Lenovo
ThinkShield

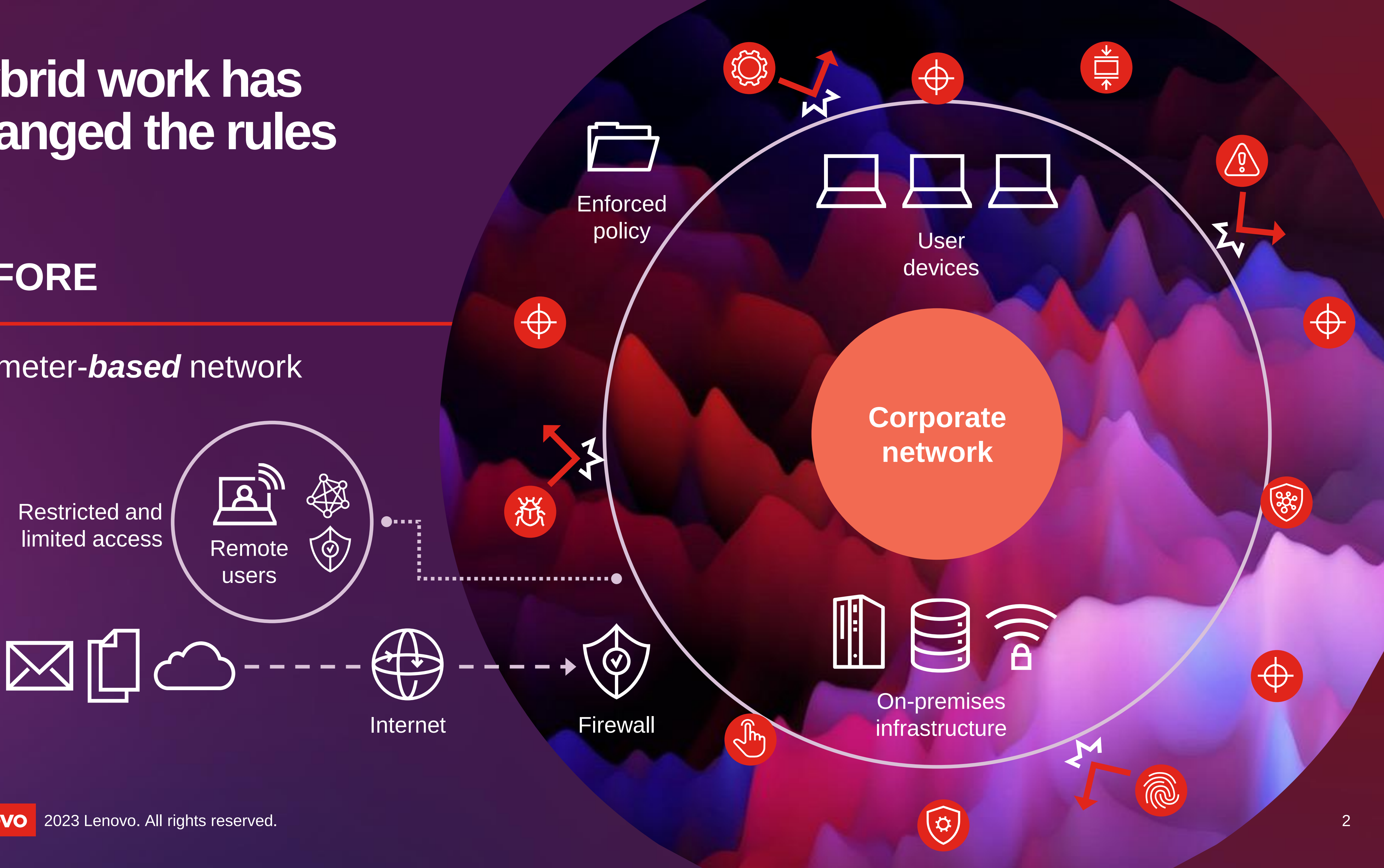
Security for the modern workforce

Speaker Name | Date

