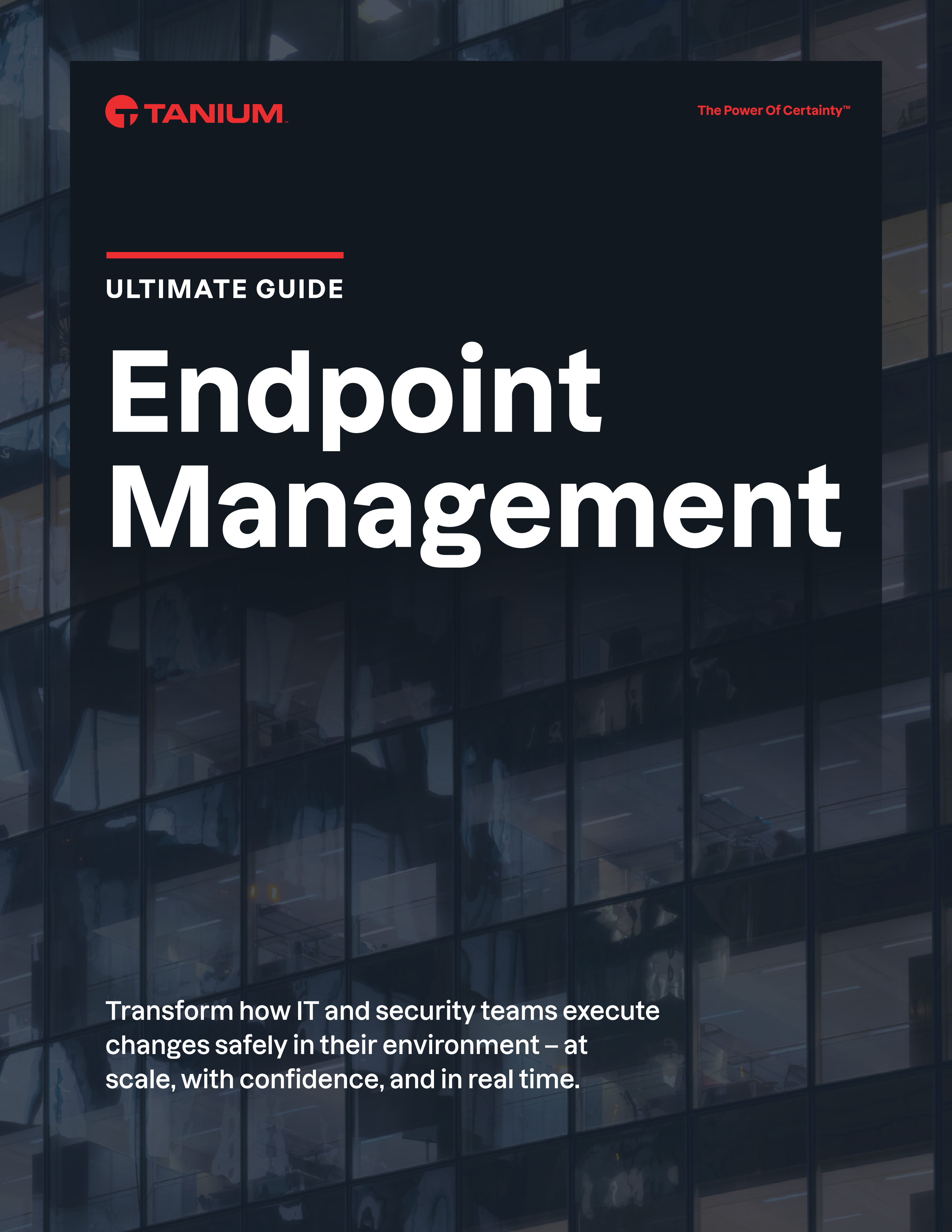


TANIUM

The Power Of Certainty™

ULTIMATE GUIDE

Endpoint Management

Transform how IT and security teams execute changes safely in their environment – at scale, with confidence, and in real time.

The Ultimate Guide to Endpoint Management

Contents

Forward

In today's IT landscape, managing endpoints—desktops, laptops, and servers—has never been more essential. With each device serving as both a gateway for productivity and a potential point of vulnerability, endpoint management stands at the core of every organization's security posture. In my 30+ years of experience, I've learned that nearly every security incident or production outage boils down to what's happening on those endpoints. Whether it's a misconfiguration, stolen credentials, or a vulnerability waiting to be exploited, the endpoint is where it all begins.

I'll never forget when I was first dubbed the "endpoint expert" in IT Ops. I knew endpoints inside and out, and I assumed it would make me a natural fit for cybersecurity. When I approached the security team, the leader humorously said, "Tim, you know the ooey gooey center, but not the crunchy outside." At the time, the focus was all about securing the perimeter, but the truth is, what happens at the endpoint is critical to the success of any security or operations program.

A few years later, that same leader returned after managing many major incident responses across the country and admitted the truth: "Nobody knew what was happening on the endpoint." We laughed about that moment, but it was a turning point for me, one that crystallized just how critical endpoints are. They're the convergence point of technology and data, where users meet the network. And that's why they need to be managed with care and precision.

This Ultimate Guide to Endpoint Management covers it all—whether you're just starting out or managing thousands of devices across multiple sites. It delves into key themes like endpoint visibility, security best practices, and the tools you need to manage them at scale. One of my favorite sayings is, "Know, Manage, Secure." You can't secure what you don't manage, and you can't manage what you don't know. That boils down to visibility, which this guide addresses in depth. You'll learn how to get both a telescopic view—seeing all your devices far and wide—and a microscopic view—drilling down to individual systems and processes. Because if you don't have that level of control, you're just guessing, or as I like to say, "managing by horoscopes."

I'm excited for you to dive into this guide, packed with insights from some of the best in the field. The contributors have done an incredible job distilling their knowledge and experience into practical, actionable advice. Whether it's preventing the next ransomware attack or keeping your systems patched and compliant, this guide is designed to help you not just manage your endpoints—but manage them well.

Thank you for investing your time in this journey. I'm confident that the knowledge and tools shared in this Ultimate Guide will help you strengthen your organization's endpoint management practices, making your systems more secure and resilient.

Thank you to all the contributors and reviewers who have made this guide possible. Your dedication and expertise are invaluable.

Tim Morris
Chief Security Advisor, AMER, Tanium

Introduction

The number of endpoints have skyrocketed in recent years, with organizations across all industries undergoing digital transformation, mobilizing operations, and transitioning to cloud and hybrid environments. **The average organization now has roughly 135,000 endpoints[1], such as smartphones, desktops, laptops, and Internet of Things (IoT) devices.**

All signs indicate this figure will keep growing as they continue to invest in new technologies, add workers, and expand their operations in the coming years.

Endpoints serve a variety of critical needs by connecting employees to network resources while enabling productivity, data sharing, and scalability. However, without real-time visibility and management, they also pose a direct threat to operations and security. Every new network device increases an organization's attack surface in both size and complexity. Each connected endpoint is a potential entry point that threat actors can use to access sensitive accounts and resources.

