VISION REPORT

The Future Of Endpoint Management

Four Key Trends Will Drive Evolution In The Endpoint Management Market

June 6, 2022

By Andrew Hewitt with Merritt Maxim, Lauren Nelson, Paddy Harrington, Chris Langlois, Diane Lynch

FORRESTER®

Summary

Endpoint management remains both a foundational capability and a difficult challenge for operations professionals as they support today's increasingly remote and hybrid workforce. Luckily, enterprises are increasingly modernizing their approach to endpoint management, resulting in better digital employee experience, improved operational efficiency, and a reduced attack surface. This report describes four primary endpoint management trends around self-healing, security convergence, experience analysis, and privacy protection and offers guidance for IT pros to manage these trends.

Anywhere Work Is Accelerating The Move To Modern Endpoint Management

As we discuss in our recent report The Anywhere-Work Guide For Tech Pros, 2022, Forrester survey data reveals that two-thirds of US firms are moving to anywhere-work models. Fifty-one percent of enterprise leaders indicate that their companies will operate in a primarily hybrid format, and 15% say they intend to move to a "mostly or completely remote model." While tech leaders will need to provide a plethora of new technologies to support the anywhere-work workforce, modern endpoint management will serve as the critical foundation for all these services, enabling IT pros to distribute, manage, and secure the latest anywhere-work technologies. Luckily, the transition to remote work during the pandemic has accelerated the move to modern endpoint management, which has six characteristics (see Figure 1):

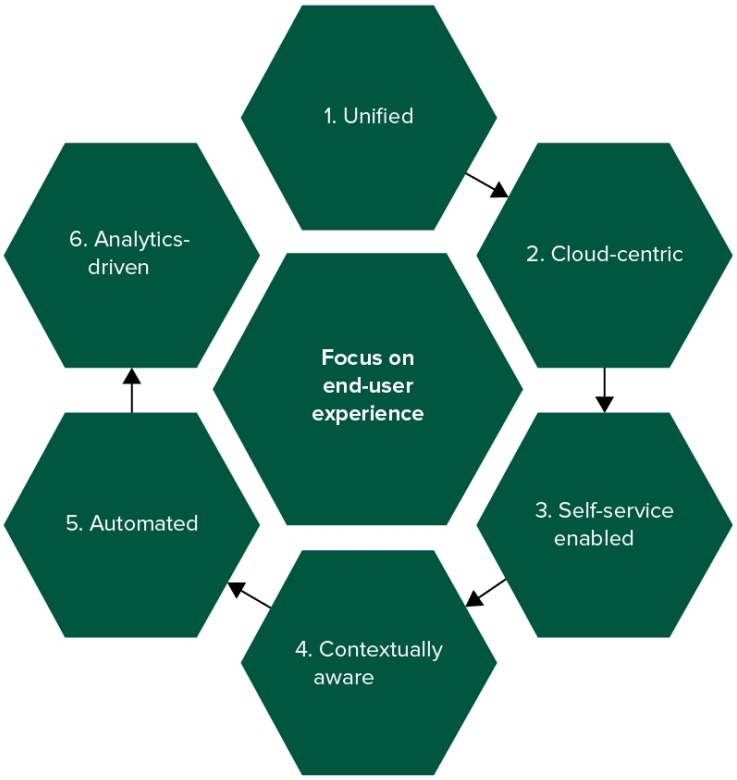
- **Unified: enabling management for all devices and apps.** According to the Forrester Analytics Business Technographics Infrastructure® Survey, 2021, 79% of enterprise infrastructure technology decision-makers say they have two or more operating systems for the company-issued PCs in their organization. Enterprises grappled with remote work in 2020, and that complexity only grew as they increasingly supported bring-your-own-device (BYOD) policies, new form factors like Chromebooks, and virtual desktops. The application landscape is equally complex — one large food distributor we recently spoke with uses 55 versions of Microsoft Excel and 95 versions of Teams. Unified modern endpoint management can tame this complexity by managing all these devices and apps from a centralized console.
- **Cloud-centric: improving support for anywhere workers.** Remote work broke traditional endpoint management processes as organizations struggled to push software patches out via VPN to domain-joined PCs, deployment processes crumbled without in-office staff to image and ship computers, and PC support suffered without in-person troubleshooting. Enterprises are increasingly using cloud to improve patching, deployment, and remote support. One enterprise architect at a multinational food distributor told us, "We don't want to manage a corporate image anymore. Our goal is to purchase the device, configure it with cloud-based APIs, drop-ship it directly from the factory to the end user's house, and automate the entire setup."
- **Self-service enabled: empowering employees with additional choice.** Employees increasingly want self-service capabilities to fix broken devices, choose peripherals, or reset a password. Forrester's 2021 data shows that the majority of

