



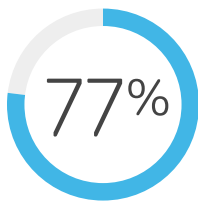
IT Pros Have Their Say on PC Security

The Latest Research and How Dell Technologies' Endpoint Security Solutions Answer the Call



TABLE OF CONTENTS

- Introduction..... **3**
- A Candid Security Self-Assessment..... **4**
- The Truth about End-Users **6**
- Data Coming and Going..... **8**
- The Security Features That Matter **9**
- A Trusted Partner **12**



of IT pros in US mid-market organizations face security-related challenges in device management.

You hear it with unsettling regularity: Your favorite social media platform has exposed the personal information of millions of users. Your preferred hotel chain has had its customer loyalty database hacked. Your healthcare company has reported millions of stolen records. In 2018 alone, 503 health data incidents affected more than 15 million patient records, compared to 5.6 million records in 2017.¹

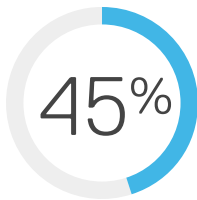
But you don't have to be a large enterprise to be vulnerable to security attacks like these. Mid-market organizations can be just as vulnerable—more so, in some cases, because they may not have the security solutions or in-house expertise to effectively prevent even the most common attacks.

It's no wonder that mid-market businesses across industries, from financial services to manufacturing, report that security continues to be a top challenge. This challenge can be particularly acute when it comes to protecting devices, given that IT has to give up a certain amount of control to the users of those devices. According to a recent survey conducted by Spiceworks, 77% of IT pros in US mid-market organizations face security-related challenges in device management.

This white paper takes a deep dive into that number, exploring the specific security challenges IT pros face securing devices, and how they go about addressing them. It also takes a closer look at Dell Technologies' endpoint security solutions and how partnering with Dell can help organizations close their PC security gaps.



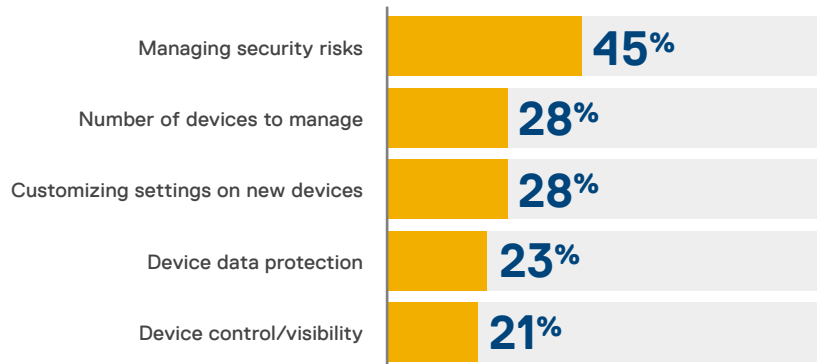
A CANDID SECURITY SELF-ASSESSMENT



of IT pros in mid-market organizations report that managing security risk at the endpoint is the #1 challenge they face.

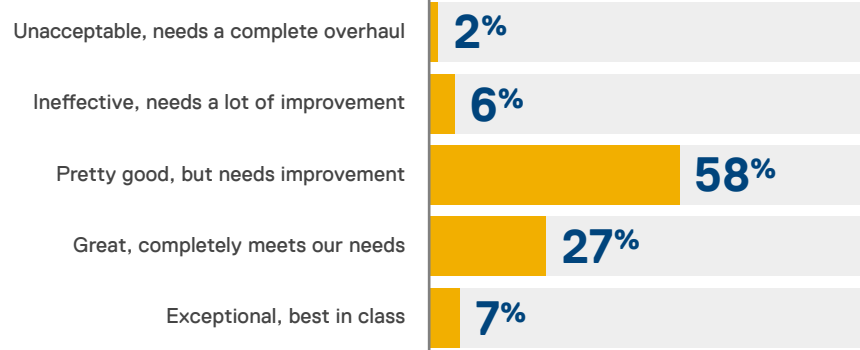
IT pros face challenges in every corner of the infrastructure. But according to the Spiceworks survey, 45% of IT pros in mid-market organizations report that managing security risk at the endpoint is the #1 challenge they face. That's 17 percentage points greater than the next challenge. Device data protection and device control and visibility also ranked in the top five.

