved in patch management and you increase the chances of information silos, visibility blind spots, and administrative overheads for IT Ops.

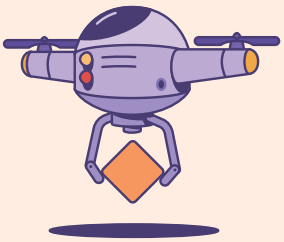
Visibility gaps and lack of audit trails:

Without continuous visibility into IT assets, software inventory, and patches, your teams are in the dark. Limited audit trails compound the problem by making accountability, compliance, troubleshooting, and process improvement that much harder.



End-user resistance:

One of the toughest patch management challenges is keeping employees on side - and maintaining IT's internal reputation. When end users delay or skip updates, they expose the organization to unnecessary risk. This resistance is often rooted in company culture, so driving meaningful change can take time.



The opportunity

Automate securely to streamline patching and reduce manual effort

There *is* a better way of managing updates, focused around:

Centralized orchestration of patching workflows to cut through complexity, unify visibility, and enhance efficiency

Automated triage, approvals, and escalations to improve prioritization, reduce alert fatigue, and accelerate response times

Full visibility across systems, timelines, and compliance to eliminate inconsistencies, improve decision making, and drive proactive patch management

Secure-by-design workflows that scale across environments with a more standardized and automated approach

"Automation is being used to push that next step – automatically seeing things as they come in from various data sources, taking that remediation item, and scanning, alerting, and even patching in real-time in some cases. Companies are looking more and more for automation platforms like Tines to handle these threats in real time, to make not only their automations, but also their infrastructure and their services a lot more resilient."

JOSH MCLAUGHLIN, SECURITY ENGINEER II, LIVEPERSON

The impact

Vibility, agility and efficiency

With this approach, IT Ops can achieve six key wins;

Increased operational efficiency

Deliver faster service to the business by removing bottlenecks

- Accelerate service delivery by eliminating manual, time-consuming tasks
- Refocus IT teams on strategic, high-impact initiatives
- Boost end-user productivity with faster fixes and timely communication

Improved stability and continuity

Keep employees productive with fewer disruptions

- Standardize patching to reduce outages and performance issues across environment
- Run updates during off-peak hours to avoid downtime during business-critical operations
- Use consistent, automated workflows to prevent errors that frustrate end users

Greater business agility

Enable faster response to emerging threats with minimal user impact

- Respond quickly to vulnerabilities before they affect business operations
- Strengthen your organization's resilience without compromising employee experience

Better visibility and alignment

Build trust with clear communication and shared context

- Provide transparent reporting for audits, leadership, and business stakeholders
- Align IT and security teams with shared data, improving coordination and response

Scalable, mature processes

Support growth without increasing risk or complexity

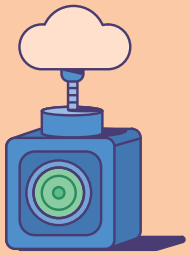
- Establish a repeatable, dependable patching foundation as your business scales
- Confidently expand infrastructure without degrading user experience

Stronger end-user trust and collaboration

Preserve productivity and build goodwill with minimal-disruption updates

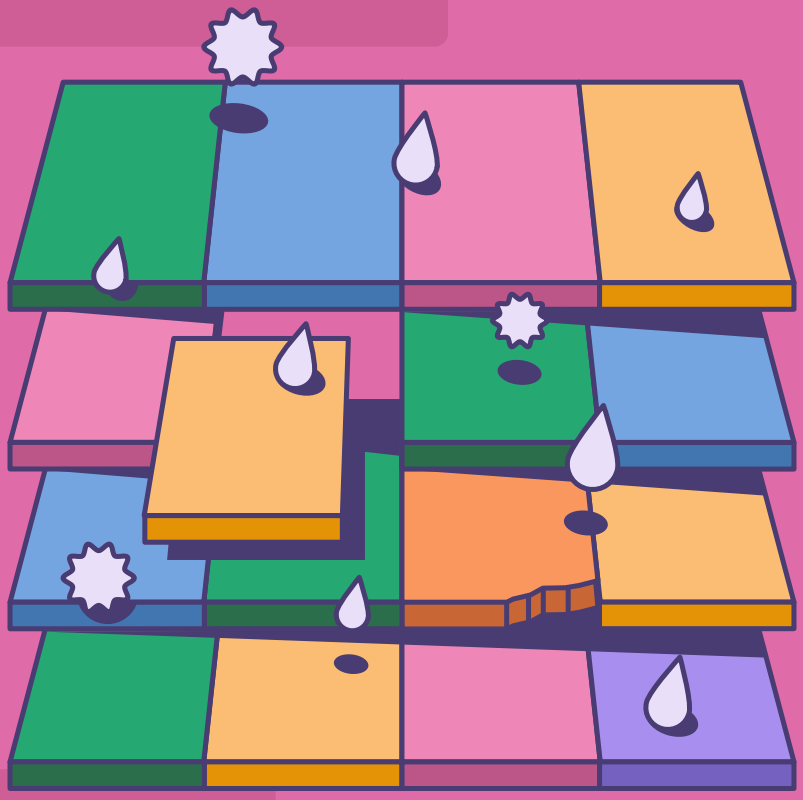
- Roll out changes in a way that respects employee time and workflows
- Improve IT's reputation as a strategic, business-aware partner – not a roadblock