employees (66%) indicate that they would prefer to use a service desk catalog or a chatbot to reset a password. That's good news for IT pros who spend an inordinate amount of time on repeat endpoint issues. A multinational energy company told us, "We're investing significantly in self-service — we recently made all of our devices, peripherals, and home-working equipment available through a portal. Employees choose the tech they need, and the solution will automatically procure it without requiring the employee to come into the office."

- **Context-aware: leveraging user information to inform management operations.** A device-centric approach to management isn't effective when employees increasingly use multiple devices. Companies are now using user-centric endpoint management platforms to apply configuration, adjust policy, and distribute applications across all of a user's devices. IBM's user-risk analytics capability in its MaaS360 unified endpoint management (UEM) product can identify risky behavior on devices (e.g., clicked phishing links, abnormal keystrokes, or files accessed in the middle of the night) and automatically raise risk levels across all of that employee's devices. This dynamic approach to risk can result in multiple remediations, such as alerts, device quarantine, or even remote wipe.
- **Automated: increasing deployment and remediation speed.** Tools such as Apple Business Manager, Google Zero Touch, and Windows Autopilot are gaining popularity as enterprises seek to reduce time configuring and deploying devices. As one senior director of technology at a large financial services company told us, "If we can modernize deployment of PCs with cloud, we can enable employees to go to Best Buy, purchase a device, and have it automatically configure itself — with no IT involvement whatsoever." Automation is also occurring at the policy level. Nationwide is using 1E's Tachyon Platform to ensure that endpoints automatically return to a guaranteed state of compliance if their configuration drifts. This real-time capability enables Nationwide to obtain information from 30,000 endpoints within 30 seconds, significantly improving time-to-remediation.
- **Analytics-driven: collecting telemetry to inform endpoint decisions.** The move to remote work led IT teams to seek more endpoint end-user experience data to understand operational health, security, and performance (see Figure 2). Today's leading endpoint management tools collect information to inform all these areas. Microsoft Endpoint Manager's Endpoint Analytics now provides analysis of startup performance, restart frequency, usage of older software versions, and more. Some organizations, like ABN Amro, are using analytics tools to better understand issues specifically for remote workers. The company uses Nexthink to identify poor VPN performance and suggest possible remediations for remote users.

