Lenovo
Government

Protecting information everywhere

A **smarter** approach to stopping evolving threats

ThinkShield

Windows 10

Smarter technology for all

Lenovo

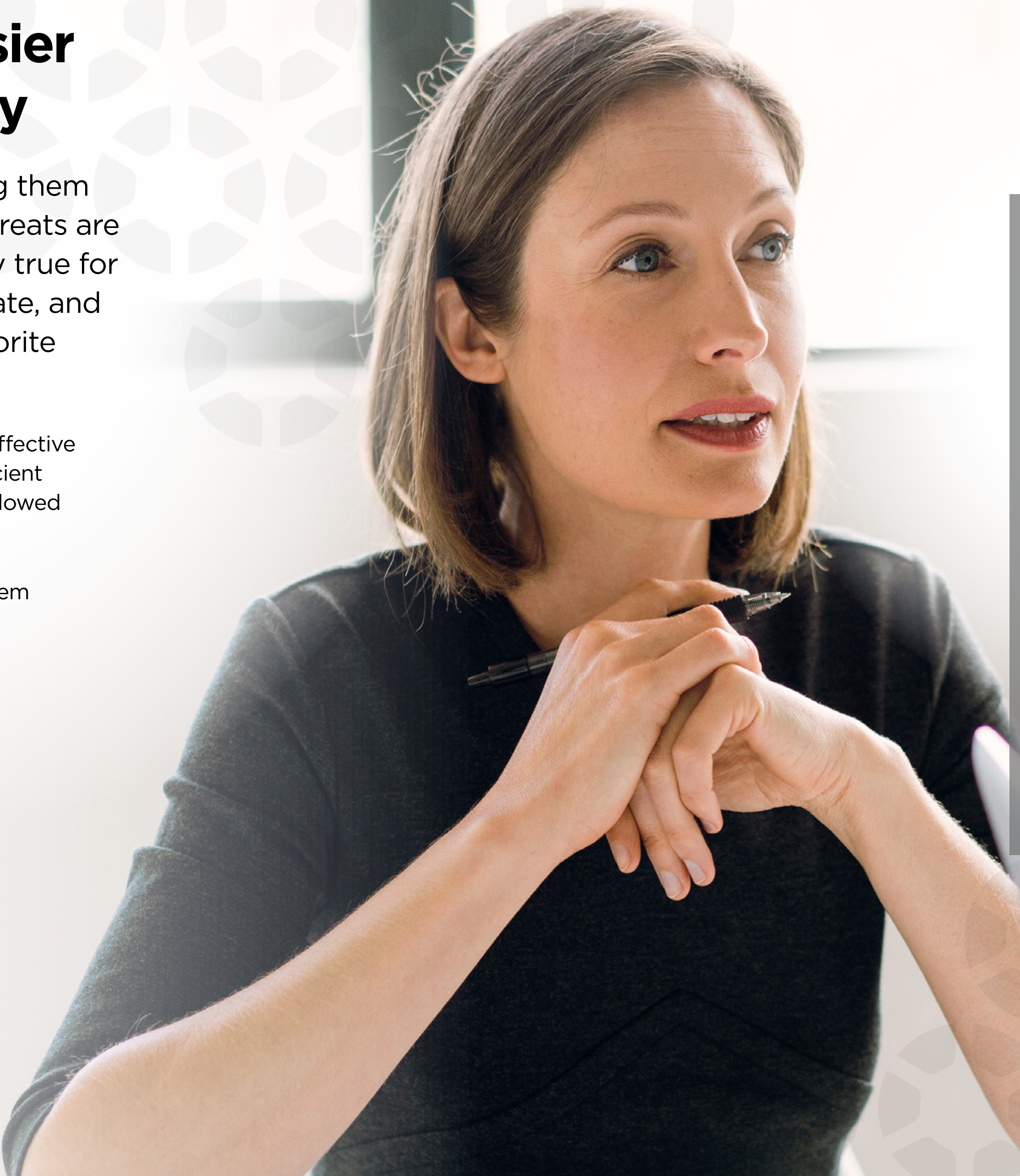
It’s not getting any easier out there for IT security

Ask any C-suite executive what’s keeping them up at night, and you can be sure cyberthreats are near the top of the list. That’s particularly true for government organizations, as federal, state, and local governments are consistently a favorite target for hackers.

