



A Comprehensive Guide to

Endpoint Management & Security

FROM THE MANAGED SERVICES EXPERTS AT TPX



Executive Summary

To do business, most of us rely on a variety of endpoints — servers, workstations, phones, laptops or tablets. The health and upkeep of these endpoints is essential to preventing downtime, disruptions and disaster, especially due to cyberattacks.

That's because endpoints often are the weakest links when it comes to security. And while many companies use measures like firewalls and antivirus protection to stave off cyberattacks, those tactics alone are inadequate in today's threatscape. And no matter how extensive your network security procedures, no network is safe when its endpoints are not.

This Comprehensive Guide to Endpoint Management & Security discusses the following:

- What is endpoint management, and why do businesses need it?
- What is endpoint security, and why do businesses need it?
- How does endpoint security compare to other security solutions?
- Why should businesses invest in both endpoint management and security?
- What should businesses look for in endpoint management and security?
- Should businesses in-source or outsource endpoint management and security?
- What should businesses look for in an MSP?
- Why should businesses choose TPx for endpoint management and security?

This guide details everything you need to know to deploy the most effective endpoint management and security solution for your business.

Key Takeaways

- Sixty percent of organizations are aware of fewer than 75 percent of the devices on their networks, and only 58 percent say they could identify every vulnerable asset in their organization within 24 hours of a critical exploit.
- Endpoint management and security are closely related conceptually but are two different practices. Endpoint management enables organizations to see the devices touching their network and manages them from afar. Endpoint security enables organizations to protect these vulnerable assets from impending security threats.
- Endpoint security encompasses a variety of practices, procedures and services that can be layered within a network, including patching, antivirus, EDR, MDR, XDR, DNS filtering and user security.
- Successful endpoint management and security depend on finding the right solution that integrates optimal tools and is backed by a superior support team.

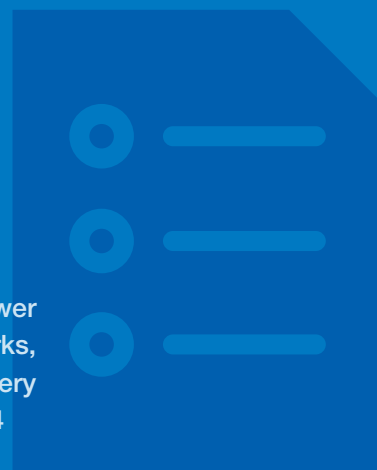


Table of Contents

Part 1: What is Endpoint Management?

- What is an endpoint?
- What is endpoint management?
- Why do businesses need endpoint management?

Part 2: What is Endpoint Security?

- Why do businesses need endpoint security?
- What are the types of endpoint security?
- How does endpoint security compare to other security solutions?

Part 3: Why Should Businesses Invest in Both Endpoint Management & Security?

- How does endpoint management differ from endpoint security?
- Where do they overlap?
- What are the unique capabilities of each?
- Why is it important to have both endpoint management and security?
- Why should all businesses, not just big companies, invest in endpoint management and security?

Part 4: What Should Businesses Look for in Endpoint Management & Security?

- What are key considerations?
- What are common mistakes?

Part 5: Should Businesses Insource or Outsource Endpoint Management & Security?

Part 6: What Should Businesses Look for in an MSP?

Part 7: Why Should Businesses Choose TPx for Endpoint Management & Security?

PART 1

What is Endpoint Management?

Endpoint management is a crucial piece of any business's network management. Thanks to enterprise mobility and the growing popularity of work from anywhere (WFA), a multitude of devices are connected to an organization's network at any time. Protection of that network is vital. Hence, endpoint management is vital.

But, let's start at the beginning...

What is an Endpoint?

An endpoint is any device that connects to your network. The list of possibilities is long and continues to grow as different types of devices are adopted for business use. Examples of endpoints include:

- Desktop computers
- Laptop computers
- Mobile phones
- Tablets
- Servers
- Printers
- Fax machines
- Routers
- Modems
- Cameras
- Smart appliances (GPS, postage monitors)
- Internet-of-Things (IoT) sensors
- Point-of-sale (PoS) systems



What is Endpoint Management?