Hybrid work has changed the rules

BEFORE

Perimeter-***based*** network



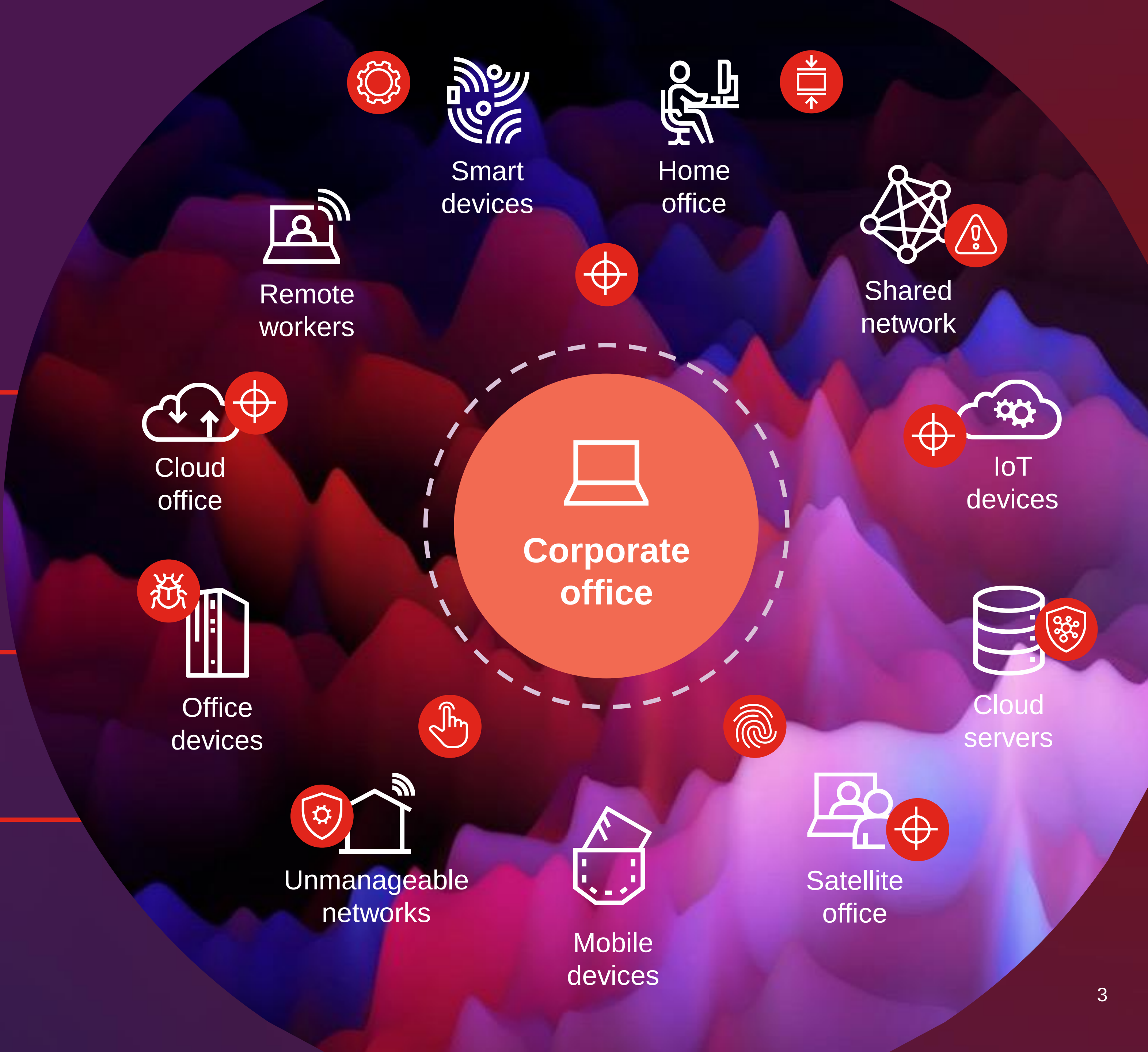
2023 Lenovo. All rights reserved.

