How to thrive in the hybrid work world

Step up security for your flexible workforce

Choose from the latest Lenovo devices with the built-for-business Intel® platform and Microsoft Windows.

intel

Windows

Smarter technology for all
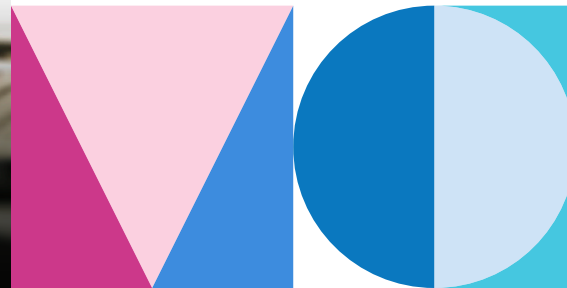
Lenovo

Securing a hybrid world

When the pandemic forced a shift to remote work for organizations of all kinds — from business to healthcare to education and more — employers, IT teams, and employees did an impressive job making it happen.

In Lenovo's "Future of Work and Digital Transformation" study, more than half the respondents said they feel more productive working from home.[1] And 94% of employers reported productivity has been the same or higher since employees began working from home at the start of the pandemic.[2]

Collaboration, too, not only held its own but forged ahead — with a huge spike in videoconferencing and new solutions to improve the quality of remote meeting experiences.

Of the three essential components of hybrid work — productivity, collaboration, and security — security has been the most challenging.

With 74% of organizations planning a permanent shift to more remote work post-pandemic,[3] the concern is growing and the need for swift and strategic response is growing with it.

intel.

Windows

Lenovo

IT's perfect storm

A number of factors are converging to challenge IT organizations. They are now responsible for securing nearly four times more remote devices than they were in 2019[4] and guiding the 49% of employees who are first-time remote workers.[5]

These remote devices are not limited to business knowledge workers. Healthcare clinicians and administrators, education faculty and staff, and government officials use them too.

The situation is compounded by nearly 80% of employees using their own smartphones for work-related tasks like voice and video calls, email, and work chat.[1]

To mitigate this, nearly 8 in 10 organizations say they will cover the cost of most devices and accessories for working from home. But less than half of surveyed employees have taken them up on it.[1] Better communication is needed.

Another threat to data security is reliance on home networks. Some organizations are providing always-connected PCs with integrated LTE or 5G to eliminate this risk. Remote employees who download unsafe apps also increase the potential for data breaches. A secure virtual platform where employees work together and save assets in a shared environment helps IT effectively manage security risks.

As the perimeter expands and endpoints multiply, the overarching challenge is finding the right balance.

IT needs to give users the simple, timely access they need while protecting the organization — people, devices, and data — and keeping it ready to weather the next disruption without a break in continuity.

intel.
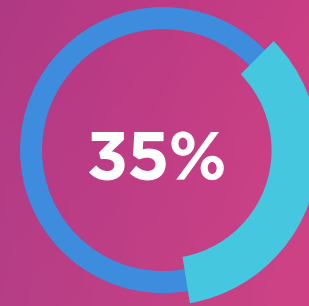
Windows

Lenovo

Proactive continuity

8 in 10 IT leaders have put data protection strategies
in place to keep their organizations running, no matter what.[1]

45% Cloud-based data backup

39% Physical data backup

35% Data security training

Anxiety

- Only 38% of global organizations believe they are prepared for a sophisticated cyberattack.[6]

- 38% of employees are not confident they know how to stay secure while working remotely.[7]

Risk

- On average, employees have access to more than 17 million company files.[4]

- Remote workers have caused data breaches in 20% of organizations.[8]

Cost

- The global average cost of a data breach is $4.24M,[9] with the public sector spiking 78.7% higher from 2020 to 2021 and healthcare up 29.5%.[9]

- When remote work was a factor in causing the breach, average cost increased $1.07M.[9]

intel

Windows

Lenovo

This way to a better night's sleep

Today's security technology delivers solutions

Pressing concerns reported by IT leaders

Heightened data security risk for first-time remote workers

Devices deployed worldwide

Remote workers need easy access to IT support

Technology solutions

AI-powered antivirus protection:
Detects, prevents, and can autonomously roll back from malware attacks

Remote manageability features maintain contact with employees and their devices

- Software with persistent endpoint visibility and management
- Central user portal to self-manage hardware settings and updates

intel.

