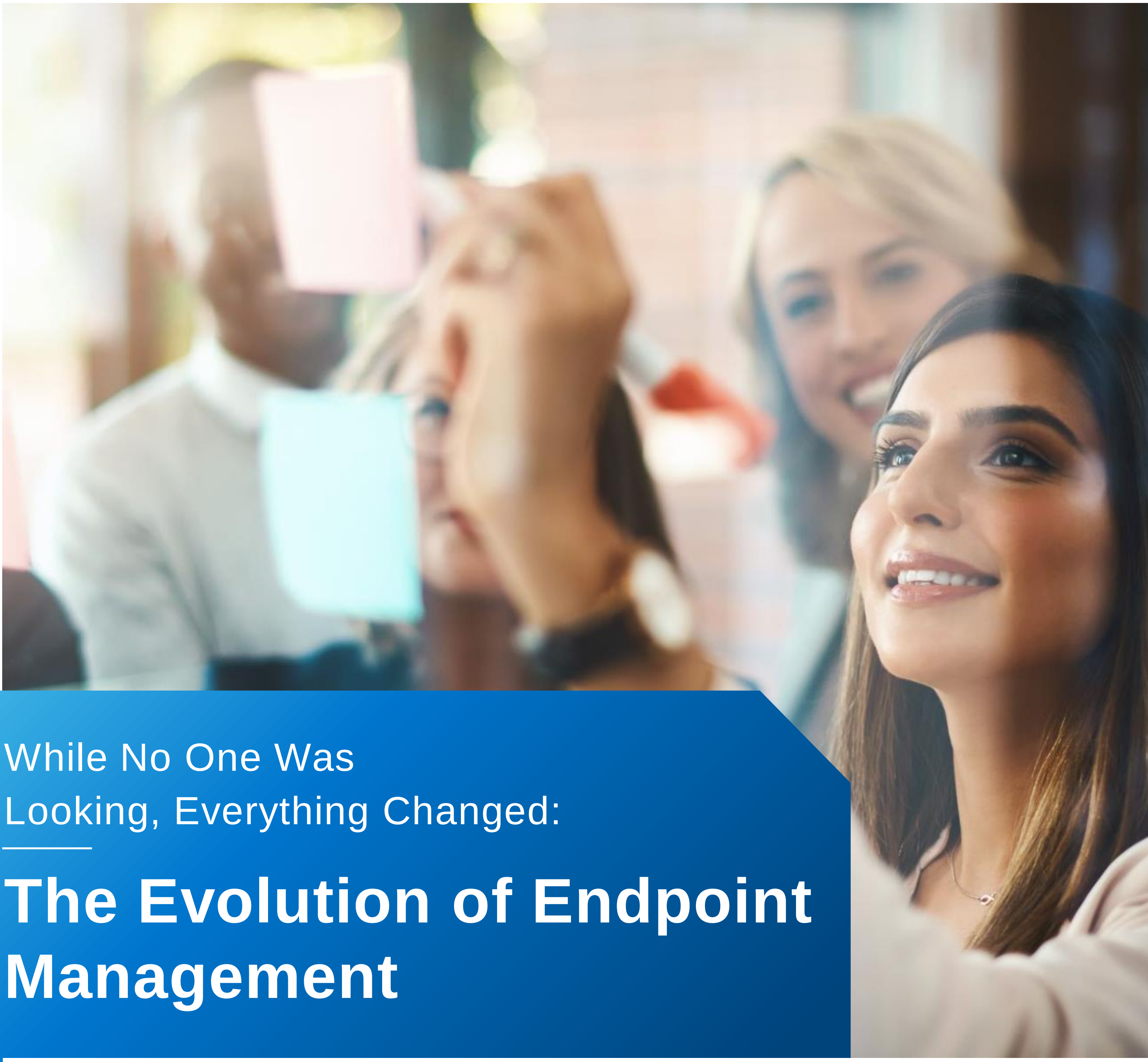


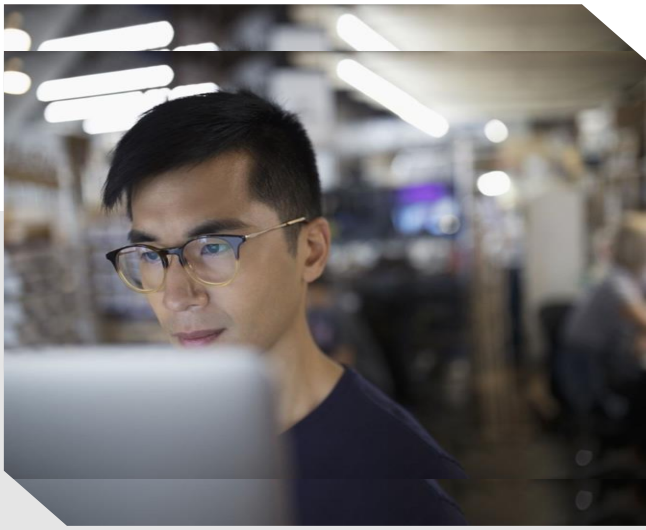
While No One Was Looking, Everything Changed:

The Evolution of Endpoint Management

Part 1: Understanding Problems and Possibilities

Introduction: Why This Matters

Most IT people working with end user computing believe they are up to date on modern endpoint management (also known as unified endpoint management, or UEM), but unless they've been following this domain closely over recent years, they may not be as aware as they think .



59+ million
Dell PC unit shipments in calendar year 2021

~133,000
Dell technologies team members

That's a radical statement but it's not without precedent, because technology is constantly advancing. Everyone knew what computing was until tablets emerged. Everyone knew what cars were until Tesla™ emerged. And so, as technologies shift and new possibilities emerge, it's normal for a mature, well-understood space to be disrupted as innovators embrace new capabilities that provide compelling value to customers.

Organizations are under new pressures and have new possibilities. Endpoint management is a rational place to add new capabilities to help organizations modernize and evolve.

Today's modern endpoint management solutions —typically delivered through a combination of systems management software and tools provided by client manufacturers -- can change the game for organizations of all sizes. But that said, change is usually perceived as difficult, often thought of as giving something up. It's human nature to want to do things the same way if everything is working. However, understanding and embracing the capabilities, versatility and value of today's modern systems management tools can give IT operations unprecedented insight and control that would accelerate operational agility and improve security posture, among other advantages.

Being one of the world's largest endpoint vendors gives Dell a unique perspective. In this two-part series, we will provide an insider's view of the changing world of endpoint management, what the possible opportunities are, and a view of what we offer in conjunction with the industry leaders in endpoint management. After reading these papers, you will be able to better identify your challenges, set your priorities, and take full advantage of the benefits of modern management solutions.

To understand the problems and possibilities of modern endpoint management, it's worthwhile to start with the status quo - the way endpoint management is perceived by the organizations we've spoken with - before covering the emerging possibilities and benefits of modern endpoint management.

Going beyond the status quo

When our endpoint management consultants talk to leaders around the world, we hear statements like these:

> “It’s old but proven - patch and update tools have been around for decades.”

> “It’s a time-consuming chore that’s dull but necessary.”

> “If it goes well, nobody notices. If there’s a problem, everyone complains.”

Of the PCs that are actively managed by organizations today, the vast majority are managed with Microsoft tools.

All these opinions make sense because endpoint management HAS been around for decades. As client-server systems emerged in the 1980s, organizations began to understand the need for a solution that went beyond an IT administrator running from desk to desk installing software, patches, and updates. The Distributed Management Task Force (now known as DMTF, and still active today) emerged in 1992, followed in 1994 with the release of one of the first commercial systems management products, Microsoft’s System Management Server (SMS) 1.0.

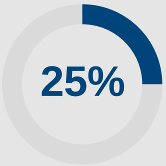
When organizations think about endpoint management, they often reflect on the capabilities included in the earliest tools. The first version of SMS provided a hardware and software inventory, software distribution and installation, and patch/update management — all foundational functions of any systems management approach today.

Today we’ve found that many IT leaders think of endpoint management as a mature and proven set of capabilities that have seen only incremental changes over the years. There is much to be gained from the adoption of new technologies and capabilities for endpoint management, as well as its role in the overall management of the device’s lifecycle.

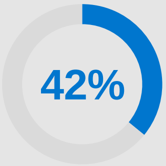
Technology and changes in the working environment provide both possibilities and challenges

Technology itself brings new possibilities but understanding how to best apply and use it can create additional challenges for organizations. It can offer compelling value but requires new thinking. Without new strategies to work with new tools, organizations often find themselves failing to take full advantage of modern technologies, dealing with unnecessary complexity, confusion, and cost. Let’s address some of the more significant changes.