Endpoint management is the practice of managing and maintaining all of the workstations, servers and devices that connect to your business network. It requires two components:

- **Visibility** — The most fundamental aspect of endpoint management is simply being aware of all devices pinging on your network and providing them access within predetermined policies and guidelines.
- **Maintenance** — Endpoint management also encompasses the ongoing process of ensuring devices are equipped with the right applications and are up to date.

Whether handled in-house or by a third-party, endpoint management usually requires a centralized remote monitoring and management (RMM) platform, which helps monitor usage and security policies and automate support functions like push notifications or patch management that are otherwise executed manually. Platforms like these allow for Unified Endpoint Management (UEM), which brings several heterogeneous devices under the same usage and security policy umbrella.



Why Do Businesses Need Endpoint Management?

Endpoints are among the significant assets for conducting our day-to-day business. But they're also one of the weakest links in our network security. Because of these realities, endpoint management is imperative in today's work culture and threatscape, even as complete endpoint visibility is difficult for many organizations to achieve.

A recent [Cybersecurity Insiders](#) report found that 60 percent of organizations are aware of fewer than 75 percent of the devices on their networks, and just 58 percent of organizations say they could identify every vulnerable asset in their organization within 24 hours of a critical exploit. Nine percent estimate it would take them one week or more.

When you think about the number of devices connected to your network, multiply that by the number of applications your employees use. Defending endpoints requires continuous monitoring and maintenance of both devices and their applications. According to [a recent endpoint risk report](#), enterprises now have an average of 96 unique applications per device. On average, 12.9 of them are mission-critical applications; of those, on average, 11.7 are security controls. The mounting number of applications is itself a security risk since each new control adds complexity to the endpoint environment.

Clearly, the need for endpoint management is great and its benefits are vast. In fact, a report from [Forrester](#) found that 71 percent of organizations plan to extend their ability to see and monitor remote endpoints.

Benefits of endpoint management include:

- Minimized security risk
- Increased visibility and access
- Reduced repair times
- Extended uptime
- Enhanced system performance
- Elevated productivity
- Improved IT usage estimates/budgeting
- Decreased costs



60 percent of organizations are aware of fewer than 75 percent of the devices on their network.

PART 2

What is Endpoint Security?

Endpoint security protects your endpoints from established and emerging cyberthreats. While many companies use antivirus software plus a firewall for network protection, the volume and variety of devices now attached to networks render those standard approaches insufficient. Even with extensive network security procedures in place, no network is adequately protected if its endpoints are vulnerable.

Why Do Businesses Need Endpoint Security?

More endpoints = more vulnerability = greater need for security solutions. According to the 2020 Cost of a Data Breach Report from [Ponemon Institute](#), most security breaches begin at the endpoint – whether from negligence (or malice) on the part of an employee, a security compromise or software vulnerability.

Why is that? Endpoints are at risk not just because of their management complexities but also because of the sensitive data they contain. Endpoints contain sensitive and proprietary information, data and credentials regardless of industry or business function. [Research](#) shows no industry is immune, with an average of 73 percent of analyzed devices containing sensitive data across sectors.

Percentage of Devices with Sensitive Data by Industry

Financial Services – 81%

Professional Services – 81%

Retail – 78%

Other – 77%

Government – 71%

Healthcare – 68%

Source: 2021 Endpoint Risk Report, Absolute



What Are the Types of Endpoint Security?

Since a successful cyberattack could cost your organization millions of dollars, it's essential to make it as difficult as possible for attackers to succeed. A layered defense helps to protect against multiple types of attacks.