“Having worked on both the IT and security side, I know that both teams have frustrations. But it’s important to realize that vulnerability management and patch management are two sides of the same coin. Security can’t necessarily dictate what vulnerability management means to a company, but we can provide feedback and give our best estimate, and give leadership the information to make those policy decisions. At the end of the day, it has to be a collaborative effort.”



JOSH MCLAUGHLIN, SECURITY ENGINEER II, LIVEPERSON

What *good* looks like



All of this sounds great in theory, but what does it look like in practice? Consider how these Tines customers use the platform to transform their patch management processes.

Crowdfunding tech company

Case study Crowdfunding tech company

"In the first 45 days, we saw our unpatched vulnerabilities drop by 50%, which I've never seen anywhere I've worked."

THIERRY PELISSIER, SECURITY ENGINEER

BEFORE TINES

The company was exposed to persistent security risks and noise from unpatched vulnerabilities reported by its EDR tool.

AFTER TINES

Tines reduced unpatched vulnerabilities by 83% in the first 90 days, from 3,000 per month to just 500.

Key workflow: Exposure management workflow

This workflow identifies medium or critical severity vulnerabilities in third-party software that have been flagged by the company's EDR platform and have been unpatched for 30+ days. Once a week, it sends a Slack message to users of affected machines with patching instructions and a deadline to complete the update by the end of the week. The message also includes a direct link to the security support channel for any questions or troubleshooting.

→ Read the full case study: tines.com/case-study-patching

myfitnesspal™

Case study MyFitnessPal

MyFitnessPal uses Tines to automate and manage its patch management process at scale.

BEFORE TINES

MyFitnessPal's patching process required automation to help scale and better manage macOS updates across the organization.

AFTER TINES

The team introduced a self-service, tiered workflow, streamlining update rollouts and reducing manual coordination.

Key workflow: macOS software update workflow

This workflow helps organizations streamline the complete lifecycle of managing macOS software updates. It features a self-service model allowing users to opt in or out of the patch management pilot group via Tines pages, along with a tiered approach for distributing macOS updates. Initially, updates are deployed to the pilot group for testing and, after one week, are automatically rolled out to the production environment.

→ Get the pre-built workflow: tines.com/qmetz

Case study
Reddit

"For patch management, one of the things we're working on is a nudge bot that will prompt you in Slack if you haven't installed (the updates)... If we don't get a response, we can go up the chain."

CIAN GEOGHEGAN, STAFF CORPTECH SYSTEMS ENGINEER
REDDIT

THE GOAL

Enforce patching in a consistent, repeatable, and documented way, without creating friction between IT and employees.

THE SOLUTION

The team is building a Tines workflow that sends targeted Slack prompts to employees, enabling patch enforcement in a way that maintains a positive user experience and strong trust between IT and the wider team.

Webinar: How Reddit upleveled their IT automation strategy

Learn how Reddit, one of the world's most popular online communities, automates critical IT processes to improve efficiency and reduce manual workloads. In this session, Cian Geoghegan, Staff CorpTech Systems Engineer at Reddit, shares their approach to automating three key areas: Device Management, Patch Management, and Access Management.

→ Watch the on-demand webinar: tines.com/reddit-webinar

Case study
Turo

"With Tines, we have real-time visibility across our endpoints and our environment."

SHASHEEN BANDODKAR, SECURITY ENGINEER
TURO

THE GOAL

Empower a lean team to enforce patching and surface critical AWS insights - without relying on manual ticket creation or cross-team coordination.

THE SOLUTION

Using Tines, the team automated the flow of real-time event data into Jira, enabling consistent, documented processes that reduce overhead and improve visibility for both internal and external stakeholders.