Hybrid work has changed the rules

AFTER

Perimeter-*less* network

Every endpoint is now an attack surface



Security threats are a “when,” not an “if”

266 days

on average to detect/ contain a breach

$4.24M

Global average per data breach ($9.05M in US)

83%

of companies experienced a BIOS or firmware attack below the OS

Potential consequences can include reputational damage, lost revenue, civil liability/fines, and remediation costs

Sources

[1] IBM, “Cost of a data breach 2022”

[2] Microsoft, “Security Signals,” March 2021

Lenovo’s heritage of security innovations

1992–2004

- Pioneered embedded security chips
- First notebook with fingerprint reader

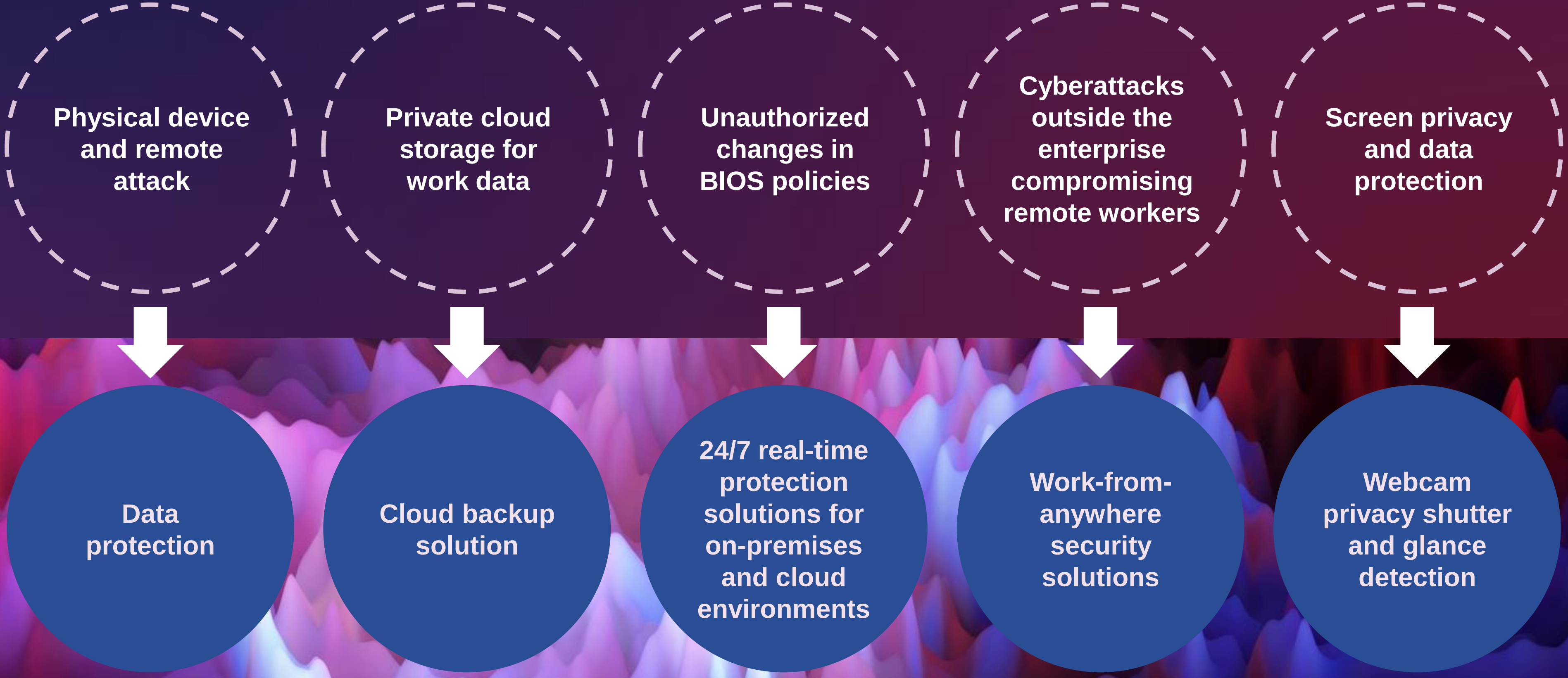
2009–2017

- Secure hard drives and dTMP encryption
- Anti-shoulder surfing protection

2018–present

- ThinkShutter
- Secured-core PCs
- Self-healing BIOS
- Exclusive OEM supply chain security

