Do You Think Your Endpoint Security Strategy Is Up to Scratch?

The IDC–HP Inc. Endpoint Security Survey

Authors:

Mark Child
Dominic Trott
Andrew Buss

IDC #EUR145260919 NA

An IDC InfoBrief | October 2019

IDC ANALYZE THE FUTURE

An IDC InfoBrief, Sponsored by hp

Executive Summary: Endpoint Security Survey

On behalf of HP Inc., IDC surveyed 500 security decision makers and influencers at organizations in key European (300 respondents from the U.K., France, and Germany) and North American (200 respondents from the U.S. and Canada) markets, across vertical sectors from across the spectrum including banking and finance, telco, and energy.

Respondents were questioned on a wide range of key factors related to their organizations' approach to endpoint security. The results, as described in this IDC InfoBrief, indicate considerable scope for critical improvements in business cybersecurity awareness.

Based on responses to key questions, IDC also segmented the respondents into two groups: "Leaders" (defined by a proactive, best practice approach to endpoint security throughout) and "Followers" (often unaware of the risks associated with their endpoint devices and still with a way to go in terms of adopting a safe approach to managing their endpoint estate).

The research findings are concerning:

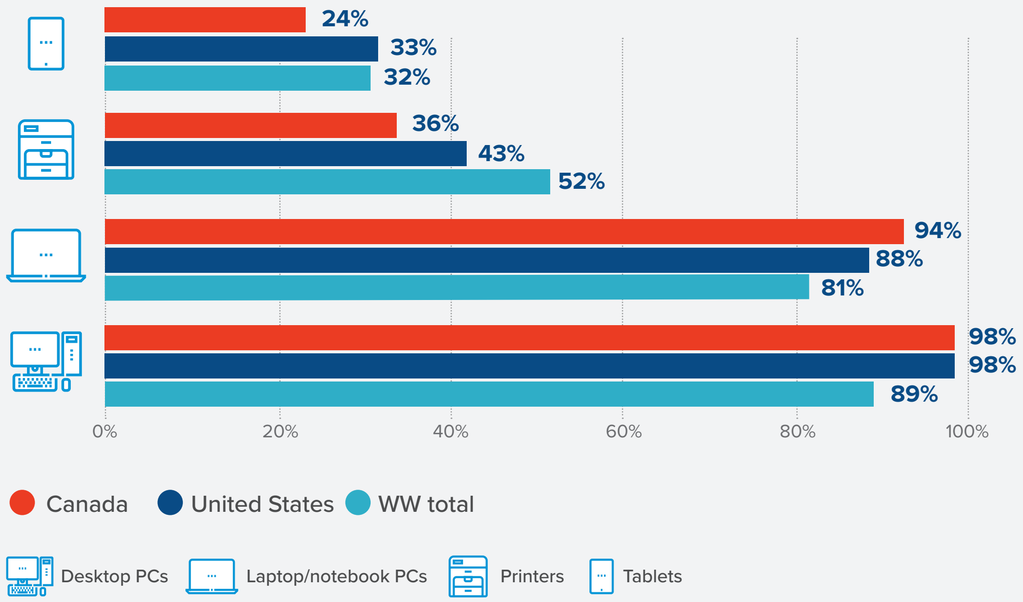
- **Many organizations do not manage endpoint security strategically, have an inconsistent approach across different endpoint types, and do not fully comprehend the risk associated with all endpoints.**
- **This results in inadequacies in processes and procedures, such as failing to include security capabilities in endpoint procurement requirements or retaining legacy devices even after they are found to have intrinsic security vulnerabilities.**
- **Even when acquiring new devices, organizations still have widely differing priorities, with security often a secondary consideration after factors such as cost and performance. What those organizations fail to appreciate is that once an endpoint has been compromised and provided an entry point to their network, the cost and damage to the business can be far greater than the savings they made or gains they achieved.**

Endpoints Are Not Considered as Equal Security Risks

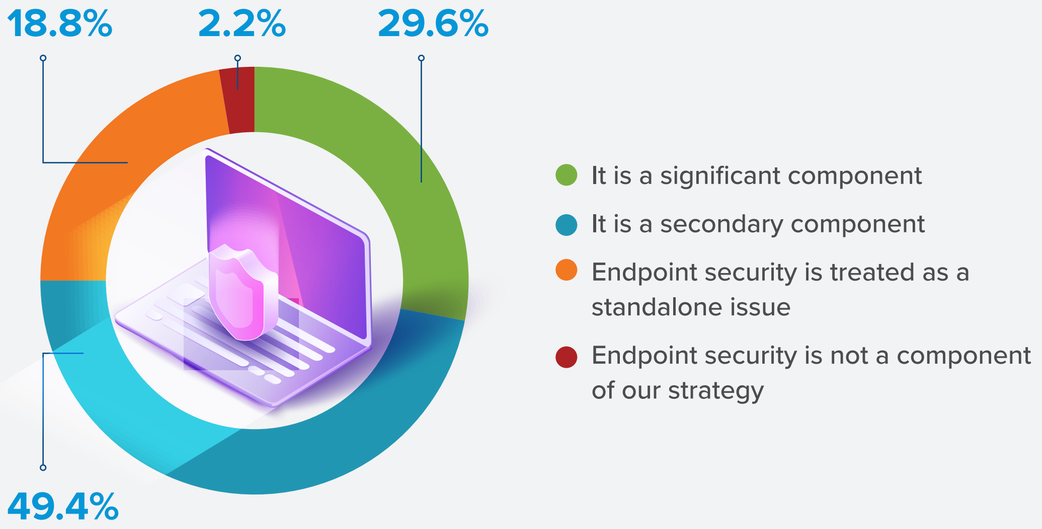
Endpoint devices are ubiquitous at all organizations and all carry risk in terms of potential for data compromise, loss, or theft.

Despite that, PCs are far more likely than printers and tablets to be included in the organization's cybersecurity strategy.

Which devices are typically included in your organization's consideration of endpoint security?



To what extent does endpoint device security form a significant component of your organization's overall cybersecurity strategy?