Furthermore, threat actors are constantly evolving their strategies and investing in emerging technologies like artificial intelligence (AI) to launch targeted attacks — and organizations are having trouble keeping pace.

According to Sophos, 32% of successful ransomware attacks last year were caused by unpatched vulnerabilities.[2] A separate study from Check Point also revealed a 30% uptick in global cyberattacks since last year.[3]

Despite this, organizations across the board are still neglecting endpoint management and security. While they are modernizing their technologies and networks, most still rely on outdated and inefficient endpoint management strategies that require manual and time-consuming workflows. IT and security teams often lack the resources to track and maintain endpoints at scale. This leads to organizational blind spots, security vulnerabilities, and higher operating costs.

To that end, the latest research reveals a critical need for modernizing and improving endpoint management. In PwC's recent 2024 Global Digital Trust Insights report, just **52% of respondents say they are happy with their endpoint detection and response strategy.**[4] Respondents also list attacks on connected devices, business email compromise/account takeovers, ransomware, and zero-day exploits among the top cyber threats.

The good news is that organizations can gain control over their connected ecosystems without making drastic changes to their operations or budgets. With the right strategy and management platform, organizations can easily create a stronger cybersecurity and IT culture driven by endpoint analytics, seamless data sharing, and compliance. For most organizations, it's just a matter of understanding the risks at hand and making the transition to modern and automated endpoint management.

This guide serves as an introduction to endpoint management, providing a foundational overview for IT and cybersecurity professionals of all skill levels. The chapters ahead cover key topics such as what endpoints are and why modern organizations need real-time visibility and control over their environments. In the later chapters, the guide takes a deeper dive into topics such as endpoint policies, the key components of endpoint management, and how to select the right platform.

CHAPTER ONE

The Beginner's Guide to Endpoints

What is an endpoint?

Endpoints are physical devices that can connect and exchange data over a local area network (LAN) or wide area network (WAN). Most organizations today have a mix of company- and employee-owned devices spread across on-site and remote environments.

Some common examples of endpoints include:

- Desktop computers
- Tablets
- Printers
- Operational technology (OT)
- Servers
- Laptops
- Databases
- Virtual machines (VMs) and environments
- Internet of Things (IoT)
  Devices such as mobile devices, wearable technology, security systems, and smart appliances

It's important to note that many types of devices do not qualify as endpoints, even though they are physically located on the network.

These include:

- Switches
- Firewalls
- Load balancers
- Storage area networks
- Network gateways
- Application programming interfaces (APIs)

Routers are another type of network device that are not typically considered endpoints. In a corporate network, endpoint devices communicate over an internal LAN that uses a router to connect to the internet. The router then connects multiple computer networks and transmits data packets between them using IP addresses. Since the router is just an intermediary device used to forward communications between the networks and its endpoints, it is not considered an endpoint device.

That said, there are some situations where a router can be considered an endpoint device. For example:

It has a web interface that allows users to configure its settings or monitor its performance.

In this case, the router is the destination of the web traffic and responds to requests from users.

It runs network services or applications that communicate with other devices or servers.

A router can act as a DHCP server, DNS server, VPN server, or firewall. Here, the router is the source or the destination of the network traffic and participates in the communication.

It's part of a network topology that uses end-to-end encryption or authentication.

For example, a router can be part of a mesh, peer-to-peer, or VPN network. The router is one of the endpoints of the encrypted or authenticated connection and must decrypt or verify the packets.

As a rule of thumb, if a device lacks an IP address (at least on an IPv6 network) and doesn't generate or consume data packets, it is not an endpoint device.

What is endpoint management?

Endpoint management is a strategy for overseeing an organization's connected endpoints. This strategy aims to improve security and compliance and boost overall business performance.

To implement this strategy, IT and security teams often deploy an endpoint management solution with the goal of gaining visibility into their managed devices. In addition, endpoint management solutions usually allow team members to configure, monitor, and patch devices.

Effective endpoint management should also provide a steady stream of data that teams can use to identify and repel cyberattacks. As such, security and IT leaders can use endpoint management to enhance their overall security posture and improve operational efficiency.

In addition, endpoint management aims to enhance and extend the capabilities of security and IT teams, enabling them to do their jobs more effectively and efficiently by reducing manual workflows. This comes as **global organizations are facing a widespread IT staffing shortage that is expected to impact 9 out of 10 organizations by 2026.**[5]

Benefits of endpoint management

Up until recently, endpoint management was a job reserved for the IT department. But with organizations becoming more interconnected and cyber threats becoming more frequent and severe, the responsibility is now commonly shared among multiple teams, including SecOps, helpdesk teams, compliance professionals, managers, and security researchers.

By unifying endpoint management into a single control panel, multiple departments can access the insights they need to generate reports, perform updates, and resolve problems.

Here are five of the top benefits of having a robust endpoint management strategy:

1. Tighten security

Most breaches today stem from poor security hygiene and weak access controls. Threat actors often scan networks looking for unpatched systems that they can use to gain access to private databases and accounts.

While there is no way to prevent cyberattacks from taking place, organizations can use endpoint management to tighten their perimeter and reduce the overall attack surface. An endpoint management platform makes it possible to ensure that each device has the latest patches and updates.

2. Improve operational efficiency

Managing applications and workloads at scale across hundreds of thousands of devices can be an enormous task, especially for overstretched and understaffed IT and security teams.

An endpoint management platform can automate critical tasks like configuring new devices and enforcing access control policies, freeing IT workers to focus on higher-level responsibilities and projects while guaranteeing operational efficiency.

3. Lower costs

Organizations often wind up overpaying for hardware and software due to issues like license sprawl and maintaining server capacity for unused devices.

With an endpoint management platform, organizations can easily identify wasteful spending. This can help to optimize resource consumption, eliminate unnecessary systems and devices, and help reallocate capital to other critical needs.

4. Reduce data silos

Endpoint data is often spread across disparate devices and databases. This makes data sharing difficult and leads to missed insights and opportunities.

A unified endpoint management platform consolidates data from all endpoints into a central database, creating a single source of truth. This ensures all teams have access to the same endpoint data, facilitating better collaboration and decision-making.

5. Ensure compliance

Enforcing security policies and benchmarks can be exceedingly difficult, especially for distributed teams.

Endpoint management enables continuous compliance through instant reporting and remediation. This reduces security risks and enables organizations to stay on top of changing regulatory requirements, avoiding fines and penalties.

CHAPTER TWO

Why Security Matters for Endpoints

The cost of cybercrime has skyrocketed in recent years, with organizations generating larger amounts of data and becoming increasingly dependent on their digital environments.