Everyday challenges



Cybersecurity challenge	Physical device and remote attack	Private cloud storage for work data	Unauthorized changes in BIOS policies	Cyberattacks outside the enterprise compromising remote workers	Screen privacy and data protection
Lenovo ThinkShield solution	Data protection	Cloud backup solution	24/7 real-time protection solutions for on-premises and cloud environments	Work-from-anywhere security solutions	Webcam privacy shutter and glance detection

Lenovo ThinkShield delivers complete protection wherever and whenever work happens

Technology you can rely on

Zero Trust supply chain

Worry-free
chip-level inspection

Straightforward
access protection

Security that adapts

Seamless integration

Work-anywhere data protection

Automated proactive prevention

Expertise you need

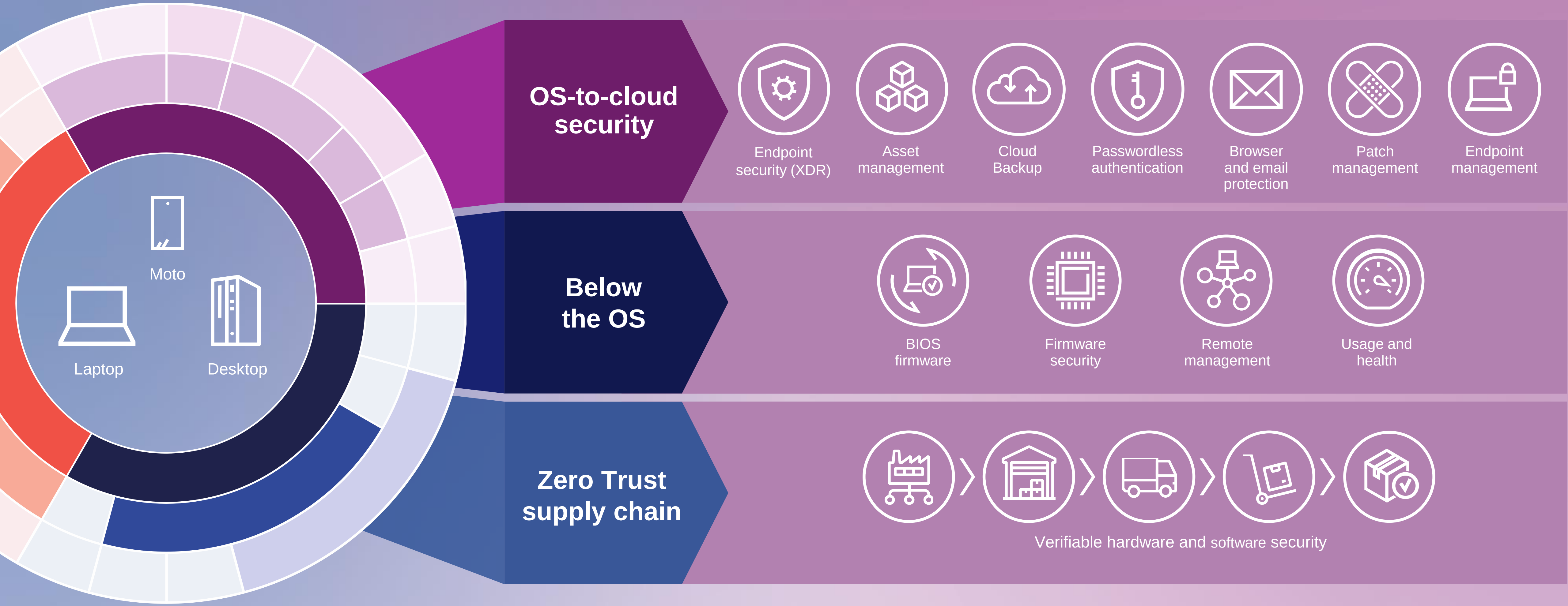
Smarter security services

Boundless data protection

Lenovo Professional Services

Integrated layers of protection

Lenovo ThinkShield has you covered at every level



OS-to-cloud security

Endpoint security (XDR)
Asset management
Cloud Backup
Passwordless authentication
Browser and email protection
Patch management
Endpoint management