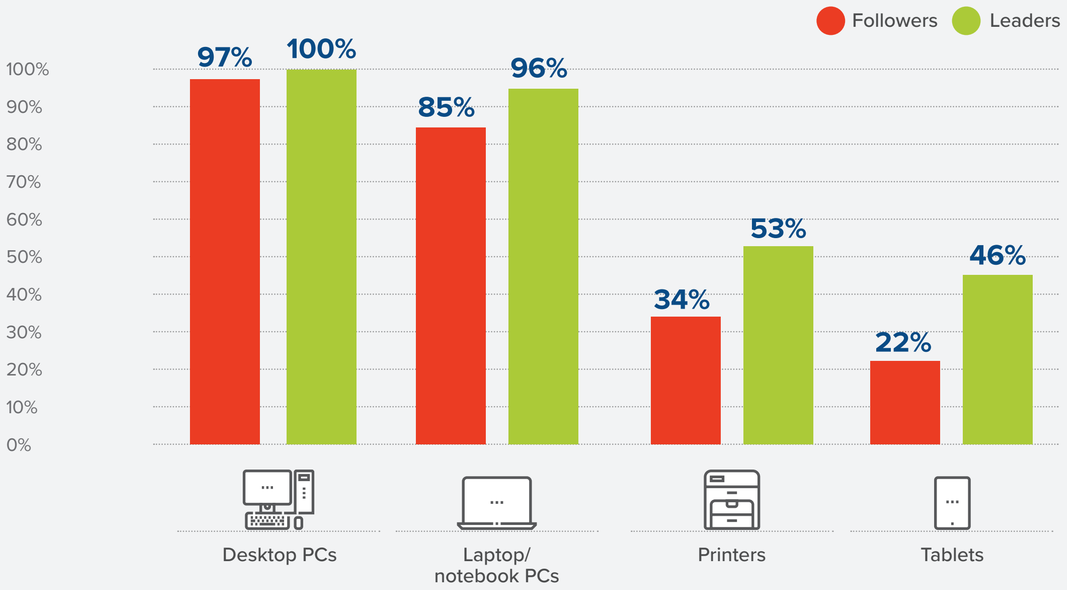


IDC research shows that almost half of companies treat endpoint security as a secondary issue and do not address it with the strategic and holistic approach it requires.

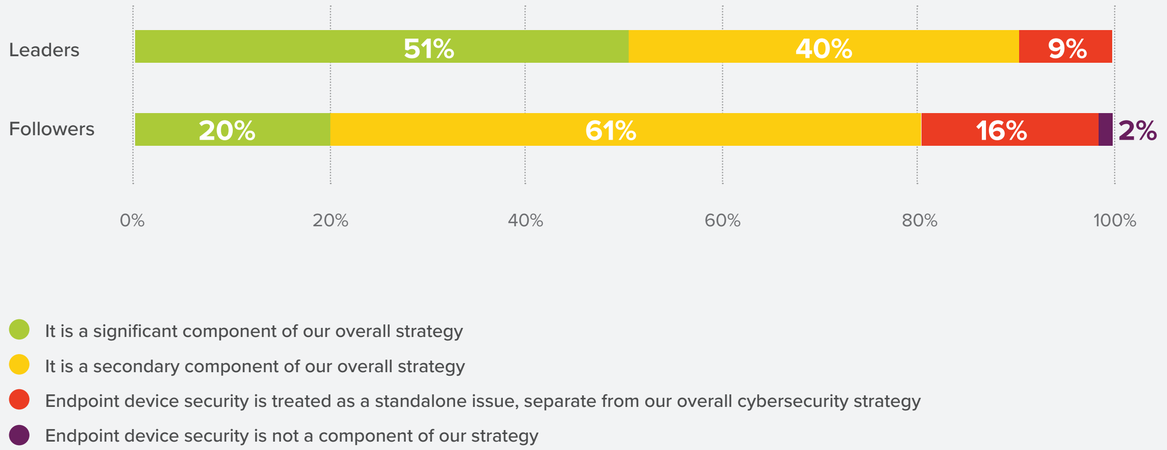
Security Leaders View Endpoints as Key to Safety

Based on the survey responses, we segmented the respondents into Leaders (which follow a proactive, best practice approach throughout) and Followers (which still have a way to go). The differences are clear from the outset:

Which devices are typically included in your consideration of endpoint security?



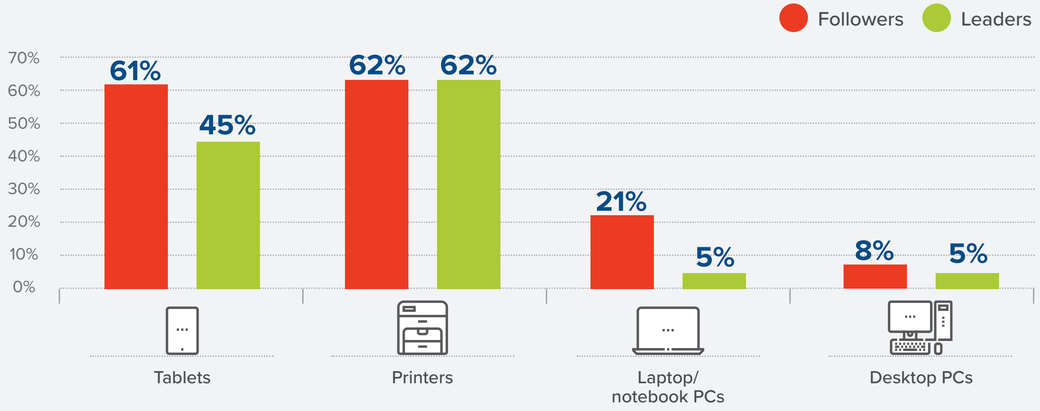
To what extent does endpoint device security form a key component of you organization's overall cybersecurity strategy?