> **According to IBM, the global cost of a data breach is now $4.88 million — representing a 10% year-over-year increase and the highest total ever.**[6]

When targeting an organization, threat actors typically take the path of least resistance. Targeting an end-user through social engineering and phishing is usually much faster than penetrating multiple layers of network defenses. Endpoint devices provide easy access to valuable databases and accounts, which is why organizations need to go above and beyond to ensure they remain secure.

What is endpoint security?

Endpoint security involves detecting, stopping, and remediating attacks against every type of endpoint at any location — on-premises, in the cloud, and across hybrid environments.

Endpoint security is a necessary component of an organization's overall cybersecurity strategy, as these devices are often the entry point for attackers who want to compromise the network and cause damage or disruption.

Why all organizations need endpoint security

While cyberattacks on large organizations tend to dominate the headlines, most attacks actually target small and midsized enterprises (SMEs). These organizations tend to have smaller IT budgets and a limited capacity for monitoring and remediating threats.

Remote work has made the problem for SMEs even worse. Employees who were once in the office on a company-owned device and always connected to the corporate network are now at home, in some cases using a personal device to conduct business that's not connected to a VPN but rather a home network that other members of the household, and lots of other unsecured household devices, also use. Cybercriminals know this — so they are increasingly targeting remote employees and their unsecured endpoint devices.

Effective endpoint security helps organizations of all sizes protect data, minimize the risk of successful cyberattacks, and maintain service availability.

A robust endpoint security strategy can lead to the following benefits:

Preventing data loss

When endpoint security tools improve efforts to secure devices, organizations can gain confidence that critical business data, such as sensitive information and intellectual property on endpoints, is safe from accidental sensitive data leaks, corruption through malware, or encryption from ransomware.

Ensuring business continuity

Another significant benefit of endpoint security is that it protects endpoints from attacks that could disrupt end users and operations. When endpoint security efforts are working, employees can use endpoints without worrying about interruptions from cyberattacks, data loss from ransomware, and other types of threats.

Strengthening cyber defense

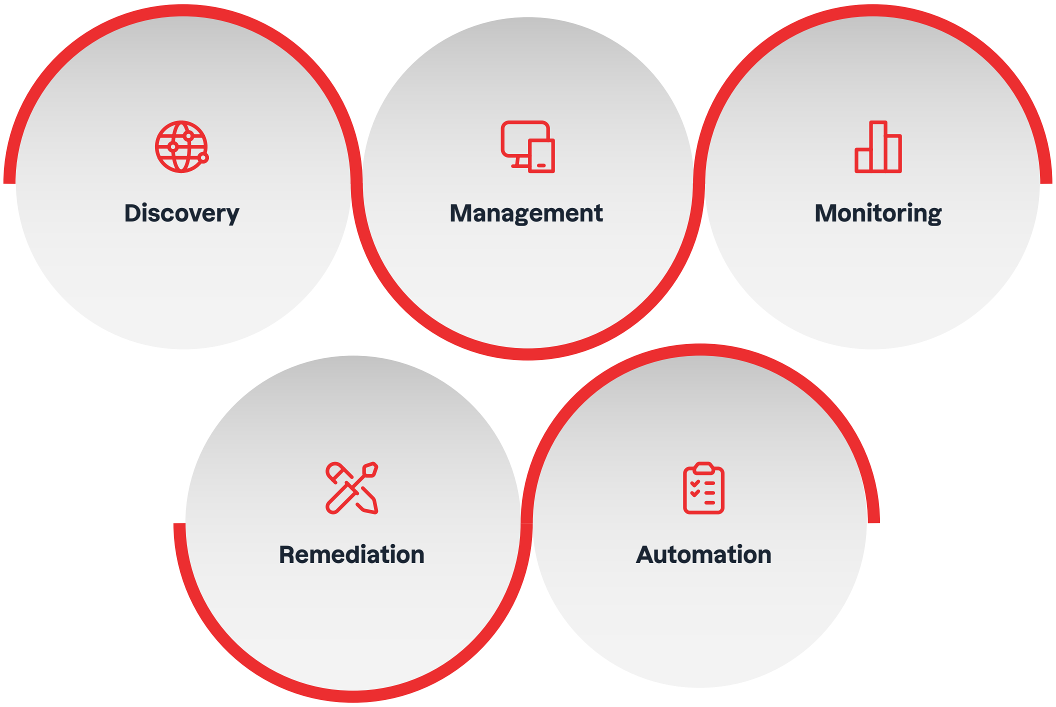
By providing teams with the insights needed to fortify endpoint security, identify threats affecting endpoints, and respond to those threats quickly, organizations can minimize the risk of cyberattacks and the damage they cause.

Lowering security costs

Many organizations wait until after they experience an incident to invest in cybersecurity. As a result, they wind up paying more for remediation and coverage. IBM's report reveals an average cost savings of $2.22 million for organizations that use security AI and automation extensively in prevention compared to those that avoid it.[6]

The five key components of endpoint security

A comprehensive endpoint security strategy must include at least five components: discovery, management, monitoring, remediation, and automation.



1. **Discovery:** To effectively protect endpoints, security administrators must know they exist. That is why every endpoint security strategy must start with identifying all your endpoints. This step involves scanning the network, discovering unmanaged assets, and allowing security teams to block each one or bring them under management.

2. **Management:** Once you know about all your endpoints, you can perform ongoing endpoint management efforts more efficiently. Endpoint management is crucial to supporting proactive security measures. Tasks like patching vulnerabilities, keeping endpoints up-to-date, effectively deploying new software, and ensuring endpoints are configured according to best practices can help organizations prevent hackers from ever gaining a foothold in their environments.

3. **Monitoring:** After discovering and controlling all endpoints, the next step is to establish real-time performance monitoring. With real-time monitoring, administrators can have an easier time identifying malicious activity, violations of security policies, and other opportunities to optimize and avoid risks.

4. **Remediation:** When threats do occur, organizations need to be able to quickly take endpoints offline to prevent malware and other active processes that could allow attackers to gain unauthorized access to additional endpoints.

5. **Automation:** While automation may not be a conventional feature of endpoint security, it is becoming a key component of a modern and proactive approach to protecting endpoints from cyberattacks. Automation can assist with many tasks, such as allowing teams to scan the network for new devices, apply consistent security policies, detect and respond to threats in real time, and remediate incidents without manual intervention.

Tips for improving endpoint security

> Connected endpoints operate around the clock, across geographical distances, and with varying levels of security and governance. Considering this, the only way to ensure endpoint security is to treat all endpoints as security threats and adopt an "always-on" management policy with continuous monitoring, updating, and patching. Taking this approach can shrink the threat surface and reduce the impact of cybersecurity incidents.

The following strategies are critical for improving endpoint security:

Map the IT environment

IBM found that one in three breaches involve "shadow" data, which exists outside of the IT scope.[6] CIOs and CISOs need to understand how many devices are on the network at any given time, their location, who owns and operates them, and whether they have the latest updates and security patches.