Figure 1

Modern Endpoint Management Leverages Six Core Principles

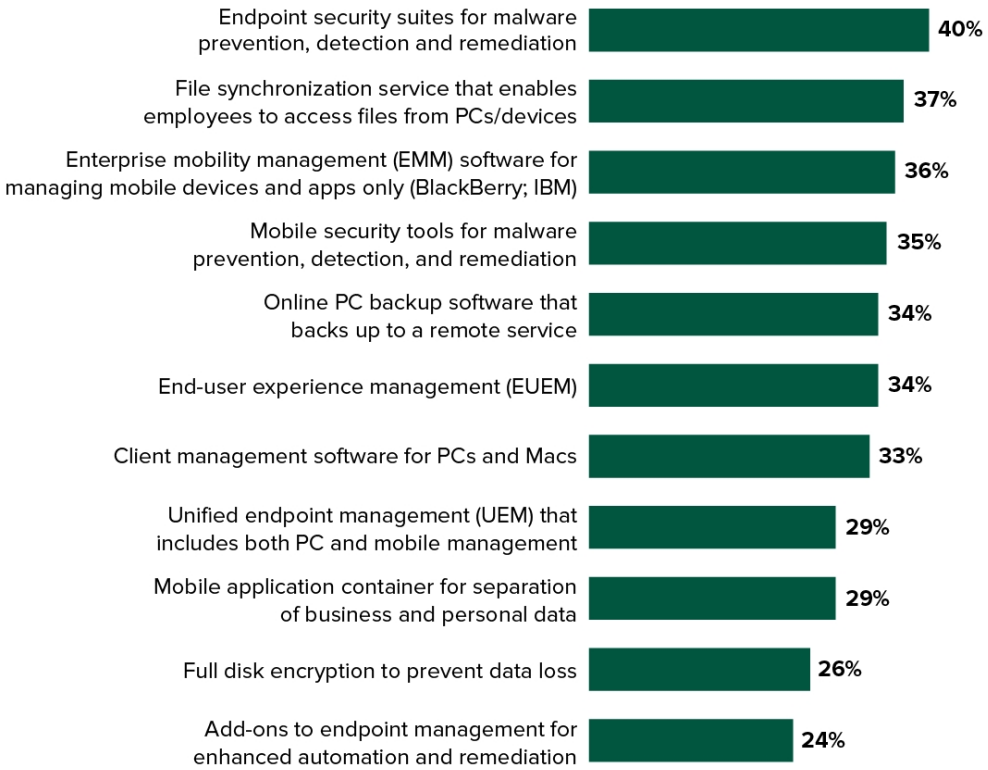


Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 2

Enterprises Will Invest In A Broad Array Of Endpoint Management Tools Over The Next Year

"Which of the following PC and mobile technologies is your firm planning to adopt over the next 12 months?"
(Multiple responses accepted)



Base: 408 infrastructure technology decision-makers
Source: Forrester Analytics Business Technographics® Infrastructure Survey, 2021

Source: Forrester Analytics Business Technographics® Infrastructure Survey, 2021

Despite Improvements, Endpoint Management Still Has Challenges

Despite recent progress, modern endpoint management still presents challenges. Today's administrators see endpoint management as a commodity process that consumes too much time and prevents them from focusing on other strategic priorities. As one IT leader at a government agency told us, "We spend so much time on operations that it prevents us from being strategic." Our interviews demonstrated that today's endpoint management processes are:

- **Too manual and costly.** Many PC lifecycle management processes, from imaging, configuration, management, break/fix, and retirement, consume valuable time and resources. A recent 1E study found that just 10% of service tickets are solved through self-service and that 71% of rebuilds today require reimaging in the office. All this extra work increases costs — a large US healthcare provider told us that it spent over $1 million in break-fix issues in 2021.
- **Divorced from security.** Patch management is critical to endpoint hygiene, but it's only useful if the enterprise has full visibility and control over the endpoint that endpoint security platforms can provide. Unfortunately, the lack of coordination means that many companies struggle to patch effectively. It's not just the technologies that need better integration, either. One senior VP of cloud security at a large US bank told us, "IT admins need far more security-awareness training. If we want to support remote work, everyone needs to understand security."
- **Blind to experience impact.** Endpoint management practices — such as patching, app distribution, and device enrollment — play a massive role in workforce enablement, but most IT teams don't have insight into how management impacts experience. Forrester's 2021 data shows that just 33% of global software decision-makers indicate that they have implemented or are currently expanding end-user experience management (EUEM) software to track experience. One multinational law firm deploys mobile apps to lawyers' phones and uses Aternity's experience-monitoring capabilities to track app usage, reduce licensing costs, and reach out to employees who weren't using the apps yet. Using these insights enabled the firm to gauge the success of its endpoint app deployment.
- **Not well designed to protect employee privacy.** Forrester's Future Of Work Survey, 2021, shows that more than half of employees wish they had more privacy protection in the workplace. Despite the best efforts of endpoint management providers to clarify what data they collect on employee endpoints, many employees still refuse to enroll personally owned endpoints into corporate

management systems. One large US manufacturer that we interviewed found that only 60% of employees wanted to participate in its BYOD mobile program. The remaining 40% refused to enroll due to concerns about the company wiping their data or seeing personal messages and photos.

Four Trends Are Driving Endpoint Management In 2022 And Beyond

While endpoint management administrators will continue to simplify and modernize their existing strategies, our interviews with dozens of enterprise companies, vendors, and experts reveal that endpoint management will evolve substantially over the next five years. As we move into the future of work, endpoint management professionals will need to evolve their endpoint management strategy in response to these four innovative trends:

1. **Self-healing at multiple levels.** The rise of AI within endpoint management platforms will enable automatic remediation of endpoint issues without human involvement. This will go beyond simple if-then policy configurations, utilizing anomaly detection and pattern recognition to “learn” an endpoint’s optimal state and return it to preferred configuration should it drift. Self-healing will need to occur at multiple levels: 1) application; 2) operating system; and 3) firmware (see Figure 3). Of these, self-healing embedded in the firmware will prove the most essential because it will ensure that all the software running on an endpoint, even agents that conduct self-healing at an OS level, can effectively run without disruption. One global staffing company is already embedding self-healing at the firmware level using Absolute Software’s Application Persistence capability to ensure that its VPN remains functional for all remote workers.