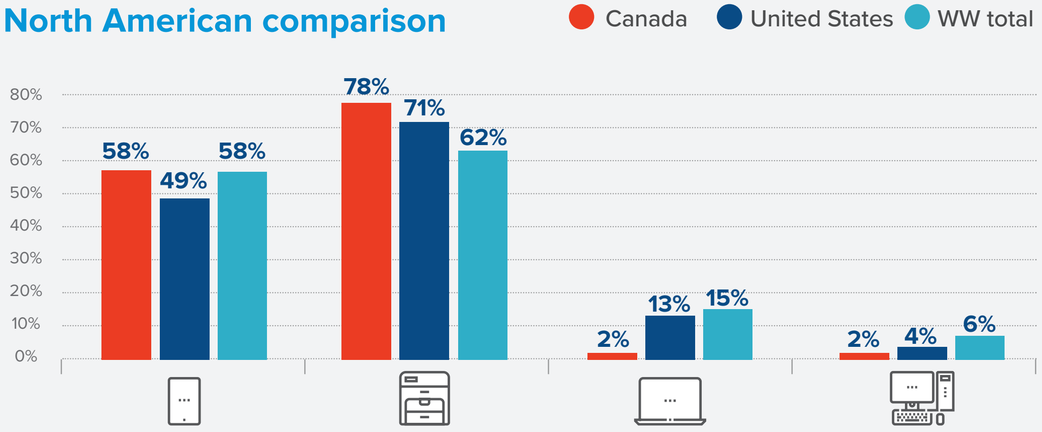
Security Leaders attach greater importance to all endpoint types and see endpoint security as a significant component of the overall cybersecurity strategy.

Endpoints Come With a Skewed View of Risk

The dangers of complacency — the share of respondents assessing endpoint types as low/no risk



North American comparison



Printers and tablets are viewed as much lower risk than desktop and laptop PCs, but the reality is that all these endpoint devices can be targeted in the current threat landscape.

Companies should apply the same level of security policies, practices, and feature requirements for each category of device, and raise the level of expectations across the board.

Misreading of Risk Impacts Procurement Decisions

When selecting/purchasing endpoint devices, are security requirements unspecified in requests for proposals (RFPs), invitations to tender (ITTs), or other procurement documents?

22%

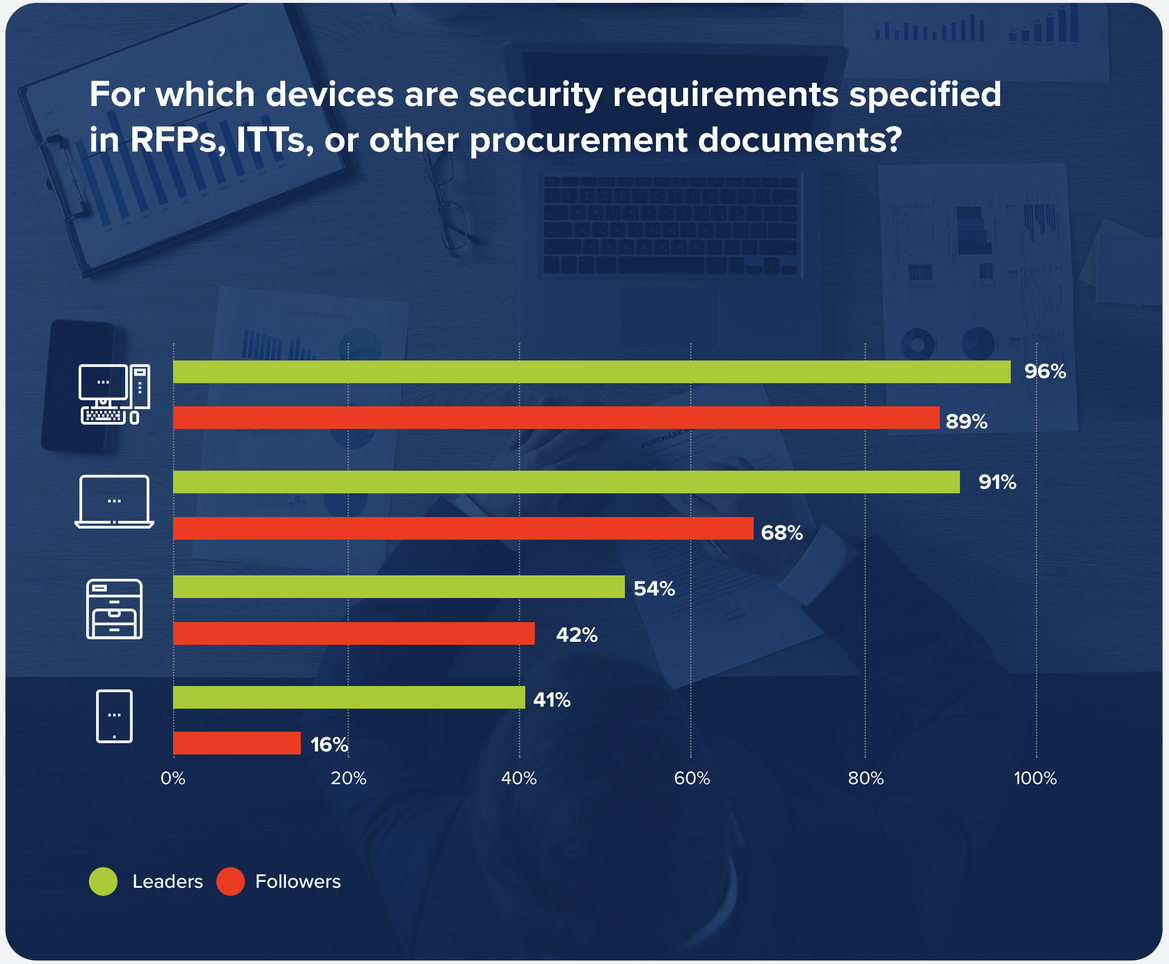
25%

28%

Despite tough privacy regulations coming into force, almost a third of companies are failing at basic security diligence when it comes to endpoint procurement.