Declutter the environment

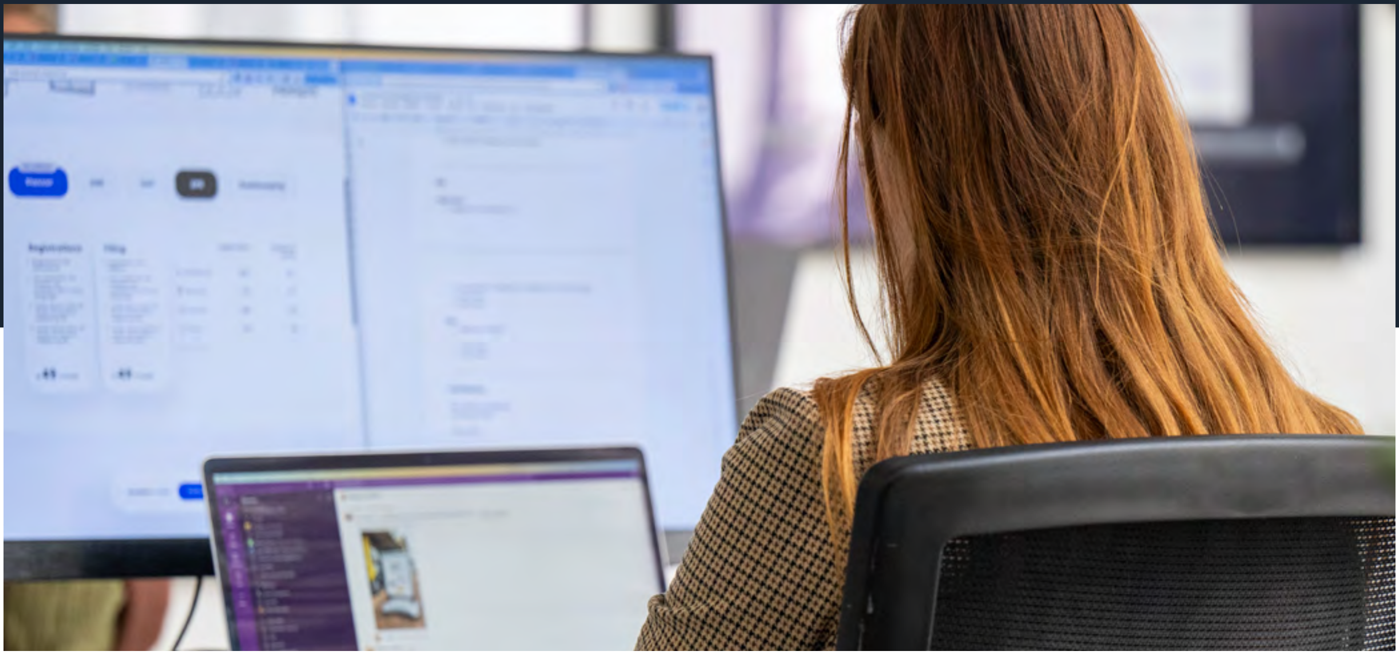
Legacy technologies are a common avenue for hackers to penetrate a network, in part because they tend to lack support or become idle. Therefore, IT and security leaders should practice endpoint hygiene by retiring and eliminating outdated tools and technologies.

Knock down silos

Many organizations struggle with IT assets that are dispersed across digital silos, each with its own admins and owners. The bigger organizations get, the more that becomes an issue. Breaking down silos and integrating IT and security teams can improve visibility and collaboration, while enabling faster and more efficient threat hunting and remediation.

CHAPTER THREE

Endpoint Policies 101



Endpoint management is an umbrella term that encompasses a wide variety of individual endpoint policies. IT and security leaders are responsible for understanding each of these policies and determining which ones are necessary for their specific environments.

IT and security leaders have many different options when setting individual endpoint management policies. These decisions will directly impact an organization's operations and security, so it's important to approach policymaking carefully to ensure both efficiency and productivity.

Endpoint management policies to know

Endpoint policies primarily center around identity access, device authentication, and threat detection. They may also include elements like data protection and network control.

Here is an overview of some common policies that organizations use to govern their endpoints.

Access control

As the name suggests, access control involves securing sensitive data and systems, making it harder for threat actors to leverage them. Access control can refer to both physical and digital systems.

A strong access control policy should fortify the network while giving users direct access to the tools they require. Administrators must implement access control policies, such as role-based access control (RBAC), alongside deep configuration visibility across the entire network to avoid security gaps and productivity bottlenecks.

Anti-malware

Anti-malware aims to protect endpoints from security threats like ransomware, spyware, rootkits, worms, and keyloggers. It involves scanning endpoints for malware, applying updates, quarantining or removing threats, and informing users about known threats and suspicious items.

Flexibility is key with anti-malware. Security administrators should be able to set multiple levels of anti-malware policies across different devices and roles.

Bring Your Own Device (BYOD)

Allowing employees to use their own mobile devices can open the door to greater flexibility and cost savings. However, it can also expose organizations to hidden security threats, with corporate-owned data and applications living on private, employee-owned devices.

Organizations use BYOD policies to enhance security across employee-owned devices. For example, this may involve creating rules to limit what applications and files users can access, restricting permissions on removable media and devices, or remotely encrypting user drives.

Firewall management

Distributed organizations need to enforce network policies for all remote users and devices. This is especially important when accommodating remote workers who may be accessing sensitive resources over insecure networks.

This can be accomplished by creating a firewall policy, which is a set of rules that determine how a device manages network traffic.

Remediation

Unfortunately, all it takes is one vulnerable endpoint to cause a cybersecurity incident that impacts the entire organization. As such, administrators need to quickly identify and remediate endpoints when they violate organizational security standards.

A remediation policy involves creating a list of rules to keep endpoints secure and compliant, detect non-compliant assets, and automatically bring them up to standard.

An effective remediation policy should have a purge function to remotely wipe nonessential data or freeze an endpoint when it's lost or stolen.

Zero Trust

Given the growing volume of sensitive data that organizations are now using, implementing a Zero-Trust architecture has become more crucial than ever.

Zero Trust is a cybersecurity approach designed to enforce security for every user, on every device, at every stage of a digital journey. With a Zero-Trust model in place, administrators can track interactions across all global locations and take action when necessary to protect the network. Some examples include suspicious logins and privilege escalations.

Key takeaways from Chapter 3

- Organizations use various policies to enforce endpoint management.
- The policies that organizations select directly impact on their operations and security.
- Some of the most common policies include access control, anti-malware, firewall management, device remediation, and Zero Trust.

These are just a few of the many different endpoint policies that IT and security leaders should know about. Some additional policies include ransomware response and patch management.

Endpoint policies should evolve over time as the organization's needs change and the threat landscape continues to evolve. Considering this, security and IT leaders should meet regularly to review policies together to ensure the organization uses the most effective strategies.

Next, we'll take a closer look at the key features you should look for when choosing an endpoint management system. ilities.