Case study: How Tines enables Turo's lean security team to do more with less

Turo enlisted Tines' no-code automation platform because it seamlessly connects systems and automates mundane tasks, increasing their impact while saving them valuable time and resources. Now, the Turo team is moving forward with confidence, knowing that as they grow, Tines is ready and capable of scaling alongside them.

→ Read the full case study: tines.com/case-studies/turo

bcm | one

Case study BCM One

"We used the tools we've bought, from CrowdStrike to RunZero, much more effectively because we have Tines."

DAN RUBINS, VP OF IT AND INFORMATION SECURITY
BCM ONE

THE GOAL

Rebuild a modern security program from the ground up, tackling over a million vulnerabilities without adding engineering or operational overhead.

THE SOLUTION

BCM One used Tines to overhaul their automation management and patching processes, reducing vulnerabilities by 55%.

Case study: BCM One transforms the way IT and security view automation

Dan Rubins assumed the VP of IT and Information Security role, and his first task was building the program from scratch. Tines offered a scalable way to hold everything together. He found he could do more through our user-friendly, drag-and-drop interface, which proved much more flexible than other platforms BCM One had considered.

→ Read the full case study: tines.com/case-studies/bcm-one

Pre-built workflows

Start building faster with real-world, pre-built workflows you can import and adapt today.

These examples come from the Tines Story Library – home to over 1,000 workflows created and shared by customers, partners, and the Tines team.

Find and reboot devices with failed Mircosoft Intune updates

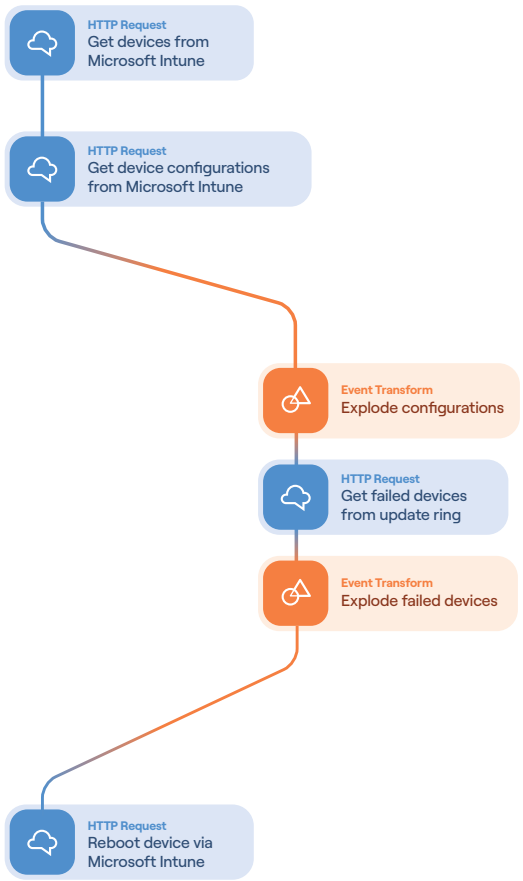
Providing fixes for failed updates, this workflow retrieves devices with unsuccessful update installations in Microsoft Intune and performs a reboot of those devices.