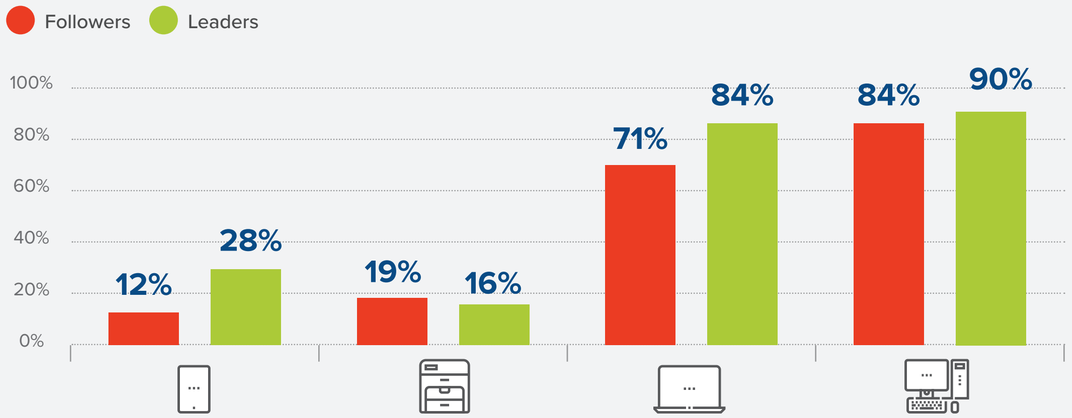
Though most organizations include security requirements in procurement requests, those requirements are not specified equally for all endpoint device types, resulting in uneven security coverage and compliance risk.

Followers lack security focus for everything other than desktops during procurement.

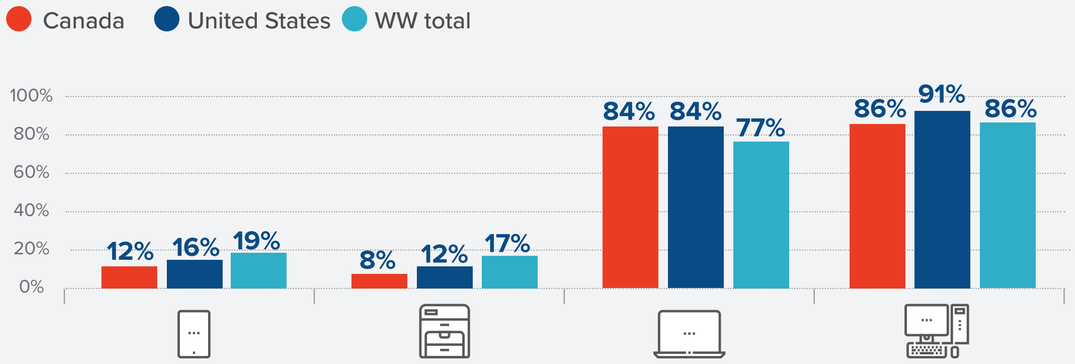


Less than 20% of Companies Consider Printers as Essential

To what extent is security a primary consideration/requirement when making procurement decisions for the following types of endpoints?



North American comparison



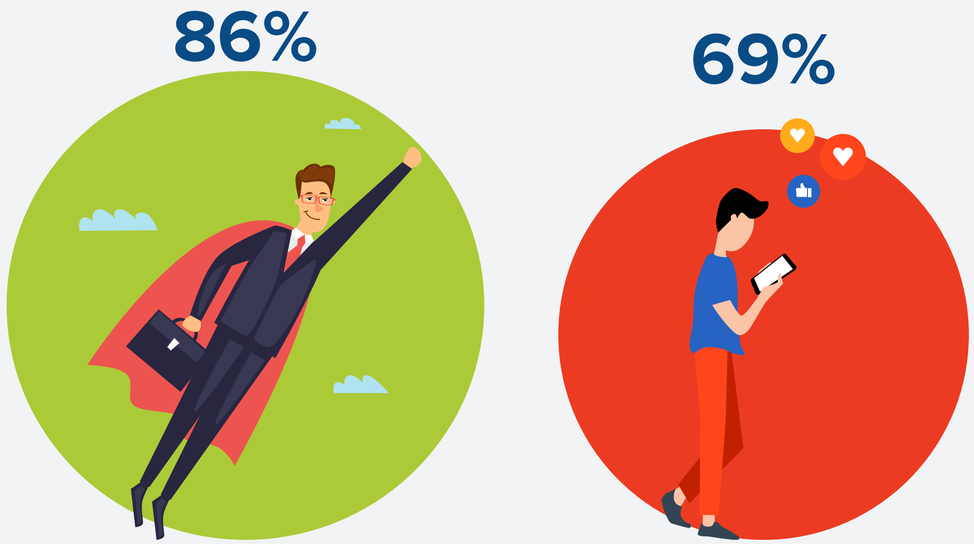
Organizational structures and processes drive differences in purchasing and management of devices.

Printer support has long been outsourced by facilities/procurement, but responsibility for security is often not assigned in these contracts. PCs are in the purview of the IT department, but the risk/benefit trade-offs of addressing endpoint security are overshadowed by other security and operational priorities.

Source: IDC/HP, IT Endpoint Security Survey 2019, n = 500

You Wouldn't Trust a Safe With No Lock

When selecting/purchasing endpoint devices, are security requirements specified in RFPs, ITTs, or other procurement documents?