The top 5 challenges IT pros face in managing end-user devices



All told, a net 77% of respondents reported facing security-related PC-management challenges, and that's where self-assessment comes in. About one-third of survey respondents say their device security management practices are great, maybe even exceptional, completely meeting the needs of the business. But two-thirds say the opposite. Their practices need improvement, in some cases *a lot* of improvement. Some go so far as to say that their practices need a complete overhaul.

How IT pros rate their end-user device security management practices



Given both the size of the challenge and the resources required to address it, IT pros in mid-market organizations need to develop a strong endpoint security foundation, managing risks to IT assets and data with a holistic and proactive approach. With cyberattacks becoming more sophisticated, more frequent, and more widespread, mid-market organizations increasingly need enterprise-grade protection but without the cost and complexity of enterprise solutions.

Meeting these challenges requires technology that has security designed-in, is easy to implement and manage, and provides industry best practices for IT security. Dell Technologies offers scalable endpoint security solutions that can save your organization time and money while helping to keep your infrastructure insulated from cyberattacks.





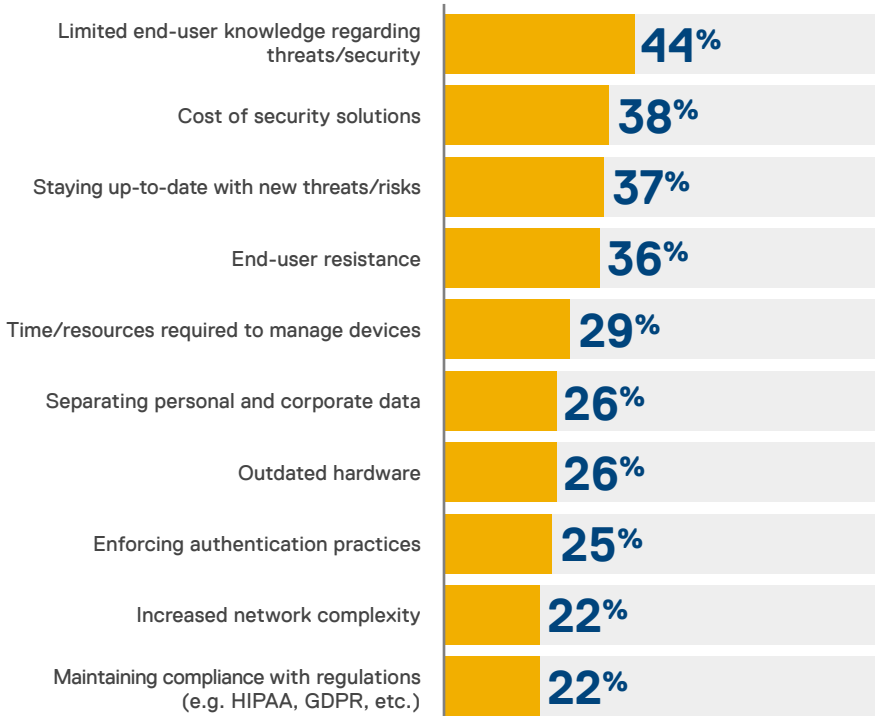
THE TRUTH ABOUT IT END-USERS

#1

End-users are the **#1 security challenge** according to IT pros in mid-market organizations.

When asked specifically about the challenges surrounding PC security management, IT pros in mid-market organizations provided a long list. Their top 10 challenges fall across a wide range of categories, including hardware, compliance, network complexity, and, of course, time and resources. But the #1 security challenge is end-users. These IT pros placed it a full six percentage points higher than the next-highest challenge, which is budget.