2. **Native endpoint security integration.** While lightweight security capabilities (e.g., setting encryption and passwords) have always been key endpoint management features, many vendors today are adding more-sophisticated endpoint security technologies to their portfolios. Endpoint detection and response (EDR), vulnerability management, antiphishing, and biometric authentication are increasingly available natively in leading unified endpoint management platforms. In the future, most enterprise buyers will want a combined endpoint management and security platform to unify visibility across all endpoints. This is already happening: A large French retailer is currently using Tanium to get visibility into off-network endpoints. When the company finds these unmanaged endpoints, it can force enrollment and deploy patches. As companies support anywhere work, we expect endpoint management players to play a significant role in migrating

VPN profiles to Zero Trust Network Access (ZTNA) solutions.

3. **Experience management convergence.** Because of the importance of delivering a strong digital experience to support the future of work, leading endpoint management tools are now building experience telemetry collection and analysis natively into their products. It started with basic endpoint-focused use cases (e.g., decreasing boot-up times) but will expand to apps, networks, authentication mechanisms, and more. Bjorn Braun, senior product manager at HP, told us that the company is increasingly building more analytics into its offer to enable proactive remediation and continual optimization of experience. Customers are still early in their journey to bring experience analytics into their endpoint management platform. As one customer told us, "We're all pioneers in this space. Nobody knows how to cook up the Gordan Ramsay dish-of-the-year digital experience. At this point, we're just trying to make some palatable cheeseburgers."

4. **Data protection without enrollment.** Increasing expectations for privacy, alongside growing interest in BYOD models, means that endpoint management tools will use data- and app-centric protections rather than full device enrollment. Forrester is seeing a rise in stand-alone mobile application management (MAM-only) approaches. This model applies to bring-your-own-laptop use cases and enables the strong separation of enterprise and personal data. It will improve endpoint manageability by reducing the attack surface and will better address employee privacy concerns about employers seeing personal data on their devices. One CISO we interviewed is currently using BlackBerry Access on personally owned laptops to separate work and personal data: "The solution provides more flexibility for employees and is saving us seven figures a year in device management costs because we don't need to enroll the device into MDM."

Figure 3

Endpoint Self-Healing Must Occur At Three Primary Levels

Level	Use case	Sample vendors
Application	ISV vendors will "harden" applications to make them tamper-proof and resistant to performance degradation.	Third-party independent software vendors
Operating system	Endpoint management tools will approach self-healing from the policy configuration perspective. When an endpoint is no longer in compliance, rules-based engines will bring the endpoint back to a prior healthy state.	1E, Ivanti, Microsoft, Tanium, VMware, and other endpoint management agents
Firmware	Firmware-based tools ship embedded within the device and ensure that everything running on the device works correctly (e.g., endpoint agents, VPNs, and software). This remains persistent, even if admins reimage or replace the hard drive.	Absolute Software and Intel

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Supplemental Material

Research Methodologies

The Forrester/Human Resource Executive© Magazine Q3 2021 US HR Decision-Maker Survey was fielded to 719 readers of HR Executive in senior HR roles. Forrester fielded the survey during August 2021. Respondent incentives included a summary of the survey results and a chance to win a $100 Amazon gift card. Exact sample sizes are provided in this report on a question-by-question basis.

This survey used a convenience sample of self-selected group of respondents interested in HR technology and is therefore not random. This data is not guaranteed to be representative of the population, and, unless otherwise noted, statistical data is intended to be used for descriptive and not inferential purposes. While nonrandom, the survey is still a valuable tool for understanding where users are today and where the industry is headed.

Companies We Interviewed For This Report

We'd like to thank the individuals from the following companies who generously gave their time during the research for this report.

Absolute Software

HP

FORRESTER®

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

FOLLOW FORRESTER

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com