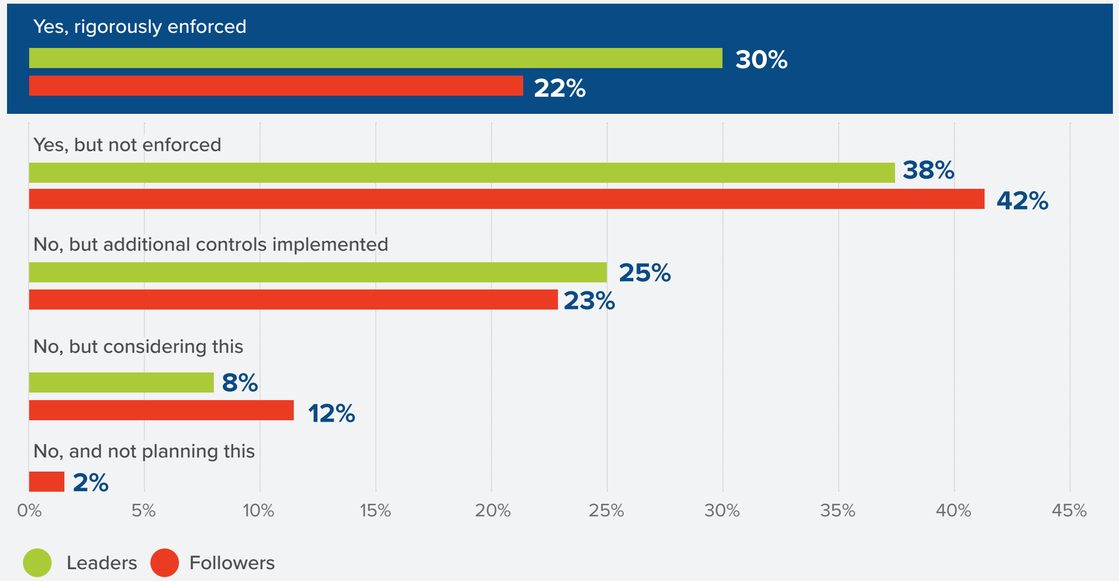


Leaders Followers

Security Leaders include security as a procurement requirement ...

... and are ready to retire devices that are a security liability

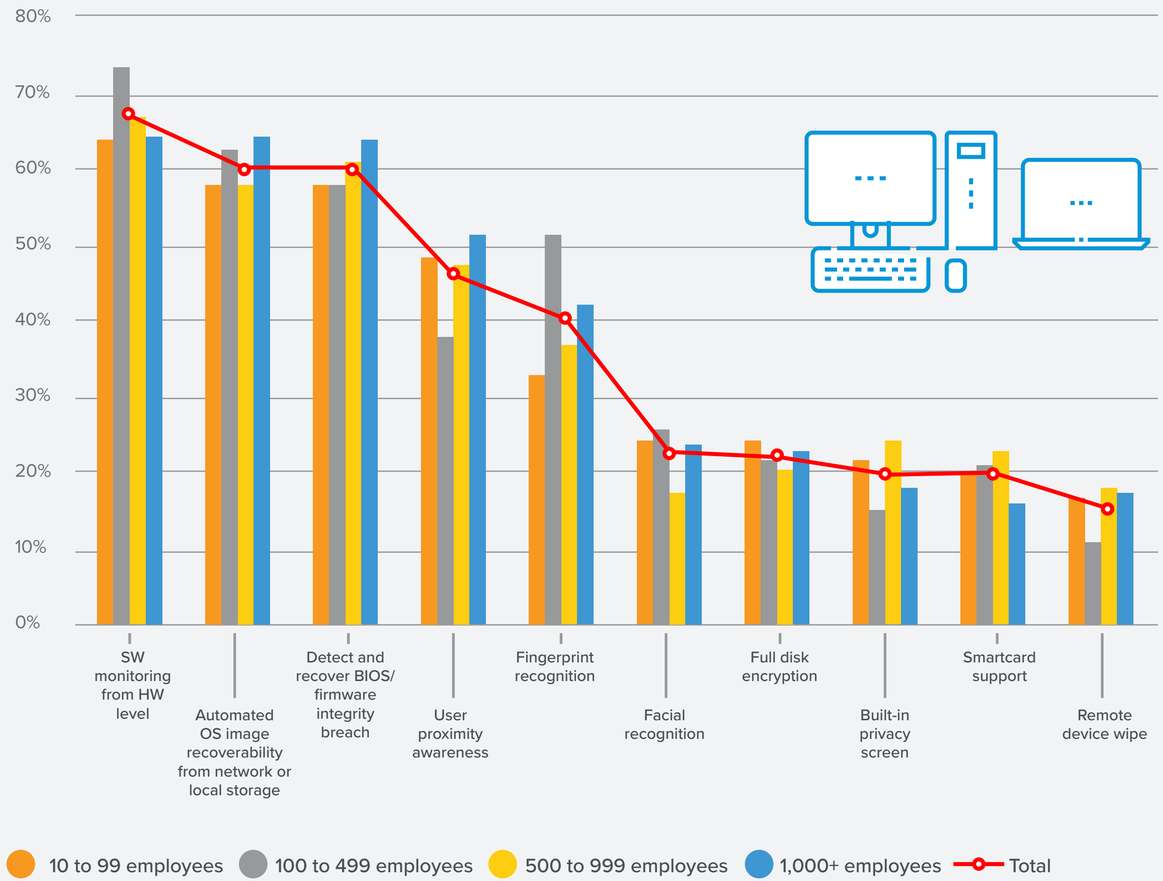
Does your organization have a policy of actively retiring devices that are shown to have unresolved intrinsic security vulnerabilities?



Many companies would like to reduce risk by actively removing older devices with known compromises, but in reality many have a policy that can't be enacted — which is no better than having no policy at all.

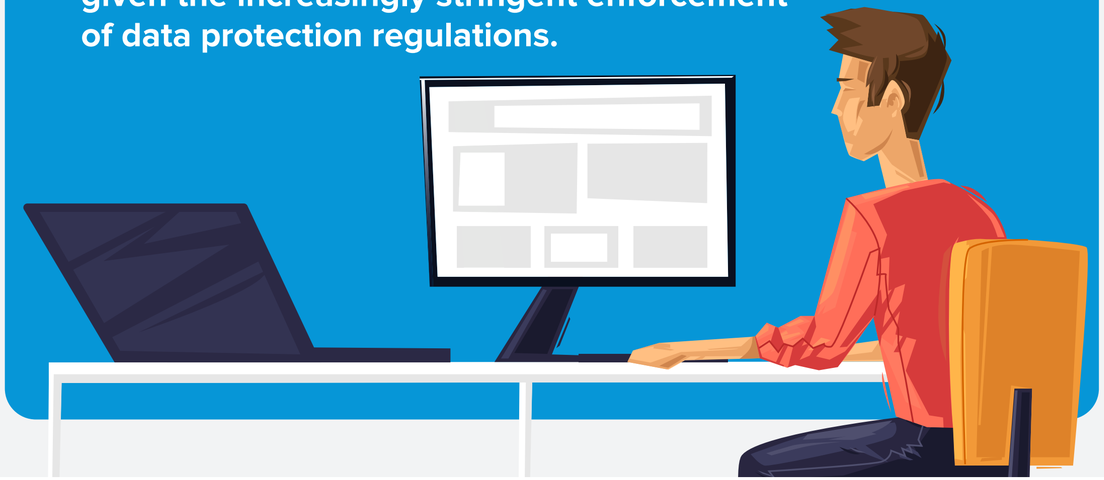
Source: IDC, IT Endpoint Security Survey 2019, North American respondents only, n=200