The top 10 challenges IT pros face in managing PC security



Respondents included four different end-user issues in the top 10: Limited end-user knowledge regarding threats and security practices, end-user resistance to security efforts, the challenge of separating personal and corporate data, and enforcement of user authentication practices.

Organizational research has attempted to quantify this bad behavior. According to Dell-commissioned research, 72% of employees say they are willing to share confidential data externally, often for the sake of boosting their own productivity.² In fact, 43% say they were directed by management to share confidential data.²

The bottom line is that end-users are the reason security processes have to be automated, the reason security policies have to be enforced programmatically, and the reason security features need to be built into the hardware. Users are unlikely to change their behaviors or prioritize security. Your security strategies have to balance productivity and security in a way that works for everyone.

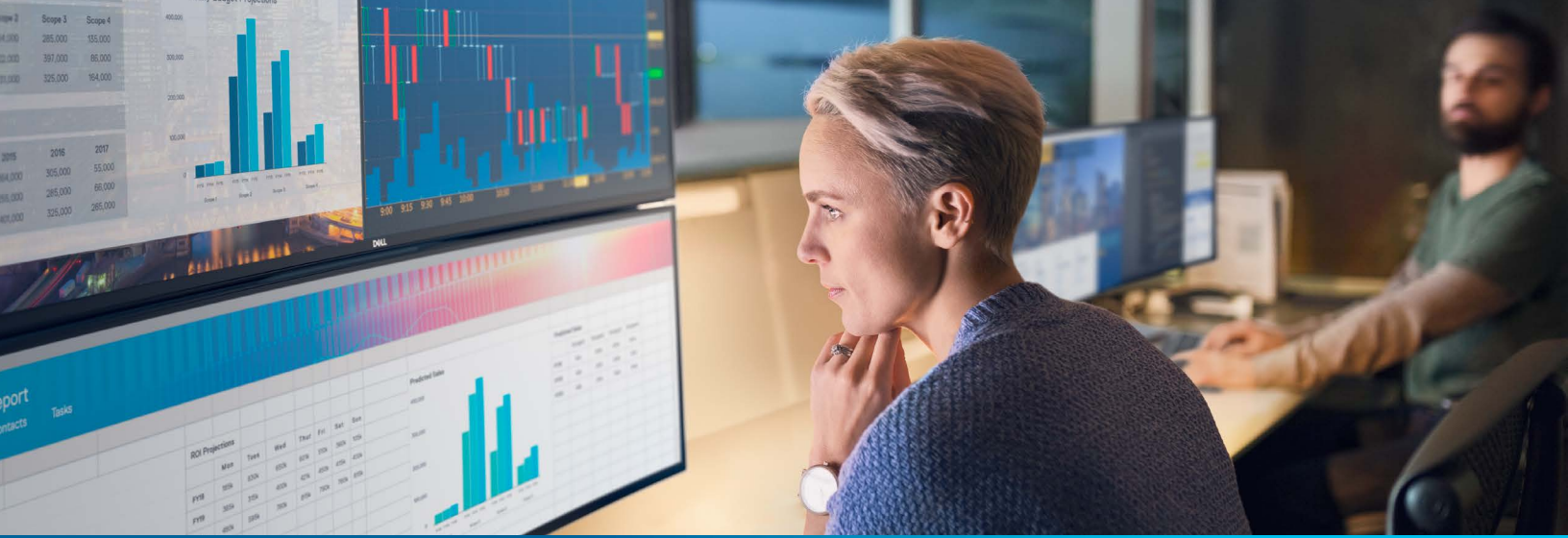
To that end, Dell Technologies delivers the most secure commercial PCs, providing protection against physical and digital attacks.³ These devices enable authenticated users to work, collaborate, and share data safely, reliably, and efficiently. You can trust that sensitive information is protected wherever end-users work—even outside the firewall.

Dell's industry-first and Dell-only security features include BIOS-level protections, multifactor authentication hardware, and an array of installed and optional security software, all designed to help protect your IT ecosystem at every endpoint.