Below the OS

BIOS firmware
Firmware security
Remote management
Usage and health

Zero Trust supply chain

Verifiable hardware and software security

Zero Trust supply chain

Exclusive OEM device hardware attestation ensuring every device is secure from the start

- **Trusted Platform Module** certifies keys for protecting data
- **Traceability** of the platform owner and users
- **Auto-verify tool** checks for changes in hardware compared to original manufacturer design
- **Customer web portal** provides easy access to files and certifications

Below the OS

Embedded endpoint security against today's threats

Privacy protection
Webcam shutter, privacy guard, and shoulder surfing protection

Secure firmware
FirmwareShield, self-healing BIOS, and HTTPS Boot to protect, detect, and recover platform firmware to a state of integrity

Secure packaging
All shipments are secured in tamper-evident packaging

Secure disposal
Secure Wipe and Secured-core PC to protect and delete data from drives without external tools

OS-to-cloud security

Implementing best-in-class security innovations that address threats between the operating system and the cloud

ThinkShield Threat Isolation
Online sandboxing of browser behavior provides an additional layer of protection

ThinkShield Endpoint Management
Automatic risk assessment and patch remediation

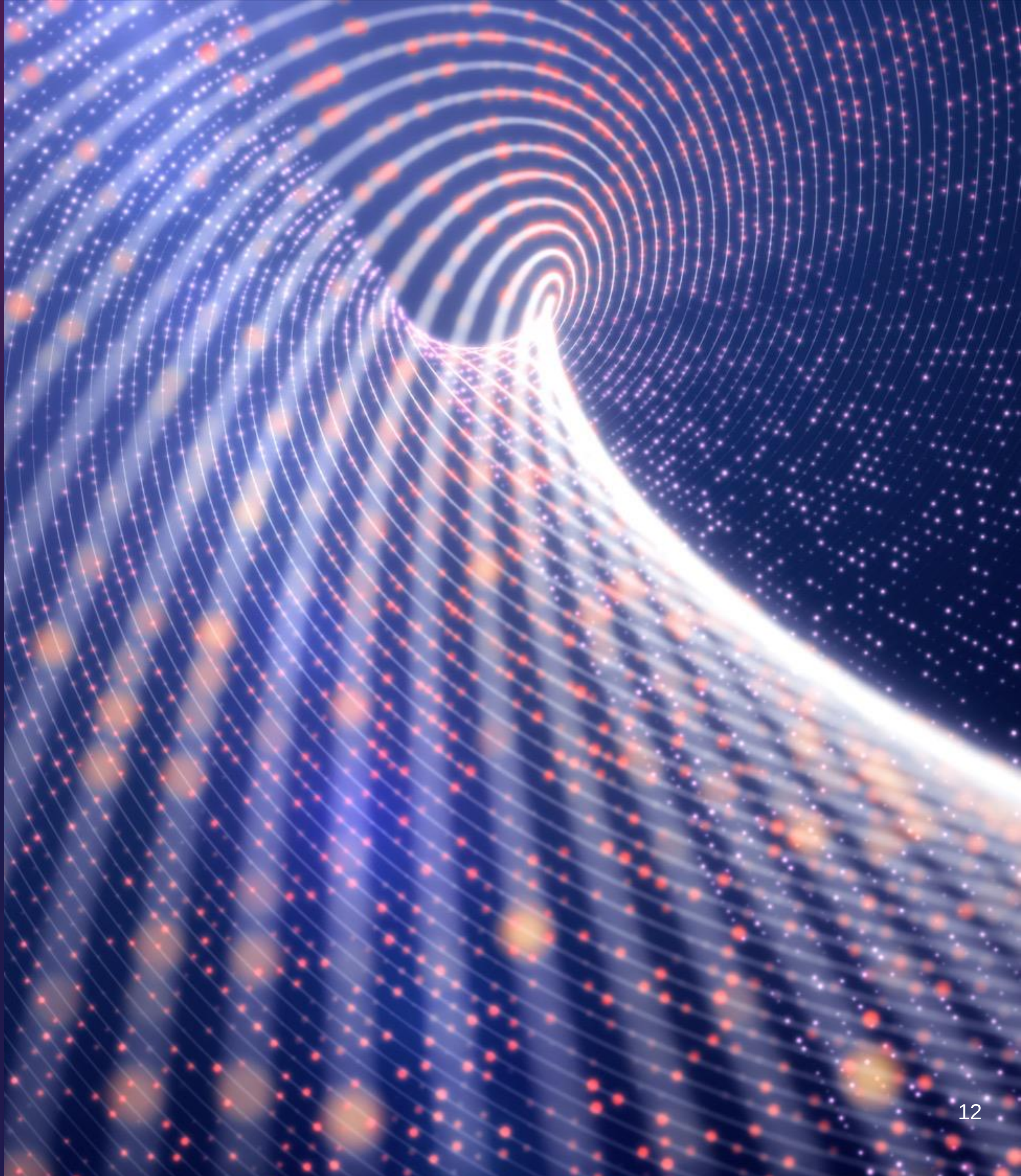
ThinkShield XDR
Analytic machine learning to identify, alter, and resolve emerging threats