What's on the Security Wish List for PCs and Laptops?



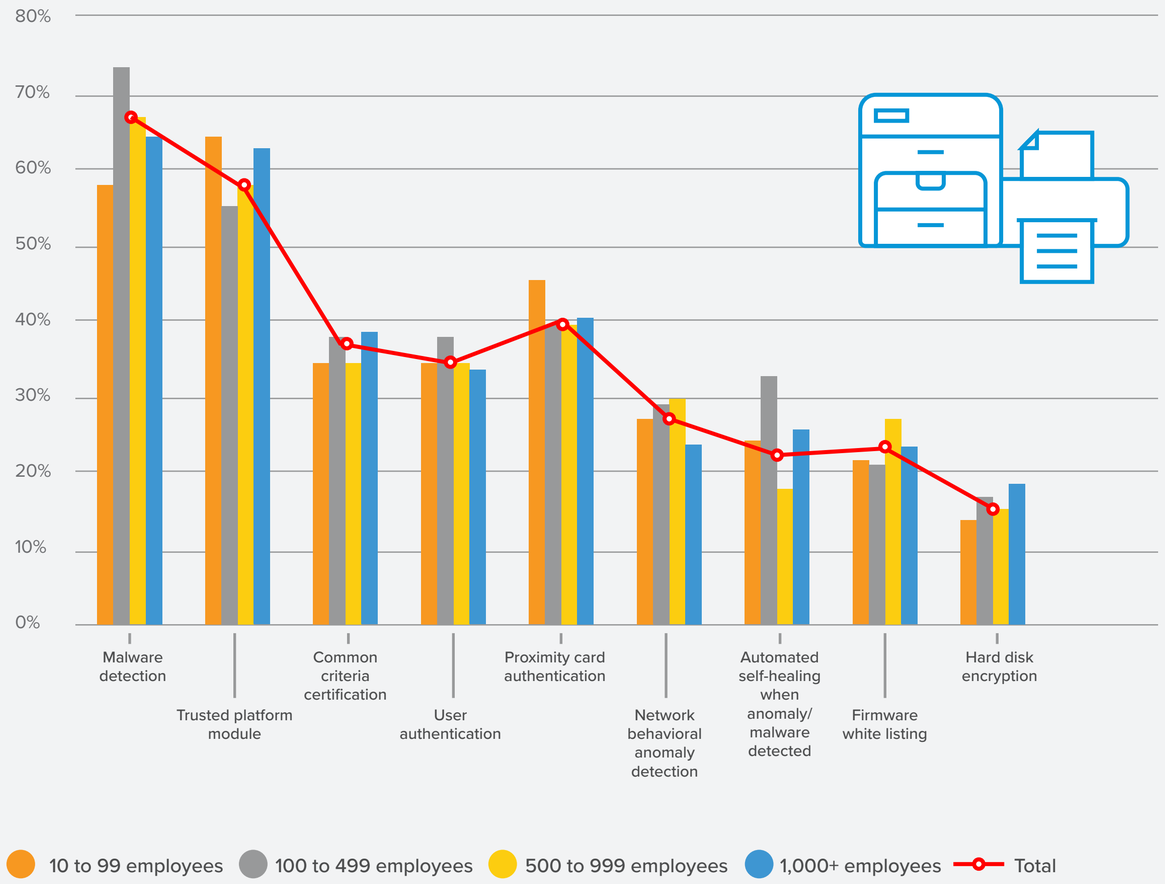
Despite the fact that many organizations are not including security requirements in their RFPs, they at least recognize the importance of security at the device level and are concerned about cyberthreats bypassing network security and protections at the PC OS/app software level to target the firmware.

Companies should seek to build resilience — on the assumption that breaches are inevitable — and look for "security by design" features that facilitate or automate detection and recovery. They should also look to accelerate the adoption of technologies such as full disk encryption, given the increasingly stringent enforcement of data protection regulations.



Source: IDC, IT Endpoint Security Survey 2019, n = 500

And What's on the Wish List for Printers?



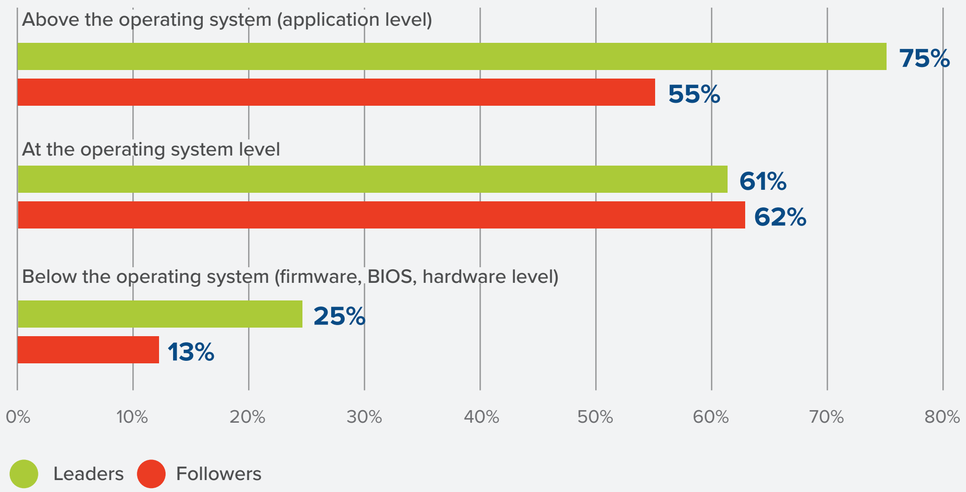
Ultimately a printer is another computer on the network, yet with its own proprietary OS and embedded applications.