When asked about the challenges to establishing an effective cybersecurity program, state CISOs cited lack of sufficient cybersecurity budget as the most common barrier, followed closely by inadequate cybersecurity staffing.[1]

In fact, 48% of states don’t have a cybersecurity line item identified in their budgets.[2]

Attacks on local governments have risen 58.5% in a single year.[3]



THE RISING COST OF DATA BREACHES

With an increasing number and intensity of attacks on state and local governments, the costs continue add up. As an example, the estimated reported ransom paid by municipalities per ransomware event from 2017 to 2020 was $125,697.[3]

MAAS (MALWARE AS A SERVICE)

There are more threats to IT today due to the proliferation of sophisticated hacking tools. Bad actors no longer need to write complex code to mount an attack — the resources are a click away. Websites now offer malware as a service.[4]

An increasingly complex landscape

The modern workplace is evolving in ways that can compound the challenge of defending against evolving and increasing threats.

Increasing mobility expands the attack surface

One of the most visible trends impacting security is the dramatic increase in remote work. A recent survey showed 61% of municipalities are allowing their employees to work from home.[5]

With more endpoints and more data in motion across more networks, the threat surface quickly expands. As the National Institute of Standards and Technology (NIST) noted in its recent publication, any information that's collected, stored, processed, or transmitted on mobile devices is especially vulnerable to attack.[6]

The increasingly mobile nature of government operations and business in general poses significant challenges for IT teams, many of which are themselves working remotely.

Regulations and compliance

Any technology solution must be evaluated with one additional criterion before it can be considered valuable for use: Does this solution help the organization comply with the highest regulatory standards?

Technologies that meet security standards in other industries may not comply with local, state, or federal government guidelines and regulations.

Security vs. expediency

For any IT security measure to be effective, it must be easy for users to understand and comply with. When users are faced with solutions that hinder access to critical data or disrupt established workflows, "workarounds" quickly develop, and that can lead to new vulnerabilities.

Security needs a people-first approach

IT security must be seamless and ubiquitous, but it has to work the way employees work. It must support and empower workers while protecting the organization and its data.

Security by Design

A smarter approach to government IT security

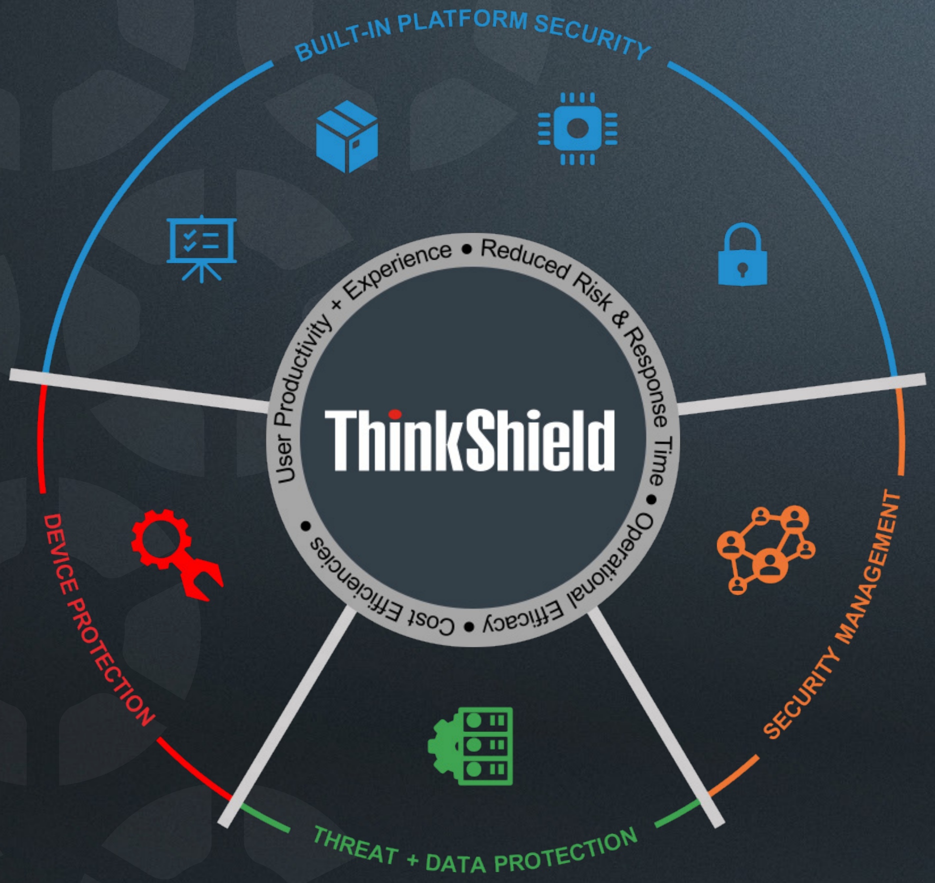
ThinkShield is a customizable solution that secures critical data and business technologies with comprehensive end-to-end protection. It's not a standalone product — it's a unique combination of hardware, software, services, and processes that protect IT across four key dimensions.