CHAPTER FOUR

Key Endpoint Management Components

While policies provide the foundation for a comprehensive endpoint management strategy, integrating with elements like asset management and incident response is essential for gaining comprehensive protection.

The endpoint management market is saturated with similar products, making it challenging to select the right system. However, not all platforms offer the same tools and features. Understanding what to look for in an endpoint management solution will save time and ensure comprehensive coverage.

Endpoint management features to look for

Asset inventory management

Unknown devices can directly threaten an organization's network. For this reason, the journey to effective endpoint management starts with asset discovery and inventory.

Asset inventory management involves discovering, cataloging, and tracking all the hardware and software within a corporate network. This allows organizations to detect potential vulnerabilities and threats more easily.

Asset inventory management must also be a continuous process, with real-time scanning and reporting.

Configuration management

> Misconfigurations currently rank in the Open Worldwide Application Security Project (OWASP) Top 10, a leading vulnerability reference for cybersecurity professionals.[7]

Oftentimes, misconfigurations occur because organizations lack the bandwidth to stay on top of changing configuration requirements.

Configuration management centers around defining, applying, and enforcing a system's desired state across computers, servers, and software. It can also entail managing and controlling information systems to optimize cybersecurity and mitigate risk.

Most traditional configuration systems were built for pre-cloud computing environments and on-premises deployments. Organizations today require modern architectures that can continuously scan any endpoint environments for misconfigurations or policy conflicts that could lead to breaches.

Digital employee experience (DEX)

Digital employee experience, or DEX, broadly refers to how employees interact with the digital tools in their workspace. When employees struggle with poor-performing technology, complex processes, confusing systems, and insufficient support, the resulting frustration not only affects the employee's well-being but can also result in dissatisfaction with the workplace overall.

An endpoint management solution should enable the IT team to improve asset visibility, identify and fix performance issues, establish efficient workflows, and refine processes more easily. As a result, employees gain easier access to the digital tools they require, and the applications, devices, and endpoints employees depend on remain available and perform as expected, leading to a smoother and more efficient digital work experience.

Deployment

While software can be great for end users, it can be a nightmare for IT teams that need to deploy, manage, and scale it.

It helps to have an endpoint management platform that lets you rapidly install, update, and remove software across the organization with minimal infrastructure requirements. The platform should make it easy to deploy groups of applications to a flexible set of targets, like user groups, locations, and departments.

Incident response

According to Cisco's latest Cybersecurity Readiness Index, organizations face a heightened risk from ransomware, credential stuffing, supply chain attacks, social engineering, and cryptojacking. What's more, **11% of organizations expect AI-related cyberattacks will be among the top three risks in the year ahead.**[8]

As cyber threats continue to intensify, organizations must look for ways to reduce the mean time to resolve (MTTR) security incidents when they occur. One of the best ways to do this is to leverage an endpoint management platform with advanced incident response capabilities like real-time threat detection and integration with Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) tools. This type of functionality can help to quickly move from incident detection to remediation and reduce the impact of an attack.

Patch management

> The total count of published vulnerabilities and exposures (CVEs) is expected to increase by 25% this year, totaling 34,888 — or roughly 2,900 per month.[9]

Tracking and patching vulnerabilities is necessary for protecting endpoints and preventing cybersecurity incidents. It's critical to have an endpoint management platform that can automatically detect, distribute, and apply updates to software, operating systems, applications, and more. This can save time, improve efficiency, and ensure that all systems receive timely patches.

Risk and compliance

All organizations today have a responsibility to protect sensitive data from threat actors. In addition, they must remain compliant by observing rules governing the use of information and IT. However, both are only possible when organizations know where their data lives at any given time.

To manage risk and compliance, organizations need to maintain complete and comprehensive knowledge of all network endpoints. In addition, they need real-time alerting in place to detect when unauthorized devices or users attempt to access private resources.

How automation is transforming endpoint management

Most IT environments are now highly dynamic and continuously growing in complexity. At the same time, IT departments across the world are struggling with a growing staffing shortage.

> In fact, by 2026, the worldwide staffing shortage will impact 90% of organizations worldwide.[10]

This means IT and security teams are often required to take on complex endpoint challenges to address new operational issues or security threats with an incomplete or misaligned understanding of the potential impact or lacking the necessary expertise in the computer environments they're tasked to protect.

As IT departments are asked to do more with less, traditional endpoint management platforms that lack modern intelligence and automation are becoming irrelevant. With teams already stretched thin and budgets not growing at the pace modern IT environments demand, IT and security operations teams must become more efficient by automating the many time-consuming and repetitive tasks they do every day.

Key challenges automated endpoint management capabilities can help customers overcome:

Rising complexity

IT departments across the board are overwhelmed with the growing number of endpoint devices, operating systems, and applications. Autonomous endpoint management systems help remove management burdens and enable organizations to do more with less.

Rising threats

Increased cyberattacks demand faster patch deployments, better device configuration compliance, and closer alignment with vendor lifecycles to reduce vulnerabilities. Endpoint automation allows teams to close vulnerabilities with greater speed and accuracy to avoid security bottlenecks.

Manual workflows

Developing and maintaining automation for common administrative tasks and applying standard policies and configurations is time-consuming and requires integration across multiple tools. Automated endpoint management streamlines administrative tasks.

Automation risk

Autonomous systems introduce risk when they're implemented without tight controls and standardization to ensure consistency, reliability, and resilience. But when teams have a constant flow of real-time data, automation becomes more reliable in highly dynamic environments, leading to fewer operational issues, disruptions, and security risks – and greater confidence.

Development bottlenecks

Automating workflows across disparate point solutions is complex and error-prone and can introduce latency during execution due to the way each solution varies in how it models APIs, data, and protocols. These differences dramatically increase the time it takes for developers to implement reliable automation.

Limited visibility

Disparate point tools create barriers to granular visibility, control, and tracking (such as data silos and error-prone manual processes) that can limit the adoption of automation capabilities. To confidently implement automation and demonstrate ROI to leadership, operators require transparent governance and controllable workflows to ensure and report positive outcomes. This becomes possible with a robust endpoint automation platform.

Key takeaways from Chapter 4

- The endpoint solution market is saturated with similar products. Knowing what to look for can streamline procurement and reduce tool onboarding.
- Some of the top endpoint management features to look for include asset inventory management, configuration management, software management, incident response, patch management, compliance, and risk management.
- Automated endpoint management capabilities can help IT staff "do more with less" and overcome operational challenges.

Sourcing an endpoint management platform can be overwhelming due to the abundance of options. Focusing on core elements like asset inventory management, configuration management, and OS patching and software management will save time and simplify procurement.

Now that you know how endpoint management can assist in your efforts to take control, improve performance, and reduce cyber risks, let's explore the pros and cons of different endpoint management solutions to choose from.

ties.

CHAPTER FIVE

How to Choose an Endpoint Management Solution

Features and components are only part of the equation when selecting an endpoint management platform. It's also important to consider the type of endpoint management solution that best aligns with your organization's needs and future goals.