Windows

Lenovo

Defend your data

Next-gen cloud-based, autonomous antivirus protection

Predict, prevent, and stop even zero-day attacks, alerting the network and rolling devices back to a clean, known good (pre-breach) state.

Data encryption

Encrypt from end to end so sensitive data can be safely shared whether it lives on a device hard drive or in the cloud.

Frictionless authentication

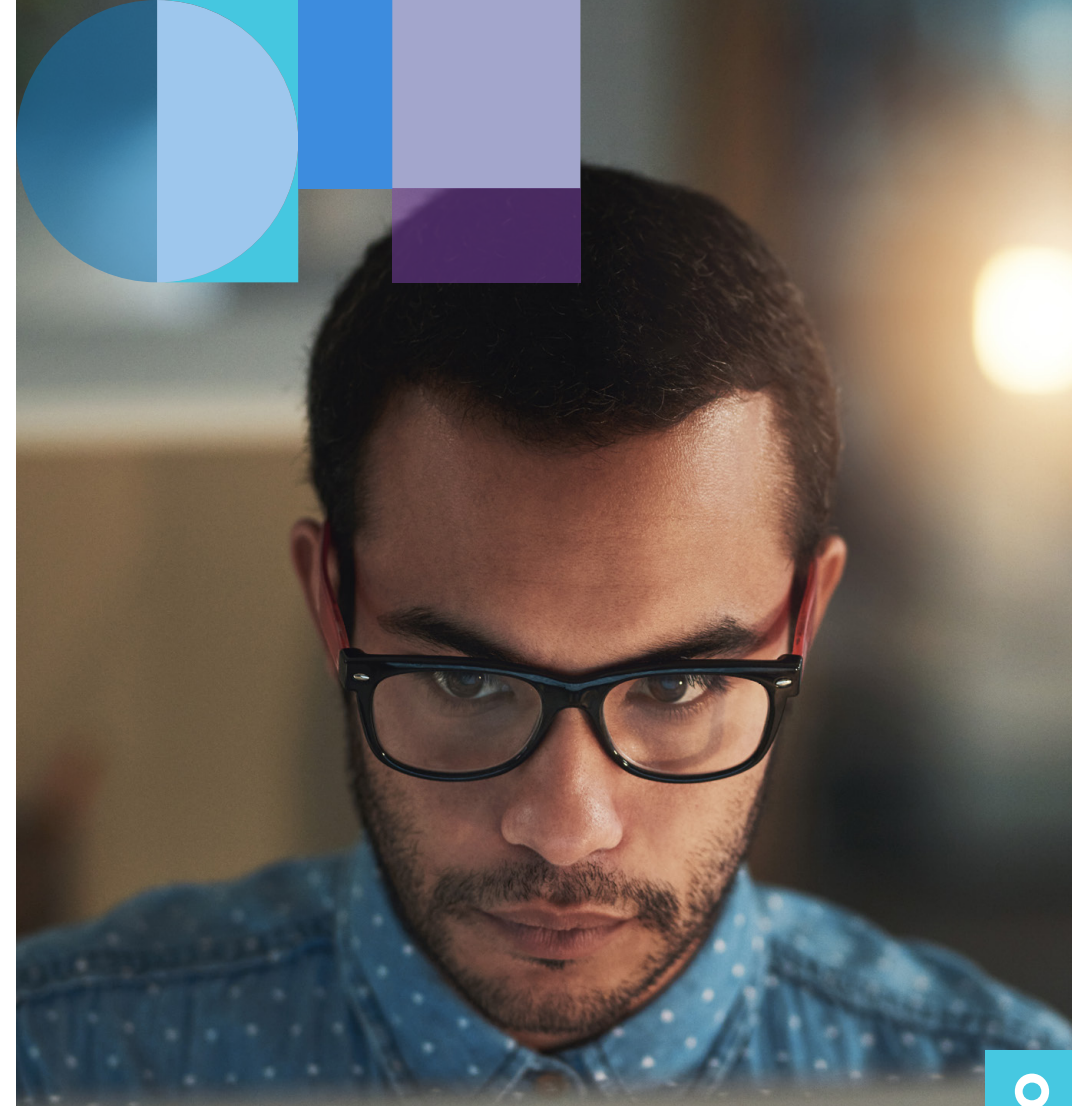Limit sensitive data access to authorized users with multiple authentication modes.