Endpoint security encompasses a variety of practices, procedures and services, including:

- **Patching** — The majority of known vulnerabilities already have a fix (or patch), but it takes an average of 97 days for businesses to apply available patches. Hence, timely patching is critical to achieving effective endpoint security.
- **Antivirus** — Antivirus software is an endpoint security technology that has been in use for many years, and your business likely already has an antivirus solution in place. However, since it blocks only known viruses and malware, it catches only 40 percent of today's threats.
- **Next-Generation Antivirus (NGAV)** — In response to traditional antivirus software inadequacies, the industry developed NGAV software, which adds artificial intelligence (AI), machine learning (ML) and behavioral detection, and threat hunting and mitigation into the mix.
- **Endpoint Detection & Response (EDR)** — EDR software can protect against attacks that NGAV misses by leveraging cross-organization analysis to identify more indicators of compromise and automatically mitigate threats.
- **Managed Detection & Response (MDR)** — MDR incorporates EDR software into a suite of outsourced services that monitor and manage your endpoint security 24/7, along with identifying, responding to and mitigating the impact of security breaches.

- **Extended Detection & Response (XDR)** — XDR (sometimes called cross-layered or “everything” detection and response) is a cybersecurity solution that combines several layers of detection and response into a cohesive and comprehensive security platform, protecting multiple types of data and devices via a more integrated approach.
- **DNS Filtering** — Computers use Domain Name Service (DNS) to communicate with the internet. DNS protection services minimize your attack risk and strengthen overall security by blocking computers from accessing internet sites containing malicious content or violating company policy.
- **User Security** — Focusing on user security is crucial to your security solution. There are several components of user security, including security awareness training, phishing simulations and inbox detection and response.
 - **Security Awareness Training (SAT)** — Training users to recognize and report suspicious activity is critical in protecting organizations from cyberattacks. Training content should be easily digestible and delivered via a channel that’s accessible to employees. Most importantly, SAT should be backed by enthusiastic and visible executive support!
 - **Phishing Simulations** — Phishing is the No. 1 way cyberattacks begin. A proper SAT program provides phishing simulation campaigns.
 - **Inbox Detection & Response (IDR)** — IDR enables users to quickly report suspicious emails for further investigation. The software routes the message through automated machine-learning functionality and security expert analysis before being returned to the user for review.

EDR vs. MDR vs. XDR



EDR software leverages advanced techniques to detect threats within its deployed environment. The solution identifies indicators of compromise, investigates the threat’s lifecycle, and takes automatic action to mitigate risks in real-time.



MDR combines EDR technology with human expertise to continuously protect against cyberattacks. Identifying, blocking and quickly recovering from advanced attacks requires a skilled security team that can prioritize responses to create the highest value for customers.



XDR can encompass EDR technology and MDR’s expert analysis and human intervention across silos of data (including offline), thereby coordinating a holistic, layered security approach across an organization. XDR usually includes endpoint, cloud and network security.

How Does Endpoint Security Compare to Other Security Solutions?

Endpoint security versus antivirus: Antivirus is one small piece of endpoint security. Additional layers of endpoint security guard against attacks that antivirus – or even NGAV – leave undetected.

Endpoint security versus firewall: Endpoint protection usually resides on the endpoint, while a firewall resides on the network. A firewall may protect the network from being accessed by unauthorized endpoints but will not protect the endpoints themselves.

Endpoint security versus network security: Network security is *not* endpoint security, nor vice versa. As implied by their names, network security measures are native to the network, and endpoint security is deployed on the endpoints.



PART 3

Why Should Businesses Invest in Both Endpoint Management & Security?

Endpoint Management Versus Endpoint Security

Endpoint management and security are closely related conceptually but are, by definition, two different practices.

- **Endpoint management** enables organizations to see devices on their networks and manage them from afar.
- **Endpoint security** enables organizations to protect these vulnerable assets from security threats.





Where Do Endpoint Management & Security Overlap?

Endpoint management and endpoint security overlap since their objectives are the same: increased control over endpoints. However, they each offer many exclusive features. For example, an endpoint management solution is more likely to provide traffic reports or app usage data, while an endpoint security solution provides insight into threat detection.