As it turns out, there are several types of endpoint management platforms on the market today that offer varying levels of visibility and control. In this chapter, we'll take a closer look at some common types of endpoint management tools you may come across in your research and compare their advantages and disadvantages side-by-side.

Comparing common types of endpoint management tools

Endpoint detection and response

EDR tools are designed to detect known threats in an environment. EDR solutions are typically endpoint logging engines that use heuristics to identify malicious activity.

While EDR tools are helpful for identifying incoming threats, they come with some limitations. For example, EDR tools can only see certain types of known threats. As a result, EDR systems can create blind spots where threat actors can hide. EDR solutions also limit the activity they will record and preserve to reduce bandwidth and storage consumption, including the number of days information is retained.

Pros of EDR

- Automatically detects incoming threats
- Can detect anomalies using behavioral analysis
- Integrates with third-party security tools like SIEM

Cons of EDR

- Only tracks known threats
- Has limited bandwidth for record keeping
- Often produces false positives

Extended detection and response (XDR)

XDR platforms use AI techniques like machine learning to detect, prioritize, and mitigate incoming threats.

In addition to pulling data from endpoints, XDR platforms also gather insights from other security tools like SIEM platforms and network security solutions. XDR monitors activity across multiple sources to detect issues and alert cybersecurity professionals.

Pros of XDR

- Provides comprehensive monitoring
- Consolidates security data from multiple endpoints and systems
- Reduces the time to neutralize threats

Cons of XDR

- Can be complex to configure and interpret data
- Expensive to implement and maintain
- Requires deep integration with other security tools

Endpoint protection platforms (EPP)

EPPs primarily offer centralized monitoring, control, and management of antivirus activity. Organizations use EPPs to monitor and manage antivirus software across distributed endpoints and generate security reports. In addition to offering antivirus protection, some platforms use technologies like machine learning and email gateways to detect anomalies and filter malicious content.

The downside to using EPPs is that they only collect data primarily from endpoints and don't integrate well with other security tools. As a result, EPPs offer limited upside for cybersecurity teams.

Pros of EPP

- Improves and extends antivirus software
- Some platforms are cloud-based
- Can help limit social engineering attacks

Cons of EPP

- They don't always integrate with other security tools
- Can be complex
- Offer limited threat detection and response

Unified endpoint management (UEM)

UEM enables organizations to manage endpoint devices from a single cloud-based console. This makes it fast and easy to control, update and protect devices. Plus, UEM lowers costs by consolidating tools and streamlining management processes.

UEM evolved from mobile device management (MDM) and enterprise mobility management (EMM). UEM extends MDM and EMM capabilities to other types of devices, and makes it possible to monitor and control different operating systems across distributed locations.

Pros of UEM

- Offers comprehensive performance monitoring
- Reduces complexity
- Helps with configuration, updates, and policy enforcement

Cons of UEM

- Traditional UEM solutions lack automation
- UEM platforms tend to lack advanced security capabilities
- Can be highly resource intensive and require hefty computational and storage resources

Converged endpoint management

Converged endpoint management brings together security operations and IT management to help control complex IT and security environments.

This approach unites endpoint tools and data and makes them viewable through a single pane of glass, providing IT and security teams with greater visibility and control over their endpoints and allowing them to make faster, more informed decisions.

Pros

- Centralizes management and security for endpoint devices
- Automates routine tasks like updates and patch management
- Provides real-time visibility into endpoints

Cons

- Requires skilled experts and training
- Can be difficult to implement and manage
- Teams can struggle to realize full value

Autonomous endpoint management (AEM)

Autonomous endpoint management is a next-generation approach that uses AI and machine learning to automate and streamline endpoint management tasks, improving efficiency, security, and the digital employee experience.

Key takeaways from Chapter 5

- There are many types of endpoint management solutions available today including EDR, XDR, EPP, UEM, and converge endpoint management.
- Endpoint management solutions offer varying levels of visibility and control.
- Organizations often use a mix of endpoint management solutions to achieve their security and deployment objectives.

There is no right or wrong answer when it comes to endpoint management. In fact, organizations often use a variety of solutions like EDR and XDR in their environments.

Regardless of which platform you select, the most important thing is to have a system in place that can pull data from endpoints and other security platforms and create a single source of truth.

Keep reading to learn more about how Tanium is helping organizations transform their endpoint management strategies and ushering in a new era of autonomous endpoint management (AEM).

ties.

CHAPTER SIX

Tanium's Approach to Endpoint Management

Many organizations are still managing endpoints using outdated tools with traditional hub-and-spoke architectures, where each hub (or server) must connect to a central server and multiple endpoints (spokes). These systems are notoriously inefficient and typically unable to scale past tens of thousands of endpoints — contributing to slow communications, performance issues, patching delays, and security vulnerabilities.

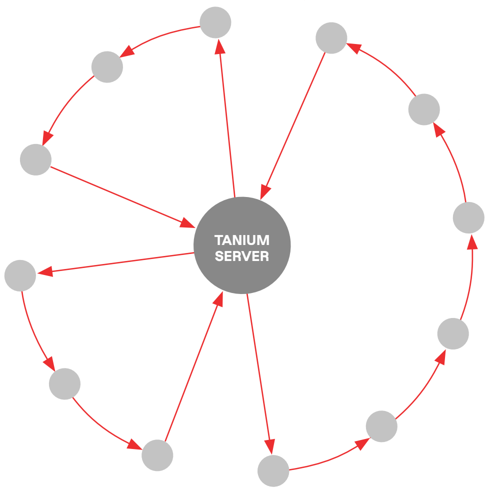
Built differently from the start

Tanium's platform starts addressing these challenges with its patented linear-chain architecture, which enables endpoints to automatically connect with nearby devices and form a secure, low-latency chain for efficient and reliable management.

This architecture enables real-time visibility and control over each distributed endpoint, allowing organizations to quickly discover assets, manage inventories, and troubleshoot performance issues. With Tanium, security and operations teams can automatically deploy patches, gain deep network visibility, and reduce their overall threat surface.

A closer look at Tanium's linear-chain architecture:

- A centralized server connects to a leading endpoint, starting a chain.
- The "leader" sends data to its neighbor, which passes it along to the next endpoint in the chain.
- This continues until it reaches another leading endpoint that communicates back to the Tanium server.
- The Tanium server aggregates data from the end of the chain.



By leveraging Tanium, security and operations teams can access real-time data across every managed and unmanaged endpoint — along with a complete suite of capabilities to control their assets, harden the network, and respond to security events.

Why use the Tanium platform for endpoint management?

There is a 90% chance a vulnerability will be exploited within 40 to 60 days after discovery.[11] However, the average time to patch a vulnerability is between 60 and 150 days – leaving threat actors with ample time to achieve their goals.[12]

The Tanium platform helps close this gap by automating updates, reducing exposure, and fortifying network defenses.