For an attacker, printers can be both an entry point and a place to hide on the network for long-term malicious activity.

This, again, drives the need for built-in security by design with the same protection capabilities that are commonplace for PCs such as malware protection.

Threats Come in All Shapes and Sizes

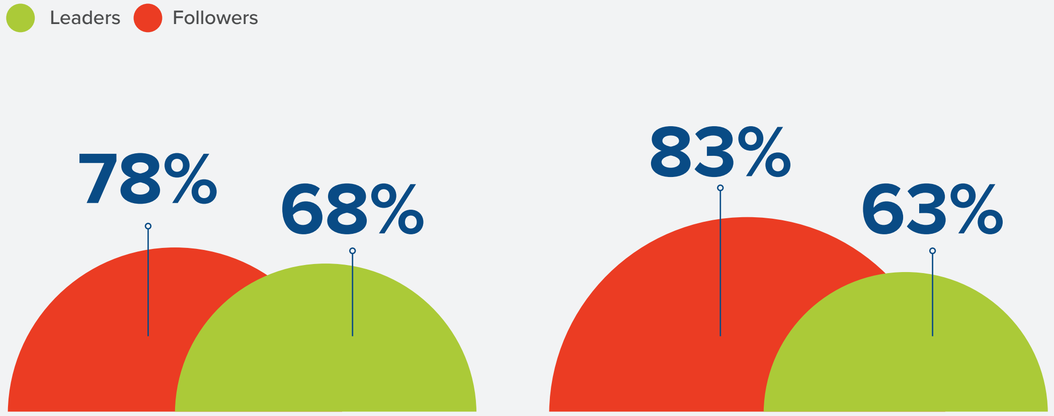
When considering endpoint PC device (desktops, laptops, notebooks) security, which of the following layers would be a priority for your organization?



Security Leaders recognize that threats to PCs come at all levels ...

... and are most likely to include printers as a cybersecurity consideration

Printers are considered within the scope of our cybersecurity team



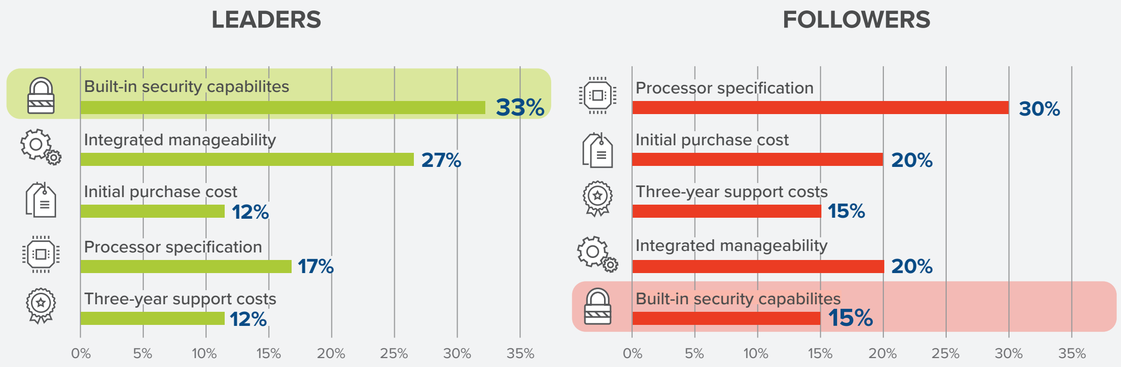
Printers are considered within the scope of our security team

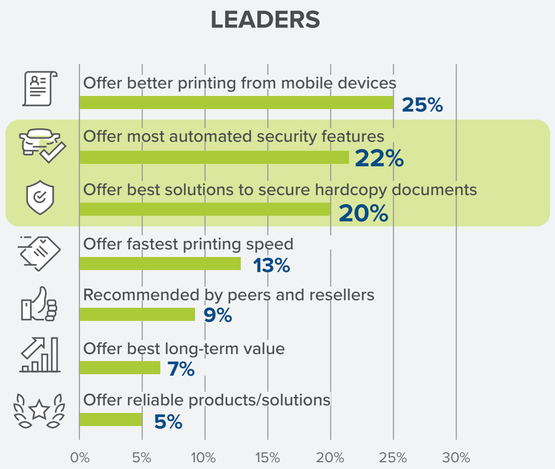
Security of printers is considered at the firmware/BIOS/hardware level

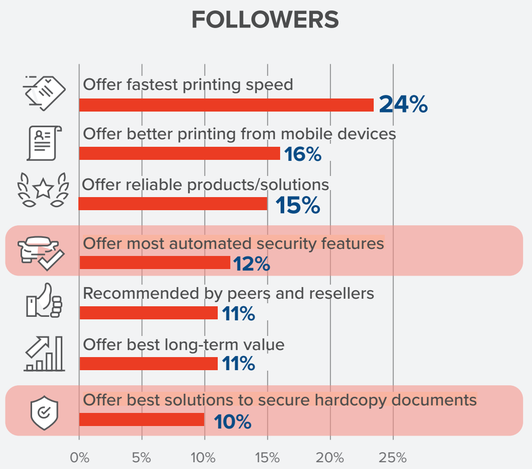
Security Leaders recognize the growing ability of malicious actors to target the physical devices themselves, rather than the OS or applications, and have started to take steps to prioritize protection hardware at the firmware level. This needs to be seen as necessary by all companies.