Patch management is one key area in which the two solutions overlap. Patch management is usually a feature of an endpoint management solution since it optimizes the applications on that endpoint. However, patch management is also key to endpoint security because out-of-date applications are prime entry points for cyberattacks.

What Are the Unique Features of Endpoint Management & Security?

Endpoint management aims to keep your servers, workstations, and devices performing optimally. Monitoring, reporting and alerts bring your attention to areas that need to be addressed. Endpoint management solutions also support lifecycle planning for hardware and operating systems.

Endpoint security is more specialized. It capitalizes on the visibility that endpoint management provides by closely monitoring and mitigating suspicious or threatening activity on our devices. Furthermore, a layered approach to endpoint security offers extra protection for those endpoints and hence the entire network.



Control of both endpoint management and security by the same team is ideal for gaining holistic visibility and achieving optimum performance and productivity.

Why Is It Important for Businesses to Have Both Endpoint Management & Security?

While some endpoint management and security functions overlap, neither solution tackles all the areas needed to ensure organizational health and resilience. When outsourcing, sometimes one provider handles issues like endpoint patching and RMM, and another takes on endpoint security. Control of both endpoint management and security by the same team is ideal for gaining holistic visibility and achieving optimum performance and productivity.

Why Should All Businesses, Not Only Big Companies, Invest in Endpoint Management & Security?

If you have endpoints and data, you need endpoint management and security. Regardless of size or type of business, your endpoints carry sensitive data – personal identifying information (PII), at the very least, which is also subject to cybertheft.

Endpoint management also is critical for the administration of applications and updates. An endpoint management solution enables your organization to:

- Practice excellent device hygiene
- Optimize performance
- Streamline support and service

PART 4

What Should Businesses Look for in Endpoint Management & Security?

Endpoint management and security solutions come in various shapes and sizes, so it's essential to scrutinize the offerings before selecting the right one for your business.

What Are Key Considerations?

Here are a few things to consider:

- How easy is the deployment? Is the solution cloud-based? Turnkey? Scalable?
- How do you receive reports and how often?
- What areas of endpoint health and hygiene are covered?
- How do you receive alerts? Are they immediately actionable? (Timing is crucial with security monitoring.)
- How does the solution's patch management work? Is patch management automated? Is patch reporting provided?
- What support is provided? Is support available 24/7?
- Does the solution include next-generation antivirus?
- What are the solution's MDR capabilities? Continuous threat-hunting? Event mitigation?
- Does an expert security analysis team monitor the solution?
- Does the service include DNS agent software?
- What type of security awareness training is provided? Is training platform management automated?
- Does the solution offer an IDR component? How quickly are safe emails returned to the user's inbox?



What Are Common Mistakes?

As you're shopping, ensure you find the right tools, a skilled team and the appropriate service approach for your business. Here are a few common mistakes to avoid when choosing an endpoint solution:

- Don't leave management to a generalist. Endpoint management and cybersecurity require the knowledge of a specialized team.
- Don't parse out different pieces of your endpoint management and security to multiple providers. A single solution is better for service, efficiency, cost savings and security.
- Don't choose a solution that doesn't integrate with your operating systems and primary applications.
- Don't select a solution that can't service all your endpoints across all geographies.

And the biggest mistake of all? Thinking your business doesn't need to focus on endpoint management and security.



The Perks of Patch Management

Patch management alone can save you millions of dollars and months of downtime. [Forrester's State of Application Security Report](#) found that application vulnerabilities are the most common cyberattack method, making patch management critical to your company's overall security. In fact, according to the [Ponemon Institute](#), 57 percent of cyberattack victims reported breaches that could have been prevented by installing available patches. In fact, 34 percent of those victims knew of the vulnerability but hadn't taken action.





The bottom line is that [60 percent of breaches](#) result from failure to apply available patches. The cost of improper patch management [averaged \\$4.24 million in 2021](#), and the average time it takes to fix a vulnerability is [205 days](#).