Here are some of the ways security and operations teams can use Tanium:

- Reduce cyber risk and administrative workloads with a highly efficient, scalable patching solution that guarantees a 99% success rate.
- Boost efficiency by fully automating patching and software deployments.
- Accelerate endpoint provisioning by up to 8x, reducing the cost of imaging and reimaging systems.
- Securely install software at scale, saving significant time using a pre-packaged gallery of enterprise applications.
- Break down silos with unified reporting across Windows, Mac, and Linux from a single pane of glass.
- Reclaim software costs from unused assets.
- Gain instant insights about the overall network environment with accurate and up-to-date data.

Customer success stories

Organizations across numerous verticals, including manufacturing, technology, healthcare, and other industries, are leveraging Tanium to manage endpoints more efficiently and securely.

Two noteworthy success stories include Synopsys, a leading EDA provider serving industry giants like NVIDIA, Apple, and IBM, and VF Corporation, parent company of The North Face, Vans, and other famous apparel brands.

Synopsys

Synopsys needed a better way to manage its massive, distributed fleet of 23,000 endpoints. After a successful PoC, the company moved forward with a full Tanium implementation.

With Tanium, all Synopsys endpoints now receive regular patching and updates, ensuring that commonly used endpoint applications like browsers and PDF readers are scanned and secured. The company also leverages Tanium for employee self-service and real-time endpoint feedback. **Synopsys has also reduced the number of servers that it needs to run security software by 70%.**

“We’re always under pressure to do more with less. Tanium has helped my team do that… Tanium makes my managers’ jobs easier, and that makes my job easier”, said Andrew Wall, Director of IT for Synopsys.

VF Corporation

VF Corporation, also known as VFC, needed to evolve and automate its end-to-end patching and security orchestration strategy to boost productivity and protect its network.

VFC is now using Tanium Automate, which simplifies IT and security task orchestration using real-time endpoint visibility and data, while also using other Tanium modules like Patch, Deploy, and Discover. As a result, **VFC enjoys tighter security with real-time visibility and a faster, more efficient patching process.** Tanium Automate also frees VFC’s patching lead to focus on deep work instead of repetitive, labor-intensive security tasks.

“My overall experience using Automate has been outstanding so far, the tool is delivering exactly what we expected,” said David Anderson, VFC’s patch automation and vulnerability remediation lead. “We are now able to quickly patch using runbooks and focus on other priorities, knowing that these critical updates are taking place in the background. Plus, runbooks only take about five minutes or so to create. The entire process gives us back countless hours in our schedule.”

Tanium integration use cases

Tanium is much more than just an endpoint management and security solution. It's also a versatile platform that directly integrates with leading security services and custom packages to enhance and extend enterprise IT and security operations.

Security and operations teams can leverage Tanium for the following needs:

Event monitoring/log aggregation

Integrate Tanium reports, alerts, and endpoint data with log aggregation systems, SIEM solutions, or alert managers to improve visibility and incident response.

Asset management

Enrich CMDBs with real-time data, uncover detailed insights, and quickly discover information about individual endpoints.

Threat response and remediation

Automate evidence gathering, create custom alerts, and remediate threats directly on endpoints.

Risk and Zero Trust

Combine Tanium with leading Cloud Access Security Brokers (CASB), Secure Web Gateways (SWG), and Identity and Access Management (IAM) tools to strengthen control and overall security.

Tanium also supports custom sensors and packages, delivering unparalleled visibility and control over endpoints. Organizations can use Tanium to check the health and status of applications and services, install and configure software, and rapidly deploy hand-crafted security fixes across the enterprise at scale.

Integration spotlight: Microsoft and Tanium

Tanium integrates with several leading Microsoft products, including Security Copilot, Defender for Endpoint, Sentinel, Entra ID, and Intune. Tanium's real-time insights complement Microsoft's advanced threat intelligence and analytics services, empowering effective and resilient IT operations at scale. Tanium received a 2024 Microsoft Partner of the Year Award in the Independent Software Vendor (ISV) Innovation category and was named a finalist in the Microsoft Commercial Marketplace categories for Global and Americas regions.

One company that's benefitting from Tanium's close integration with Microsoft is innovative real estate organization Jones Lang LaSalle (JLL). JLL uses Tanium and Microsoft to simplify and enhance security for roughly 90,000 endpoints. The company has also reduced cybersecurity spending by about 20%, which translates to $5 million in savings.

> “By using a best-in-suite approach with Tanium and Microsoft, we have made orchestration and automation more seamless.”

Dane Thomas
Head of Global Security Engineering, JLL

Integration spotlight: ServiceNow and Tanium

Tanium’s close integration with ServiceNow’s intelligent workflow automation platform helps organizations achieve 100% asset visibility, reduce risk, and improve agent, employee, and customer experiences. Tanium can combine with ServiceNow to create a complete and accurate CMDB, respond to vulnerability risks, and enhance overall compliance.

Pharmaceutical provider AstraZeneca relies on Tanium’s integrations with ServiceNow and Microsoft to protect its IT systems and vital research activities. These integrations have improved cooperation with IT and created new opportunities for automation while streamlining patching and threat elimination.

> “Thanks to the power of Tanium and our integration with ServiceNow, our businesses will be able to decide on timeframes for pulling their patches – as opposed to IT pushing things down.”

Jeff Haskill
VP of Enterprise Technology Services, AstraZeneca

Key takeaways from Chapter 6

- Tanium offers a groundbreaking approach to endpoint management, with a unique platform architecture and converged system.
- Customers are realizing the benefits of using Tanium solutions to gain more control, streamline costs, and ensure more effective endpoint security.
- The platform seamlessly integrates with popular services like Microsoft, ServiceNow, and more.
- The Tanium platform delivers autonomous endpoint management (AEM) by leveraging real-time insights from cloud-managed endpoints to recommend and automate endpoint changes safely and at scale. Read on to learn more about Tanium AEM.

CHAPTER SEVEN

The Next Evolution of Endpoint Management

IT and security teams currently face significant challenges due to frequent OS and software updates, configuration drift, and rapid exploitation of vulnerabilities.

Moreover, the landscape of cyber threats has become more hostile. The probability of a vulnerability being exploited reaches 90% between 40-60 days after discovery, as indicated by Kenna Security.[13] A Verizon study found that organizations witnessed a surge in vulnerability exploitation by nearly 180 percent last year.[14] All this while IT leaders grapple with an overall skills gap in their staff, with 93% indicating it impacts automation efforts, as reported by CompTIA.[15]

Organizations must deploy patches quickly, ensure device compliance, and align with vendor lifecycles to mitigate risks, all while overcoming budget constraints, skill shortages, and more.

Introducing Tanium Autonomous Endpoint Management

Autonomous endpoint management, or AEM, is a next-generation approach to endpoint management that uses composite AI to provide intelligent automation and decision-making capabilities – and Tanium is at the forefront of this paradigm shift, empowering ecosystems with the real-time platform for AI.