TOOLS

Microsoft, Microsoft Azure

USE THIS FLOW

tines.com/zjkeb



Update Linux system packages using Ansible Tower

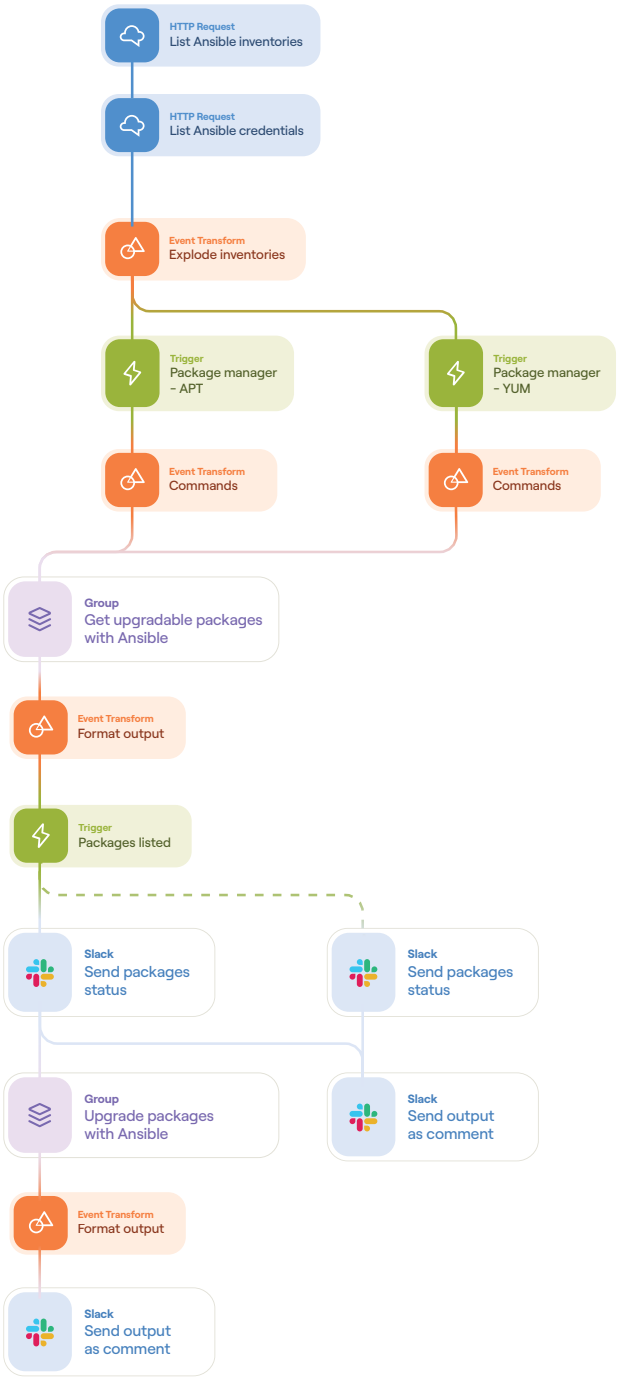
This workflow uses Ansible Tower to list Linux system packages and update them on a regular basis. It also sends packages that could be updated to Slack for approval.

TOOLS

Ansible, Slack

USE THIS FLOW

tines.com/zkptq



→ Sign up for the always-free Community Edition: tines.com/community-edition

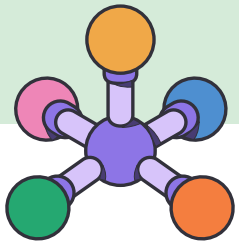
Automating

patch management

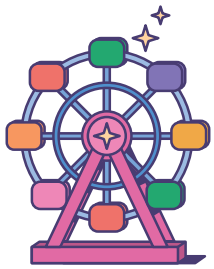
A checklist for getting started

If you're inspired by these real-world examples, it might be time to explore automated patch management in more depth. But before you get started, consider how you'd answer the following questions:

- Do you have clear visibility into patch status across all environments?
- Are your workflows consistent, auditable, and easy to repeat?
- Can your team deploy patches without relying on manual steps?
- Do you have a fallback plan if a patch fails?
- Can you handle exceptions automatically, like skipping updates for users on leave?
- Do you have a reliable patch source, and have the patches been tested in the appropriate environments before rolling out to production?
- Will patching occur in regular maintenance windows, or is it an emergency patch? If the latter, is downtime required? If so, have you considered how you'll communicate this with end users?
- Is there an order/priority for the patches? Which are the most important? Which systems should get patched first? Should certain systems not get patched at all?
- Have the appropriate backups been made prior to patching?
- Is there a clear audit trail, and have patches been approved as per your process?
- What testing is required after patches have been applied?
- Are other teams on standby in the event of issues?
- Do you have a clear path of communication with the vendor? (This may be necessary if patching causes issues, and rollback fails or is not possible.)



Building your strategy



Identify

Your first step is to determine how your patch management process will work. You'll need to identify what vulnerabilities and updates take priority, and find the endpoints that are exposed or unpatched for these vulnerabilities.

An automated workflow can help consolidate information from services like your vulnerability management tool, MDM, and patch management application. This enables you to plan which devices need to be prioritized and who you'll need to communicate outages or updates to.

Structure

After identifying what devices need to be patched and when, the structure of a patching process can start to take shape.

Automation can help you build patch groups, so you don't take all of your infrastructure offline at once during patching, or do a phased rollout of updates to end-user endpoints to allow better adoption and address employee concerns. You don't need to manage these groups manually as your IT assets grow.

Patch

Once you have the structure in place, you can roll out the actions needed to patch your endpoints. This is often more than just forcing an update to your connected endpoint via an agent - these actions might also include notifications and delays for appropriate downtime.