Cloud use in client device management



of enterprises utilize multi-cloud management tools today



of enterprises utilizing PaaS services for mobile services

The cloud isn’t just for data centers. It’s a proven approach to consolidate the management of client devices that increases consistency and simplifies updates across device populations and locations. Cloud-based device management allows changes to be made in one place, tested, scheduled, and rolled out to designated devices. Many organizations have expanded to include both cloud and traditional server-based management of client devices, which provides more flexibility for situations where management must remain on-premises in some locations. The adoption of cloud management increased with the growth of remote work and pushed many organizations using Microsoft SCCM to embrace the use of cloud tools for device updates, which reduced the impact on limited VPN bandwidth. Cloud-based management also allows IT to better control application and OS updates, which often affect end user experience.

Shifts in device variety and volume

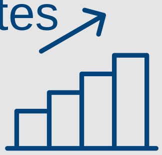
Many organizations provide their employees with at least two devices: a PC and a phone. Some empower their employees with bring-your-own-device policies that add flexibility and employee satisfaction but increase management complexity. To complicate matters further, organizations are beginning to understand the need to manage devices like cloud clients, Chromebooks and peripherals attached to the client device, some of which may function in a closed management ecosystem. Endpoint management is tasked with managing more devices and more device diversity than ever before – also meaning that provisioning devices for low/no touch deployment becomes more important, as it frees IT staff for more important work.

Greater pressures for compliance management and zero trust adoption

Our customers tell us that maintaining compliance is an ongoing, complicated challenge that must be done faster than ever before. Many organizations are also well into their journey to establishing a zero-trust approach – and updated devices have a critical role to play in this. Staying up to date with application and security compliance – with associated patching and updates – can be a full-time effort for multiple resources.

Telemetry

180 zettabytes Of data By 2025[1]



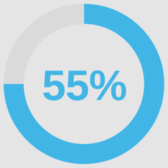
Years ago, clients started to provide ongoing data on performance, system health, and operational status that could be aggregated and analyzed to help organizations make better decisions. As IT operations teams are being asked to cut expenses, boost productivity and accelerate responsiveness, telemetry data and associated analytics provide potential for powerful insights to detect and remediate problems before they impact productivity. Further, telemetry has a key role to play in zero trust, which provides for continual and contextual use of this data to inform management and policy.

[1] Statista.com, Volume of data/information created, captured, copied, and consumed

AI/ML

Autonomous data-driven decision making is an emerging technology that, when powered by artificial intelligence and/or machine learning, offers real potential for improving endpoint management. Being able to automate application provisioning, updates, and problem detection enhances productivity and responsiveness. Using device telemetry as inputs to AI/ML engines is a great opportunity to enhance many aspects of endpoint management and we expect adoption to increase.

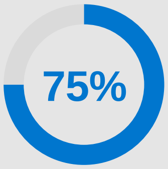
Security



of organizations agree they must assess the risks created by remote worker devices[1]

Endpoint security is a critical concern for organizations and endpoint management capabilities, like the servicing and patching of the OS, help ensure the best possible security profile. Today's organizations are struggling to keep pace with needed updates and resolutions for security. Researchers found that approximately 88% of all data breaches are a result of an employee mistake.[1] Expanding endpoint security capabilities into endpoint management is an emerging approach that adds additional security insight and control, bridging the gap between SecOps and ITOps and helping organizations stay secure.

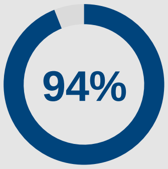
Shifts in where work gets done



of knowledge workers expect a flexible work environment - there is no doubt that the future is hybrid. [2]

Many organizations have shifted from a view of the office being the center of work to being just another tool that employees decide how to use. With the increase in remote working, devices are expected to be delivered to employees wherever they are, ready to be used. Endpoint management must cope with the shift to hybrid work without compromising endpoint performance, security, and stability.

The importance of employee experience



of CIOs believe the IT experience is important when it comes to attracting new talent[3]

Employees today place increased importance on their experience at work, which includes the client devices – and since many are remote, their perceptions of the organization can be greatly influenced by their experience with the technology that's provided to support their work. They are annoyed when their devices don't fully function or shut down multiple times for updates in a day. Further, the "Glassdoor Effect" means that potential employees have more insight into employers and the experience that their current employees have, making this a key factor in hiring as well as retention. Net: client devices and their management are key contributors to employee experience – both good and bad.