In Their Own Words

What are IT pros' biggest frustrations with end-user device security?

- ◆ “The biggest frustration with securing end-user devices has always been, still is, and probably will always be, the end-users themselves.”
- ◆ “My biggest pain point is the end-user’s lack of concern for data security.”
- ◆ “People will click any link, especially if it’s from Facebook.”
- ◆ “Typically end-users don’t like change. After any change, we hear grumbles.”
- ◆ “The user will always find a way to circumvent security protocols.”
- ◆ “There has to be a balance between usability and security, and that balance shifts depending on the security level of the data in use.”



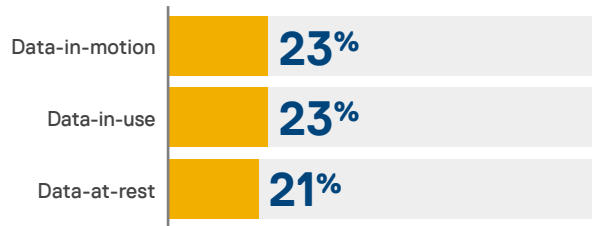
DATA COMING AND GOING



Data-in-motion is susceptible to hacking, data-in-use is susceptible to malware, and data-at-rest is susceptible to physical theft.

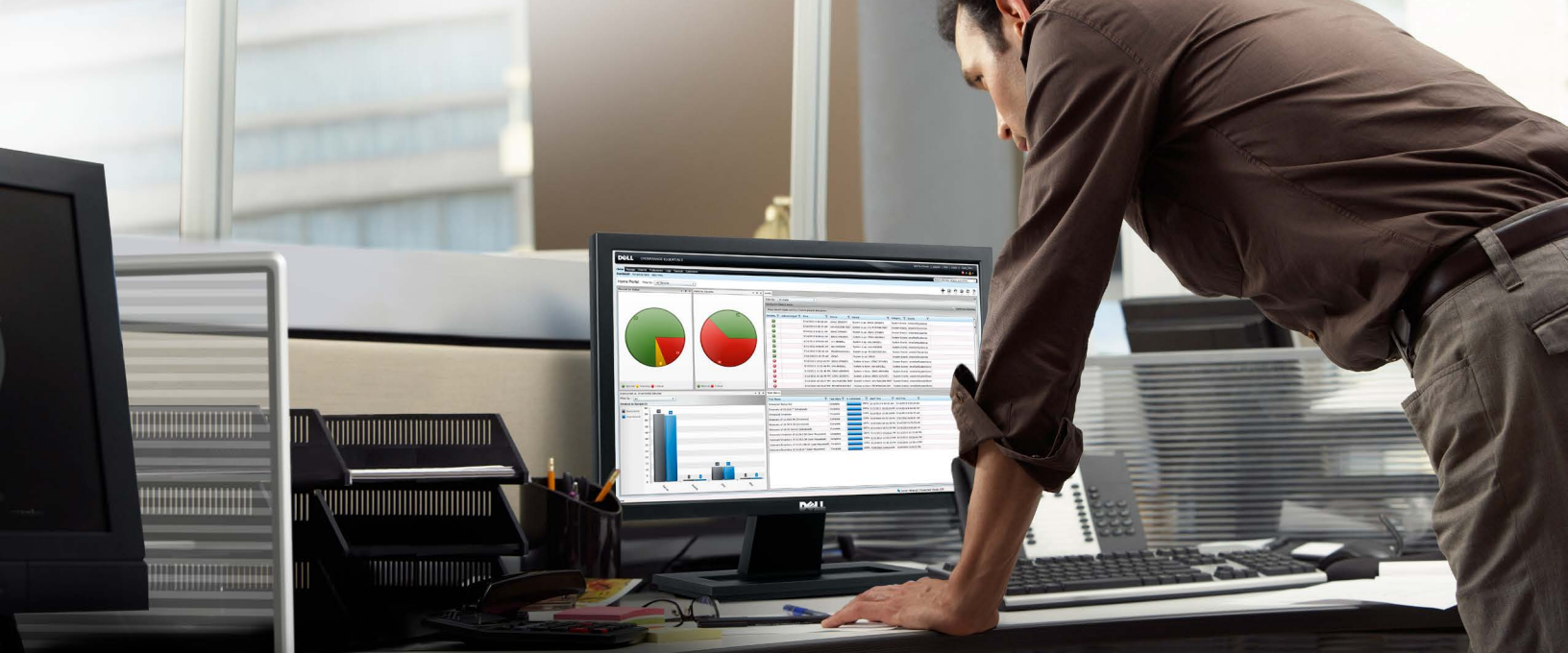
While data protection does appear in the survey's top 5 list of device management challenges, slightly less than one-quarter indicated that it was a problem. Likewise, less than a quarter reported that data-in-motion, data-in-use, and data-at-rest each were at high or extremely high risk.