ThinkShield Passwordless MFA
Universal multifactor passwordless authentication

OS-to-cloud security

The Lenovo ThinkShield OS-to-cloud solution offers endpoint security management including:

- AI-powered EPP (patented 24/7 solution to protect devices in real time for on-premise and cloud environments)
- Work-from-anywhere protection
- Data defense
- Lenovo Patch (update and patch BIOS, drivers, and third-party apps)
- Patented solution to protect browser, email, and file explorer
- Remote management of BIOS passwords
- Cloud backup
- Asset management



Security for the modern workforce

Why Lenovo ThinkShield?

- Get resilient enterprise-class solutions from a trusted engineering leader
- Deliver peace of mind to your customers, teams, and leadership
- Deliver frictionless experiences to your hybrid workforce
- Free up your time for what matters most

Commercial notebooks

Motorola phones

Desktops and all-in-ones

Mobile workstations

Lenovo ThinkShield

Find out what’s possible.

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

Commercial notebooks

Motorola phones

Desktops and all-in-ones

Mobile workstations

Smarter
technology
for all

Lenovo

thanks.

Lenovo ThinkShield for Motorola devices

Protection against emerging threats today and for years to come

Protect what matters

- Protection from the factory to the phone
- Hardware and software defense against malware, phishing, and more

Moto KeySafe

- Tamperproof hardware security
- Isolates PINs, passwords, and cryptographic keys

FIPS 140-2 | Android Enterprise Recommended

4 Years of software support

- Keep security systems updated
- Protect against targeted attacks, ransomware, and evolving threats

motorola

Top cyberattack vectors (paths/methods)

Attack vector	What is it?	Customer impact	Suggested defense
Ransomware/malware	• Computer program that invades, damages, disables, restricts, locks computer systems and data	• Severe operational downtime • Loss of business and personal data • Ransom payment to unlock systems and data • Loss of reputation	• Endpoint detection and response (EDR) solution • Data encryption solution
Phishing/spear phishing/ malicious websites	• Email communication that looks like a genuine organization/internal email • Fake website that installs malware/ steals passwords	• Severe operational downtime • Loss of business and personal data • Ransom payment to unlock systems and data	• Virtual containment for browsers and email clients
Credentials/password leaks	• User IDs and passwords leaked online due to malware/phishing/malicious website attacks • Leaked credentials due to unrelated data breaches	• Stolen credentials used to infiltrate business IT environments for stealing intellectual property and confidential data	• Passwordless multifactor authentication
Outdated operating system/application(s)	• Hackers and malware using vulnerabilities in outdated/unpatched operating systems and applications	• Customers vulnerable to ransomware attacks, data thefts, severe loss of productivity	• Unified endpoint management system • Patch management system • Endpoint detection and response (EDR) solution