Not All Organizations Get Their Priorities Right

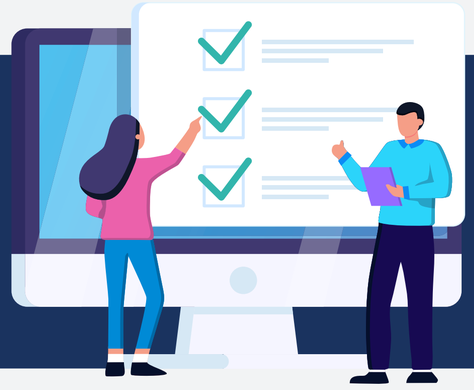
What are the top factors that guide your choice of PCs/laptops/notebooks?







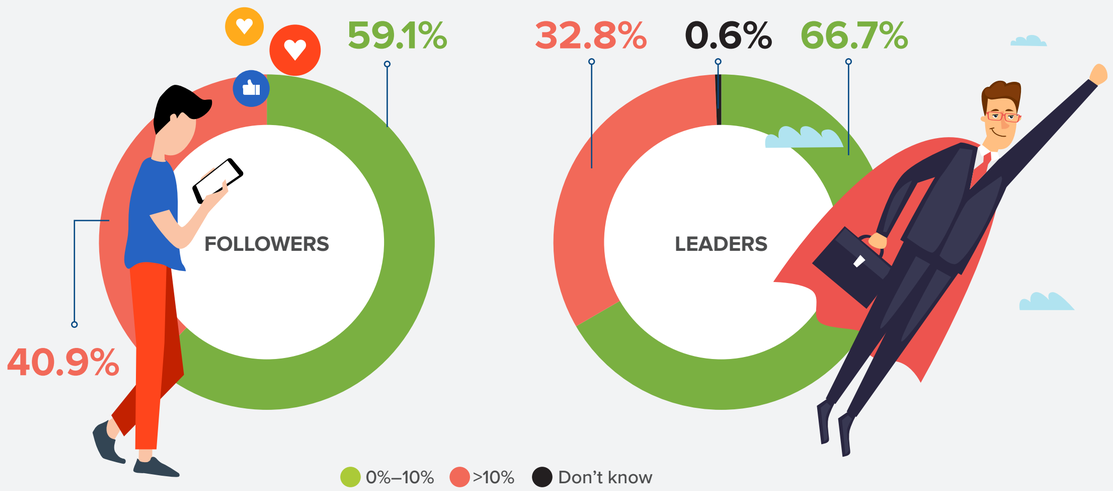
When choosing PCs, security Followers rank security as the lowest priority and focus on cost and performance. Any breach or loss of data will likely result in a significant penalty compared with those that have assessed the risk and invested in secure devices.



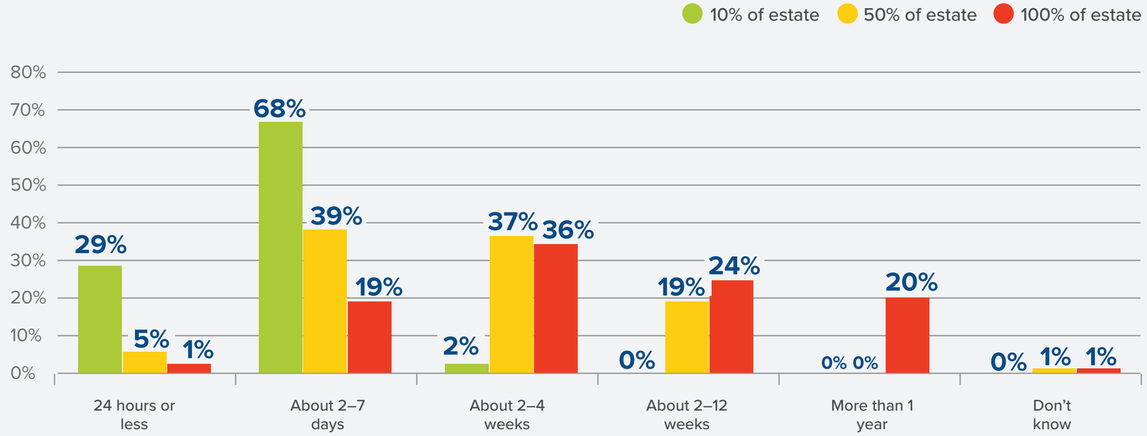
For printers, the difference between Leaders and Followers is quite stark: for Leaders, security represents two of the most important factors out of seven; for Followers, it ranks among the least important factors.

Investing in Security Procedures Protects Businesses from Current and Future Threats

What percentage of your organization's user accounts have been compromised in the past year?



In a recovery situation (e.g., following an incident such as a NotPetya style attack), roughly how long would it take to recover functional PC devices for your organization (OS, not user data) for:



Attackers only need to compromise one account to cause damage to the organization

If even 10% of systems are offline for a week, the cost to the business can be substantial

Leaders recognize that appropriate security investments can significantly improve the risk posture of the business

Take Your Endpoint Security to the Next Level

BE AWARE

- Threats to endpoints come at all levels (firmware, BIOS, OS, application layer)
- Firmware-level malware infections threaten all endpoints from PCs to printers — for printers this includes the OS and application layers

BE PRAGMATIC

- Security requirements should be included in all procurement specs, RFPs, and ITTs, and should be aligned with endpoint security strategy
- Intrinsically vulnerable devices should be retired according to strictly enforced policy

BE SECURE

- Start with good security hygiene across PCs and printers: put an admin password on the device including the firmware and close unneeded ports and protocols
- Assess any device security provided at the hardware level, which may aid mitigation or managing the cost of dealing with security incidents

BE STRATEGIC

- Incorporate endpoint security within overall cybersecurity strategy and ensure you remain up to date with threat trends
- Include all endpoints equally in the endpoint security plan, not just PCs

BE RESILIENT

- Post-attack recovery can take from days to months — have a tested DR plan in place
- Require capabilities such as image recovery and BIOS recovery support; the goal for all endpoints should be device-level resilience and recovery automation

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Global Headquarters
5 Speen Street Framingham, MA
01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com