Security by Design starts with developing standard security requirements for each device to address a current and evolving threat landscape.

This approach continues into securing our supply chain with robust practices and policies.

Our Trusted Supplier Program, a rigorous vetting process, ensures every supplier meets the highest standards for end-to-end supply chain security. Requirements for suppliers include quarterly compliance assessments, onsite asset protection reviews, and the implementation of need-to-know control of information security and logistics processes.

For the state and local government IT environment, ThinkShield helps provide privacy and security.


BUILT-IN PLATFORM SECURITY
SECURITY MANAGEMENT
THREAT + DATA PROTECTION
DEVICE PROTECTION
ThinkShield
User Productivity + Experience • Reduced Risk & Response Time • Operational Efficacy • Cost Efficiencies •

BUILT-IN PLATFORM SECURITY
Our holistic approach to security starts with the built-in ThinkShield security solutions that come standard on industry-leading Think® devices

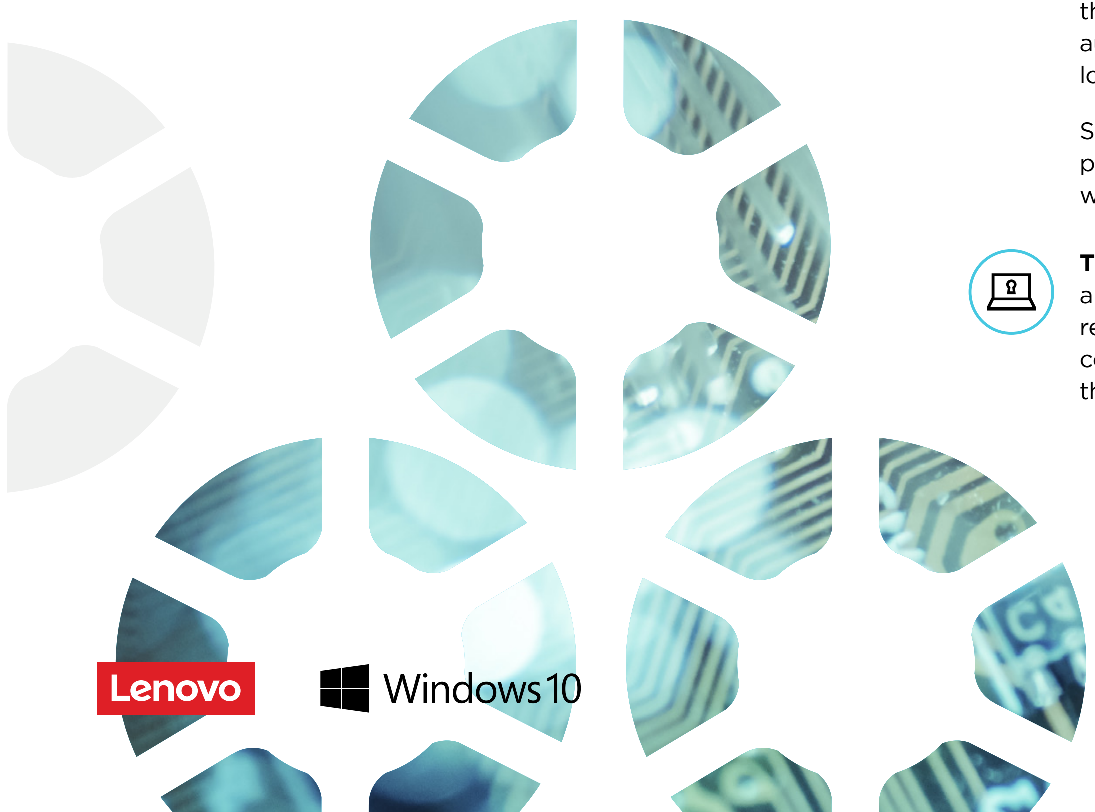
DEVICE PROTECTION
Security hardware features and service offerings that add another layer of device protection

THREAT AND DATA PROTECTION
Security solutions that seamlessly integrate with Lenovo devices, ensuring your critical data and business technologies are protected

SECURITY MANAGEMENT
Solutions that provide capabilities to deploy, monitor, and report IT assets

Privacy — Keep data and user activity secure

Today's government is constantly in motion, and security measures need to keep up. It's not always easy to know who can see a device's screen throughout the day. That's why we offer PrivacyGuard and Shoulder Surfing Protection.