Gartner states that, "AEM represents the most significant advancement in endpoint management in over a decade."[16]

Gartner further explains in its 2024 Hype Cycle for I&O Automation that AEM accelerates patching and configuration management while lessening digital friction — leading to better compliance, productivity, and employee experience.[17]

> “Autonomous endpoint management (AEM) combines capabilities of unified endpoint management and digital employee experience tools with AI and machine learning to accelerate endpoint patching, configuration and experience management,” Gartner says. “The AEM approach will eventually replace disparate tools and architectures with cloud-based, intelligence-powered capabilities. AEM reduces IT overhead, increases compliance and enables efforts to be redirected toward employee enablement and business-value-added work.” [18]

To support Tanium AEM, we’re developing several foundational technologies designed to be used individually by Tanium users or combined into workflows across the Tanium platform.

Real-time cloud intelligence

Tanium AEM is built on a foundation of real-time cloud intelligence that analyzes trends, impact, and usage patterns across millions of endpoints instantly. It uses a unique cloud-scale, multi-model stream processing system that combines various analytical and AI models for the required insights. Tanium AEM continuously refines these insights based on evolving IT conditions and technologies.

Automation and orchestration

Tanium Automate streamlines IT and security task automation with real-time data. It lets users automate complex tasks quickly by replacing manual steps with simple no- to low-code solutions to:

- Build playbooks with minimal or no coding for common operations and security tasks
- Enable various skill levels to create effective automation
- Set criteria for each step before moving forward
- Keep complete visibility of actions with audit logs, current status, and future plans
- Execute Automate playbooks using Tanium APIs with tools like ServiceNow or Microsoft security solutions

Deployment templates and rings

When large-scale changes to endpoints are needed, Tanium AEM leverages deployment templates and rings to help reduce disruptions by implementing changes in alignment with the organization's operational flow. This allows for phased deployments and ensures they are well-managed and repeatable.

With deployment templates and rings, organizations can:

- Configure progression criteria leveraging real-time data to safely deploy changes across rings
- Take advantage of reusable deployment plans to consistently deliver changes
- Create custom deployment plans that are tailored to different levels of risk tolerance

> "I highly recommend using Tanium Automate, especially for busy security teams that are trying to save time on manual, repetitive tasks like patching. Automate drastically simplifies security orchestration and gives you back countless hours to focus on deeper work."

David Anderson
Patch automation and vulnerability remediation lead, VFC

Revolutionize decision-making and execution for IT and security teams

Tanium AEM pulls real-time data from millions of endpoints to enable intelligent automation and feed insights and actions into platforms like Microsoft and ServiceNow – minimizing disruptions, increasing productivity, and reducing risk. What's more, Tanium AEM provides IT and security teams with greater control over all recommendations and automation, enabling them to make informed and efficient decisions, reduce manual tasks, and take operational posture to new heights.

Organizations that embrace autonomous endpoint management should expect a multitude of benefits from maintaining a more secure, resilient, and compliant environment.

Tanium AEM benefits include:

Operational resilience

By deploying changes using insights from real-time analysis of changes to endpoints globally, combined with deployment rings and visibility to the real-time impact of changes, IT teams can avoid costly disruptions that impact productivity.

Enhanced security posture

Proactive identification, prioritization, and remediation of cyber risks from vulnerabilities and configuration drift help protect organizations from cyber threats, safeguarding sensitive data and maintaining customer trust.

Reduced IT support costs

Automatic resolution of several endpoint issues reduces IT and security support overhead that can also disrupt and impede employee productivity.

Ensure compliance

Continuous monitoring, industry benchmarking, and automated compliance checks ensure that organizations meet regulatory requirements, reducing the risk of fines and legal issues.

Scalable IT management

Automating routine tasks frees up staff to focus on strategic initiatives that drive growth, optimizing the use of human resources.

Increased IT agility

Automated processes and real-time data allow IT to quickly adapt and support evolving needs.

This shift to AEM is the latest development in Tanium's journey, which began with deploying a unique single-agent, linear architecture endpoint management solution and eventually evolved into a cloud-first converged endpoint management platform. Tanium is continuously pushing the boundaries of endpoint management with Tanium AEM, and remains committed to providing unmatched visibility, control, and remediation of endpoint devices for global organizations.

Key takeaways from Chapter 7

- Tanium AEM represents the next evolution of endpoint management and uses AI to enhance change management and security monitoring.
- Tanium now offers Tanium AEM, which brings intelligent automation and feeds insights and actions at any scale.
- Organizations can leverage AEM capabilities to revolutionize how they make decisions about endpoint and risk management.

Endpoint management may seem overwhelming, especially for distributed organizations with expanding IT footprints. However, gaining real-time visibility and control over endpoints is critical for preventing security incidents, reducing IT sprawl, and minimizing costs. And, with the help of Tanium AEM, it's something any organization can do, regardless of their budget or level of expertise.

Tanium is helping organizations across all verticals to modernize their operations and experience the next generation of autonomous endpoint management. With Tanium, they can instantly execute changes at scale with greater speed, confidence, and precision.

Schedule a live, personalized demo to experience how Tanium can solve your organization's endpoint management challenges.

ULTIMATE GUIDE

Endpoint Management

Transform how IT and security teams execute changes safely in their environment – at scale, with confidence, and in real time.

ENDNOTES

1 https://www.tanium.com/blog/what-are-endpoint-devices/

2 sophos-state-of-ransomware-2024-wp.pdf

3 Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks - Check Point Blog

4 https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html

5 IT Skills Shortage Expected to Impact Nine out of Ten Organizations by 2026 with a Cost of $5.5 Trillion in Delays, Quality Issues and Revenue Loss, According to IDC

6 Cost of a data breach 2024 | IBM

7 https://owasp.org/Top10/

8 https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m03/cybersecurity-readiness-index-2024.html?CCID=cc004537&OID=rptsc032169&DTID=pdixsp001642

9 CVE count set to rise by 25% in 2024 - Help Net Security

10 IT staff shortages damage the bottom line: IDC report | CIO

11 https://www.infosecurity-magazine.com/news/companies-average-120-days-patch

12 https://www.infosecinstitute.com/resources/vulnerabilities/time-to-patch-vulnerabilities-exploited-in-under-five-minutes/

13 https://www.infosecurity-magazine.com/news/companies-average-120-days-patch

14 https://www.verizon.com/business/resources/reports/dbir

15 https://www.comptia.org/content/research/state-of-the-it-skills-gap

16 2025 Innovation Insights: Autonomous Endpoint Management report., Gartner

17 https://www.gartner.com/doc/reprints?id=1-2IAMNFIT&ct=240806&st=sb

18 https://www.tanium.com/resources/gartner-hype-cycle-for-it-management-intelligence-2024/

TANIUM.

The Power of Certainty.™

Visit us at www.tanium.com and follow us on LinkedIn and X.