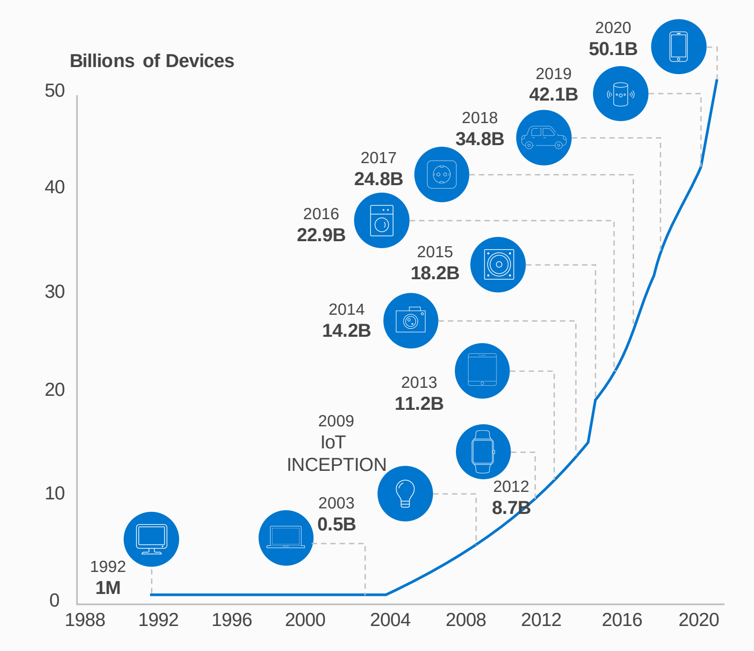
In short, technical and organizational changes are putting pressure on endpoint management toolkits. How are vendors adapting?

[1] Keeper.io: Cybersecurity in the Remote Work Era
[2] Qualtrics: Why CIOs will be at the Center of Future of Work Strategies

Embracing automation capabilities

To cope with the pressures of technological and organizational change, today's management approach must go beyond the old mindset for client devices of just patch and update to take advantage of rich telemetry and data in concert with AI/ML models which reduce effort, help keep devices safe and in compliance, and enhance end user experience.

Today's businesses utilize more devices than ever before. Endpoint proliferation requires a solution that keeps everything managed, monitored, and under control – while capturing the opportunity to use data-rich telemetry from across devices to optimize experiences.



of companies have 10+ monitoring tools, with more than one-third having 30+[1]

Today's modern endpoint management includes:

Systems Administration 1

Remote provisioning, resetting, and repurposing any device remotely is a fundamental function for any forward-looking organization. Without it, manual intervention results in time and energy, resulting in lower end user satisfaction and productivity loss.

Application Monitoring 2

Organizations that can watch performance, use patterns, and identify application vulnerabilities from a centralized platform have a better chance to resolve issues and protect users and organizations from threats.

Automation 3

To cope with distributed scale and skill gaps, automated provisioning, automated remediation of app vulnerabilities, automated system optimization, automated user, device, and application monitoring and automated updates become useful capabilities that improve end user productivity and satisfaction.

Data protection 4

Endpoint management platforms that control data flow outside trusted apps and devices help organizations improve safety, confidentiality, and compliance. This capability is especially useful for organizations with BYOD policies.

[1] StackState: The Shift to Observability. And Why It's Time.

Security Management 5

Managing the deployment and monitoring of your client devices through advanced threat protection working in concert with device security telemetry defends against threats while automating the management and the workflow with SecOps. Problems must be identified and remediated in minutes or disasters ensue.

Telemetry supported policy analytics 6

Constant telemetry provides a foundation for advanced endpoint analytics and data-driven change management at any level, giving valuable insight for configuration, support, and procurement decisions.

Increased scale and span 7

Ideally, progressive endpoint management platforms should allow a single IT administrator to manage more endpoint devices than ever before, regardless of location or connection. The idea is that platforms should make administrators more effective by expanding streamlining workflows while increasing functionality.

Unified insight 8

The trend is toward console and tool reduction but also, towards getting better, more embedded intelligence – AI that automatically improves the user experience without requiring users to leverage a new tool or dashboard.

What comes next

Endpoint management is evolving to meet the technological and organizational changes we've spelled out by rapidly adding new features and functionalities to help organizations. Even as you read this paper, endpoint management vendors are working to improve their products to better align with the problems, possibilities, and technologies of tomorrow.

Now is a good time to explore the landscape of modern endpoint management to start identifying new technologies that align with your priorities. You have great opportunities to take advantage of what modern endpoint management software vendors are doing in conjunction with endpoint device manufacturers like Dell.

Now we've set the stage and given you a broad overview. Take a strong look at your environment and make some assessments.

- **What's working well?**
- **What needs improvement?**
- **What's dangerous or risky?**
- **What could open up new opportunities?**

You're in an unprecedented spot to move from legacy to leading-edge. In the next part of this series, you'll learn more about how Dell solutions can help you take advantage of new technologies and processes to modernize your client management. Visit www.dell.com/command or contact your Dell Technologies sales representative.