PrivacyGuard provides an integrated e-privacy filter that prevents others from looking over your shoulder to get valuable information — without the need for third-party aftermarket privacy filters (which frequently get lost or thrown away and need to be replaced). Having a preinstalled e-privacy filter is more secure and is one less thing the IT team and users have to deal with.

Shoulder Surfing Protection incorporates gaze detection technology, which notifies the user if someone else is looking at the screen and even detects which side of the screen they're watching from. Gaze detection can also automatically blur the screen when the user looks away.

Shoulder Surfing Protection includes built-in presence detection that locks the device for walk-away security.

ThinkShield Built-In Platform Security includes a webcam privacy shutter that covers both the regular and IR cameras. This physical camera cover gives patients and users peace of mind that the camera isn't on or being hacked.

The ThinkShield approach to privacy extends through the end of a device's service lifecycle with multiple options for secure disposal to protect user privacy.

The secure wipe feature in the BIOS reliably deletes all data from a drive without the need for external tools.

The Keep Your Drive service allows customers to keep the hard drive of a device if it should fail, eliminating the need for tracking drives in transit.

THE THINKPAD® T14i SECURE ACCESS
You'll find all these ThinkShield features on the ThinkPad T14i Secure Access, a workhorse laptop that brings all the performance that's made the ThinkPad® family a global best seller with features and options designed specifically to address the needs of secure working environments.
LenovoForGovernment.com

Security —
Authentication and data

Limiting access to sensitive data to only authorized users is a cornerstone of any security practice. ThinkShield provides multiple ways to verify a user's identity, including frictionless multifactor authentication.

NETWORK SECURITY
Based on the device's IP address

GPS SECURITY
Based on geo-location

FACIAL RECOGNITION
IR cameras that support Windows Hello

BLUETOOTH
For phone proximity authentication

PASSWORDS AND PINS
Intel Authenticate Secure PIN, Windows 10 typed and visual PINs

MATCH-ON-CHIP FINGERPRINT READER
Includes Quantum Matcher anti-spoofing algorithms

FIPS 201 COMPLIANCE
Meets requirements for personal identity verification (PIV) of government employees and contractors

NFC
Secure NFC tap-to-logon compatible with all major single sign-on providers, including Imprivata®

Having all these features built in means devices protected by ThinkShield fit seamlessly into existing security protocols with no additional hardware required.

Lenovo Windows 10

Security — Real-time endpoint protection

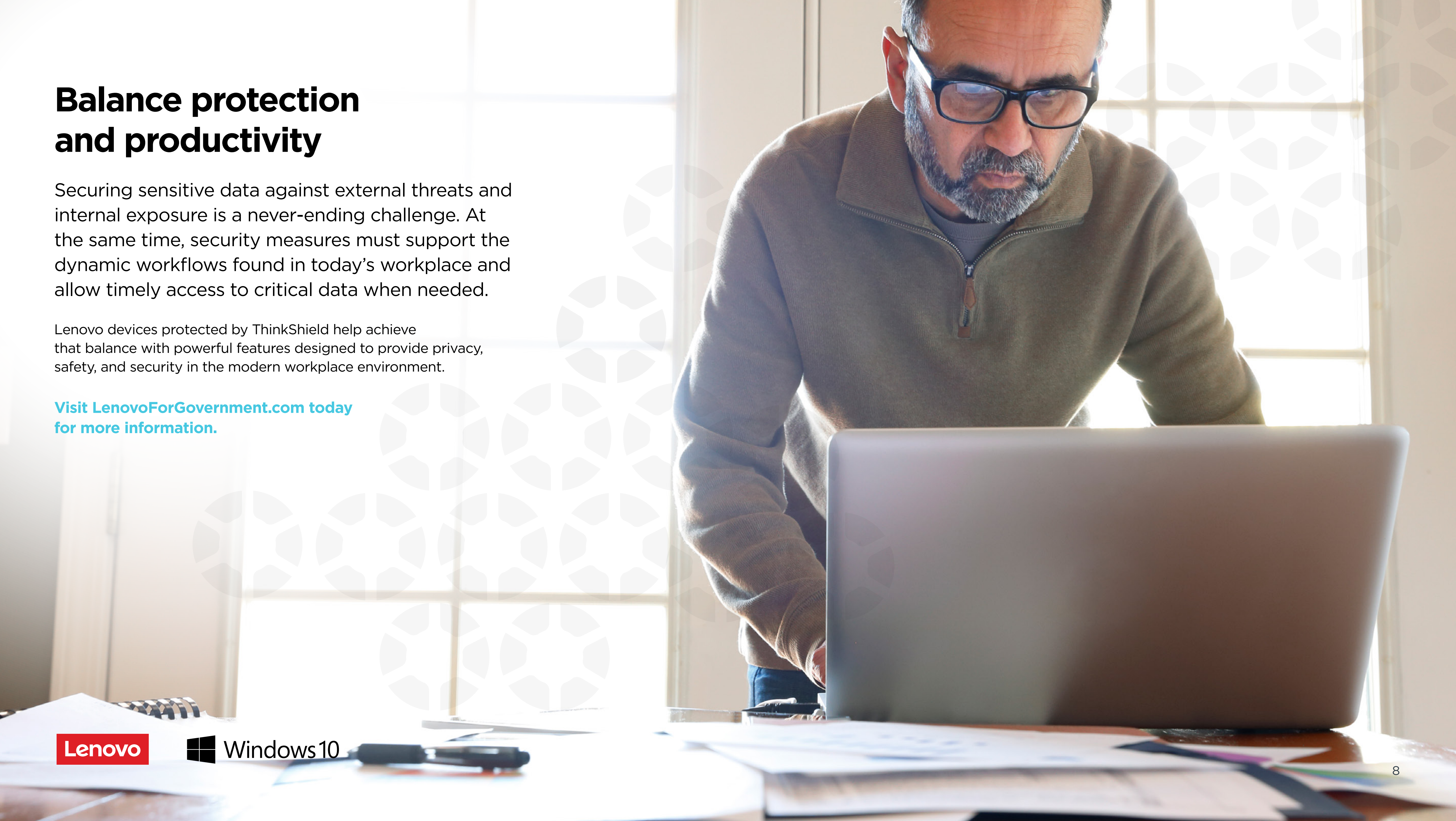
ThinkShield includes features designed specifically for real-time endpoint protection.