Types of data IT pros rank as high or extremely high risk




These responses may not reflect the true risks associated with device data, especially given the high level of risk IT pros associate with endpoint security. Data-in-motion is susceptible to hacking, data-in-use is susceptible to malware, and data-at-rest is susceptible to physical theft or improper sanitization or disposal. Although IT pros rate the risk approximately the same for each type of data, each one requires its own protection mechanisms. For IT pros who don't have the time, resources, or expertise to parse out security requirements for each type of data, a single-source solution is critical.


You need to be able to authenticate users, control access to data across the entire IT ecosystem, and monitor data use in real time. Dell, the #1 leader in data protection, provides data security and data protection solutions that help end-users stay productive while data stays protected. These solutions are built to ensure that industry-leading security is standard from the BIOS to the working environment, establishing a platform root of trust.




THE SECURITY FEATURES THAT MATTER

Whether it's data security, identity security, or device security, IT pros rank every category high in importance.

 **Data security**, including encryption, remote erase/wipe capabilities, secured browsing, data removal, and visual hacking protection, was ranked somewhat or very important by 97% of survey respondents. A strong majority of them—69%—described it as *very important*.

 **Identity security**, including passwords, biometric access controls, and automatic logoff, was also ranked somewhat or very important by 97% of respondents, with 64% describing it as *very important*.

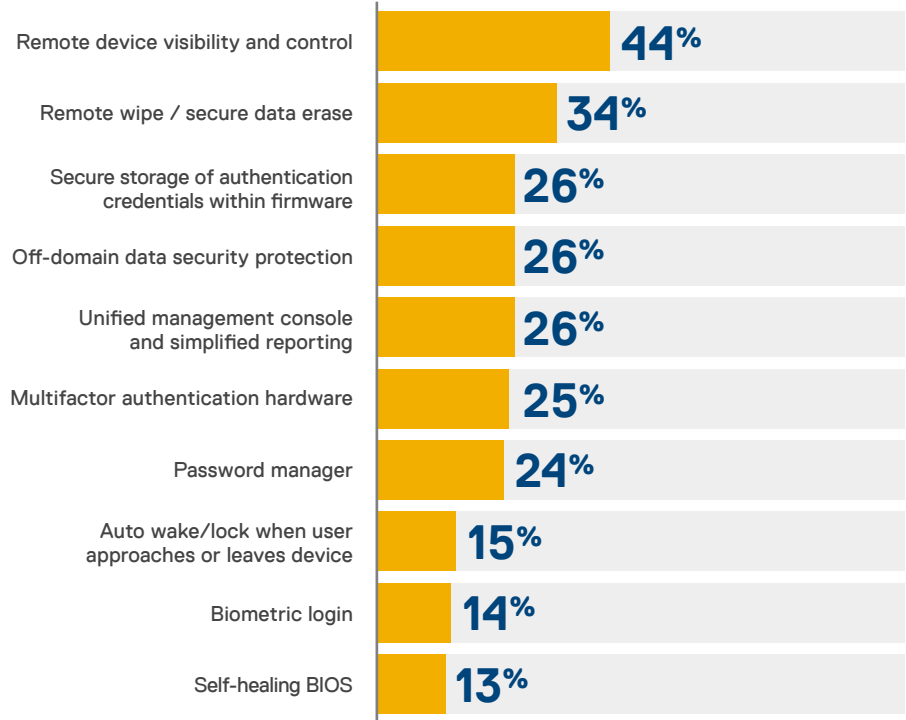
 **Device security**, including BIOS firmware/boot protection and automated intrusion detection, was ranked somewhat or very important by 95% of respondents, with 62% describing it as *very important*.