Endpoints require proactive management and security to keep your business efficient and protected.

PART 5

Should Businesses Insource or Outsource Endpoint Management & Security?

In-house endpoint management and security are costly and challenging. As a result, most organizations outsource for both practical and strategic reasons. The table below details some of those challenges and how outsourcing addresses them.

	 Budget	 Tools	 Talent	 Time
In-house challenges	Securing, maintaining and future-proofing adequate investment	Evaluating and sourcing complex, specialized tools	Hiring and retaining specialized talent (the unemployment rate in cybersecurity is zero)	Diverting IT resources from proprietary and business-building activities
Outsourced advantages	Access provider's specialized investments and economies of scale; ability to scale on-demand.	Access best-in-class tools from knowledgeable professionals.	Access rare talent without the headaches of recruitment and turnover.	Access endpoint management and security services expertise without burdening internal personnel or sacrificing high-value projects.

Many companies outsource their endpoint management and security for all these reasons, plus focusing efforts on building the business instead of building a security team). That's because, in most cases, outsourcing isn't just more realistic and affordable but the best option for both business strategy and resource allocation.

PART 6

What Should Businesses Look for in an MSP?

Outsourcing endpoint management and security to a managed services provider (MSP) is the most cost-effective choice for most businesses. However, the all-important security component is crucial to MSP selection.



Many MSPs lack the higher-end security expertise and infrastructure necessary to meet the needs of businesses of all sizes, especially those subject to regulations such as HIPAA or PCI. Additionally, smaller, local MSPs often struggle to provide services outside their home areas or service regions.

Small MSPs also face many of the same resource and availability issues that come with having smaller staffs. As a result, many MSPs become more reactive than proactive, negatively impacting service levels and reliability.

For these reasons – and because your organization's security is at stake – it's crucial to choose an MSP with the scale, financial strength and technical resources (e.g., a 24/7 security operations center) to deliver reliable and responsive endpoint management and security.

What Capabilities Should Your Managed Endpoint Provider Deliver?

Your MSP should have a range of capabilities, including:

Cutting-edge tools to:

- Deliver proactive endpoint management and security 24/7/365
- Provide robust visibility into endpoints and activity
- Protect your endpoints from new and emerging threats
- Track and report endpoint activity across your organization

A world-class team that's:

- Available when needed
- Skilled in multiple disciplines
- Expert in endpoint management and security

Top-tier service, including:

- Automated monitoring and alerting
- Proactive maintenance
- Efficient problem resolution
- Focused attention on your account



PART 7

Why Choose TPx for Endpoint Management & Security?

Achieving effective and reliable endpoint management and security is easy with TPx. We arm you with leading remote monitoring and management tools and a team of industry-leading experts to ensure your endpoints are healthy, productive and secure.

What Are the Key Features of TPx's Managed Endpoint Solution?

- Automated monitoring, alerting and reporting
- Endpoint patching
- Remote endpoint support
- Device lifecycle management
- Managed next-generation antivirus (NGAV)
- Managed detection and response (EDR + service)
- DNS protection
- Security awareness training (SAT)
- Managed inbox detection and response (IDR)



Why Use TPx for Managed Endpoints?