SentinelOne — Autonomous endpoint protection
SentinelOne delivers next-generation antivirus protection powered by patented behavioral AI. This advanced, autonomous threat detection completely replaces an antivirus solution and expands to include active EDR (endpoint detection and response) for known and unknown malware strains, enabling devices to self-heal from broad modes of attack instantaneously.

WinMagic — Drive encryption
A highly configurable, full-scale encryption for the enterprise environment that protects sensitive information stored on devices. Centrally manage encryption on devices across all platforms using a choice of SecureDoc FDE, FileVault2, BitLocker, dm-crypt, and Self Encrypting Drive. Easily track encryption and manage keys for SecureDoc devices and third-party applications, platforms, and entities through a single console.

Absolute® — Endpoint visibility and control
Embedded directly into Lenovo device firmware, Absolute is an endpoint visibility and control solution that provides persistent security management. It automates endpoint hygiene to support self-healing capabilities. Its real-time remediation control allows remote investigation of potential threats and prompts action if a security incident occurs.

Secured-core PC — Guard against attacks below the OS
Secured-core PCs guard against attacks aimed below the operating system, keeping malicious code out of the BIOS. Deep security integration between hardware, firmware, and the Windows 10 Pro OS builds a bedrock of security at the heart of the device. Secured-core PCs boot up against a security checklist known as the “root of trust.” If processes and movements deviate from the norm, boot-up is aborted.



Balance protection and productivity

Securing sensitive data against external threats and internal exposure is a never-ending challenge. At the same time, security measures must support the dynamic workflows found in today's workplace and allow timely access to critical data when needed.

Lenovo devices protected by ThinkShield help achieve that balance with powerful features designed to provide privacy, safety, and security in the modern workplace environment.

Visit LenovoForGovernment.com today for more information.

Get smarter with ThinkShield

Connect with Lenovo. We’re experts at breaking down barriers and building smart solutions. When you’re ready, we’re here to help.

- Contact your Lenovo Account Representative or local Business Partner
- Visit LenovoForGovernment.com

SOURCES

[1] https://www.statista.com/statistics/1074350/leading-barriers-to-a-state-cyber-program-usa/

[2] https://www.statista.com/statistics/1074258/us-states-with-cyber-security-budget/

[3] https://www.darkreading.com/attacks-breaches/as-cyberattacks-soar-us-state-and-local-government-entities-struggle-to-keep-up/d/d-id/1338304

[4] https://www.itprotoday.com/cloud-security/malware-taking-new-shape-malware-service

[5] https://www.americancityandcounty.com/2020/04/24/the-pandemic-and-the-future-of-remote-work-for-local-government/

[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-1.pdf

Lenovo