Secure disposal

Protect your data, even when your device reaches end of life — with options to keep your hard drive or securely wipe the data and dispose of the device in an environmentally sensitive manner.

intel.

■■ Windows

Lenovo

Snapshots of 4 high-stakes industries

	Healthcare	Financial	Education	Government
Top issues	Patient privacy/HIPAA compliance — Securing virtual visits — Security budget	Highly regulated industry — Credential and identity theft — Increased vulnerability from AI automation	Student safety — Standards compliance — IoT and CMS threats — Security budget	Complex infrastructure environment — Large number of compliance standards
Biggest threats	Phishing — Data breach — Ransomware	Data theft and manipulation — Phishing — Ransomware	Phishing — Data breach — Ransomware	Ransomware — Trojans — Data breach
Average cost of a breach	$9.23M[9]	$5.72M[9]	$3.79M[9]	$1.93M[9]
	Highest average breach cost of any industry[9]	238% surge in cybersecurity attacks from February to April 2020[10]	"Educational institutions must brace themselves for a continuing onslaught of cyberattacks." *Malwarebytes*	48% of states don't have a cybersecurity line item identified in their budgets[11]

intel.

■■ Windows

Lenovo

Looking for a supplier? Look for a partner.

As hybrid work takes hold and evolves, most organizations are still feeling their way. The best technology providers go beyond selling components to work with you as a trusted advisor and true partner. Seek out technology leaders who collaborate with other leaders to deliver end-to-end solutions — compatible hardware, integrated software, and services that make your life easier — with one point of contact.

Now is the time to invest in technology that powers the hybrid workplace and empowers the hybrid workforce — securely. Together with our partners Microsoft, Intel, Absolute, and SentinelOne, Lenovo delivers solutions to keep your organization protected no matter where work is.

intel.

Windows

Lenovo

Partner with Lenovo on solutions for the hybrid future of work.

When you're ready, we're here to help.

Contact your Lenovo Account Representative or local Business Partner

Visit **www.lenovo.com/FlexibleWorkforce**

Sources

1   Lenovo, "The Future of Work and Digital Transformation," February 2021

2   Mercer, "U.S. Employers Flexing for the Future," August 2020

3   Gartner, "COVID-19 Bulletin: Executive Pulse, 3," April 2020

4   McKinsey Global Institute, "What's next for remote work: An analysis of 2,000 tasks, 800 jobs, and nine countries," November 2020

5   Security Magazine, "Increasing Cybersecurity Gaps and Vulnerabilities due to Remote Work During COVID-19," June 2020

6   IBM, "2019 Cost of a Data Breach," 2019

7   Media Pro, "2020 State of Privacy and Security Awareness," 2020

8   Malwarebytes, "Enduring from home: COVID-19's impact on business security," August 2020

9   IBM, "2021 Cost of a Data Breach," 2021

10 VMware, Modern Bank Heists 3.0," May 2020

11 Statista, "US states with cyber security budget," 2018

intel.

Windows

Smarter technology for all

Lenovo