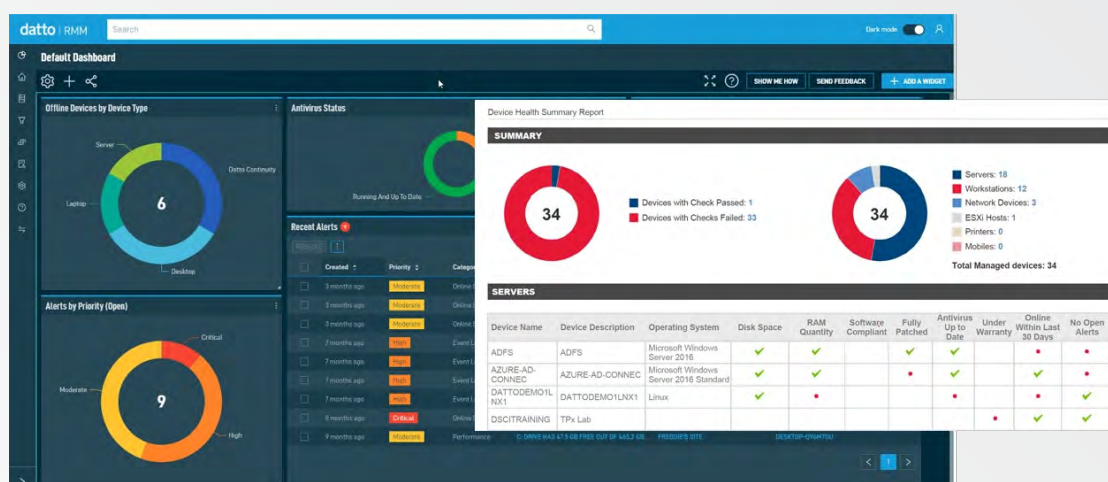
TPx takes the heavy lifting from your endpoint management with:

- Monitoring, alerting and response 24/7/365
- Best-in-class management and security technologies
- Industry-leading 15-minute response time (for MDR)
- Cross-functional experience and expertise
- A virtual IT team is available when you need them
- Proven support methodologies

Benefits include:

- Minimized security risk
- Increased system visibility and access
- Reduced time to repair
- Enhanced system availability
- Improved system performance
- More effective planning

TPx Endpoint Management Dashboard



You can access reports, view device inventory and status, check alerts, take remote control of a device, and run pre-built scripts/processes in your TPx RMM platform.

Why Choose TPx?

You have enough challenges in your business life. You don't also need to worry about data breaches and the potentially catastrophic impact on customer relations, business operations, workflow and your bottom line. At TPx, we have the products, services, experience and certifications to keep your network safe and running smoothly.



We solve the biggest remote IT issues – cybersecurity, connectivity and collaboration – under one umbrella.



Our buying power enables us to customize your solutions for maximum effectiveness within your budget.



We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, AWS, SMC and more.



We combine everything you need – communications, collaboration, security and more – to be your single-source provider.



We provide enterprise-class and white-glove support for ongoing, proactive support tailored to your business.



Our experts become your team members. Instantly gain access to a multitude of remote work expertise without adding personnel.



We modernize your IT, connectivity and communications while minimizing your risk from cyberthreats.



With 18,000 clients in 49,000+ locations, we're big enough to get the job done and small enough to be agile.



We mix and match solutions and deliver a variety of service levels customized to meet your needs, including managed and co-managed options.



We offer a complete WFH solution, including managed endpoints, UCaaS, firewall/VPN and Microsoft 365.



We provide remote administrative support for operating system configuration changes, such as adding users and changing passwords.



On top of the WFH solutions, you can add on other TPx services, such as managed connectivity, to create a custom solution.

All-in-One Managed Services Portfolio Built for Work at Home & Beyond



Managed IT

TPx delivers fully managed and co-hosted IT services that enhance performance, optimize networks and improve system stability. Our best-of-breed technologies combined with our service expertise keep critical IT systems operating smoothly. Join the thousands of companies that trust TPx to manage their IT infrastructure and get the peace of mind you deserve.



Managed Security

With cybersecurity threats growing in frequency and complexity, you need the right security in place to prevent, detect and stop cyberthreats. TPx offers a multilayered approach to security with best-in-class software that is backed by our highly trained security experts. Protect your business and keep your data secure with TPx.



Cloud Communications

Bringing people virtually together is easy with an intuitive unified communications solution like UCx with Webex. It's a single app for calls, messaging, meetings, video, screen-sharing and more. Whether you're a small business, enterprise, or call center, you can experience quality voice and unmatched collaboration capabilities with UCx.



Ready to Take Charge of Your Endpoint Management & Security?

[CONTACT US TODAY](#)