How IT pros rate the importance of specific security categories

	Not important	Somewhat important	Very important
Data security	3%	28%	69%
Identity security	3%	32%	64%
Device security	5%	33%	62%

To meet today's security needs, IT pros look for a number of PC security features and functionality when evaluating new devices.

The 10 most important PC security features



That's why Dell Technologies offers numerous industry-first and Dell-exclusive features that instill trust in the security of your device ecosystem.



SafeBIOS: This exclusive off-host BIOS verification guards the PC BIOS from low-level attacks while providing visibility to unplanned changes. Only Dell maintains a protected image off host to verify BIOS integrity.



SafeID: Available only from Dell, SafeID provides ironclad authentication integrity by securely storing and processing credentials in a dedicated security chip. SafeID keeps passwords, biometric templates, and security codes within firmware, locked away from a malicious application attack. It helps protect login integrity by isolating authentication routines from the OS environment and memory, it helps protect against password theft by malware, and it stores all credential types to allow a single point of migration.



Express Sign-in: Dell is first to offer a proximity sensor in its business-class devices that can wake the PC when the user approaches and auto-lock the device when the user leaves. In conjunction with optional identity-secured logins—including facial recognition and third-party software such as Windows Hello—Express Sign-in enables more secure, efficient access to help authorized users stay productive.



Intel® Authenticate: This hardware-enhanced multifactor authentication solution is embedded in Intel® Core™ vPro™ processors across Dell's portfolio. Hardware options include fingerprint readers and smart cards.

In Their Own Words

Why do IT pros trust Dell?

- ◆ “We’ve never had any issues with Dell, and they’ve stayed on top of security trends over the years. They also offer a range of options, such as smartcard access and fingerprint readers.”
- ◆ “Dell offers secure solutions and has a broad portfolio.”
- ◆ “Dell makes a good, reliable product.”
- ◆ “They have a history of secure, hardened workplace devices.”
- ◆ “They have spent the time and effort over the years to be a proven secure provider of end-user devices.”



A TRUSTED PARTNER

Security begins with the endpoint. With Dell Technologies as your security solutions partner, you can focus on business priorities knowing that only authorized users can access your devices, and that customer data is protected at rest and in motion—everywhere it goes.

Unlike a multi-vendor approach that results in piecemeal solutions, Dell Technologies can simplify IT for organizations by serving as that single trusted partner. Dell Technologies provides hardware, software, and services that support in-house IT teams, freeing them up for higher-value tasks while saving time and money. With Dell Technologies, you can unify your security approach, helping you stay ahead of threats and giving you piece of mind.

[Learn more](#)

DELLTechnologies

About the Survey

Dell Technologies commissioned Spiceworks to conduct a survey in April 2019. This survey targeted IT professional and decision makers in mid-market organizations to understand current perceptions and practices around end-user device security. Survey results reflect responses from 256 participants in organizations in the US with 100 to 500 employees.

Sources

- ¹ Bryant, Meg, "Data breaches compromised 15.1M patient records last year," *Healthcare Dive*, February 13, 2019. <https://www.healthcaredive.com/news/data-breaches-compromised-151m-patient-records-last-year/548307>
- ² Seals, Tara, "Employees Are Sharing Confidential Info at Alarming Rates," *Infosecurity*, April 24, 2017. <https://www.infosecurity-magazine.com/news/employees-are-sharing-confidential>
- ³ Based on Dell internal analysis, November 2017