Report

After all this effort, you still need to confirm that your patching automation efforts are working as expected and meet any compliance requirements.

Automation can compare device information to confirm that the vulnerability or update has been patched before, when it was enrolled in the patching process. It can also help confirm system status over various tools to ensure that processes are still running as expected, post-patching.

Iterate

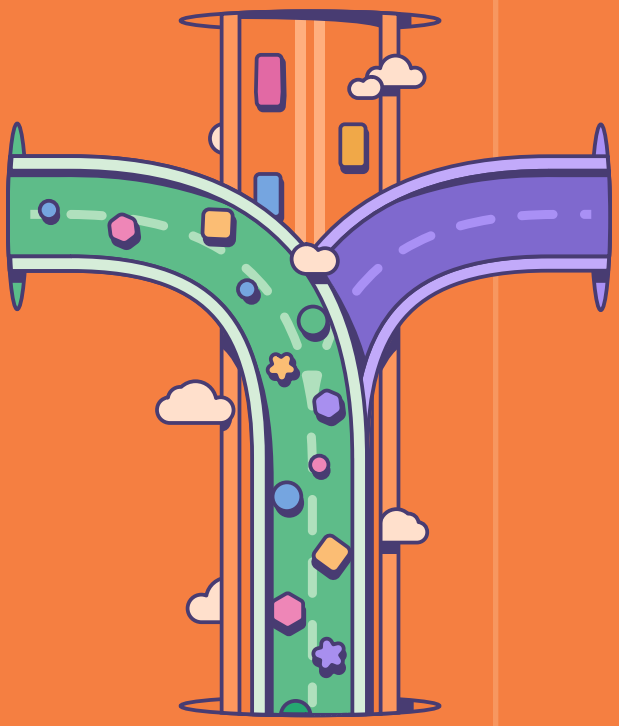
As you get a handle on your patch management automations, you can add additional features to your processes. Some ideas would be:

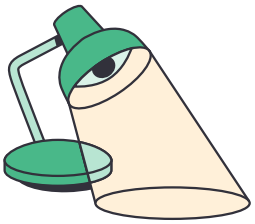
- Timezone-specific communications and patch prompting for regional IT teams and end users.
- Approvals when emergency patching is identified to review any potential impact on fast patching.
- Identifying when employees are on PTO and delaying enforcing updates to the end user's device until they're back at work.

The Tines advantage

With Tines, you can level up your patch management program with enhanced visibility, collaboration, agility, and more.

Tines' IT customers report the following:





End-to-end coordination

Automate patch scheduling and coordination across systems, with full control, auditability, and flexibility.

Seamless integration across the stack

Connect patching workflows to ITSM systems (e.g., Jira, ServiceNow), asset management tools, and communication platforms to create a clear paper trail and accelerate resolution.

Secure, streamlined approvals

Run secure approvals and escalations without manual bottlenecks, using logic-based workflows that adapt to your policies.

Real-time visibility

Gain up-to-the-minute insight into patch status, exceptions, and timeline progress with live dashboards and notifications.

Stronger collaboration

Work together in real time, experiment safely, and control access to sensitive data - all within a single platform.

Enterprise-grade flexibility

Tines supports transparency, compliance, and scale, whether you're deploying in hybrid cloud, self-hosted, or fully on-premises environments.

Maximized value from your existing stack

Increase the value of your IT tools by integrating them through Tines for more unified, efficient workflows.

Empowered team members

Tines is instantly legible with a short learning curve, so frontline and junior team members can build and adapt workflows without writing code.

Getting started

For too long, patching has been a source of stress and risk, not strength and resilience. And this pattern threatens to become further ingrained as IT complexity and threat actor ingenuity accelerate. But it doesn't have to.

Whether you're focused on reacting to emerging threats, building operational resilience, or both, Tines helps IT Ops teams move faster with less friction. That's good news for your security posture, end user productivity, and business agility. It helps improve security-IT collaboration, reduce enterprise risk, and ultimately carve out more time for IT teams to work on higher-value tasks. It's time to get patching right.

→ Sign up for the always-free Community Edition of Tines: **tines.com/community-edition**

→ Learn more about Tines for IT Operations: **tines.com/solutions/it-operations**

RESOURCES CITED:

https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/03/software-provider-fined-3m-following-2022-ransomware-attack/

https://securitybrief.co.uk/story/microsoft-s-2024-vulnerabilities-hit-record-high-report-says

https://info.flexera.com/CM-REPORT-State-of-the-Cloud

tines