Trust your security. Trust your people. With Lenovo.

How to keep your workforce safe in an evolving cyber security environment

Smarter technology for all

Lenovo

The irrevocable move towards hybrid working has created a challenging cyber security environment.

Today, most workers need to be equipped for hybrid working. As a result, threat protection needs to be extended across multiple clouds and different platforms.

This creates a complex digital environment that can be a hidden harbour of unknown threats. Enforcing security policies across devices and different digital layers is a seriously daunting task. It's the stuff of sleepless nights for those charged with delivering protection.

Secure hardware and Cloud equation – a unique partnership: Lenovo has a unique partnership with Microsoft, in which hardware powered by ThinkShield is combined with Microsoft Cloud Security services.

Security by Design with Lenovo ThinkShield

At Lenovo we understand the urgent need for sweeping protection. Reflecting best practice protection, we're driving our ThinkShield security approach to increase the security of our device portfolio by design.

This goes all the way from securing supply chains through to developing new Lenovo products that are secure and engineered by the makers of the world's most trusted business PCs.

Our unique ThinkShield portfolio of hardware, services, software and processes deliver protection and reaches all levels of the enterprise. Our partnerships with industry-leading security providers enable sweeping defenses that encapsulate, contain and drive a Zero Trust strategy, powered by Microsoft security solutions.

Zero Trust. The future of cyber protection. The shape of a new direction.

Zero Trust is a major departure from traditional network security in which there is a ‘corporate perimeter’, or devices connected via a VPN, which is very much the norm today.

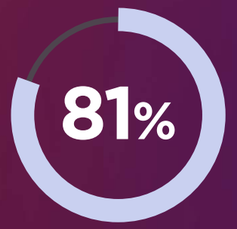
The guiding principles of Zero Trust are, ‘Never trust. Always verify.’

In today’s world of hybrid working, devices should not be trusted by default, even if they are connected to a ‘permissioned’ network.

Zero Trust assumes an attacker is inside the network. Trust is established based on **context** such as the **user identity and location, the security status of the device** and the **app or service being requested**. There are policy checks at each step.

This ensures that only **the right people with the right resources on secure devices can access your data.**

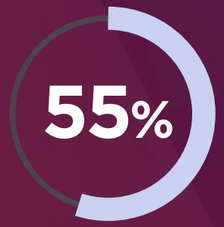
The need for Zero Trust has never been more urgent:



of enterprises have begun the move to hybrid working[1]

reduction in the risk of a data breach[3]

1,070%
increase in ransomware between July 2020 and June 2021[4]



of organisations report detecting a phishing attack in the last 18 months[2]

decrease in calls placed to IT and help desk analysts[3]

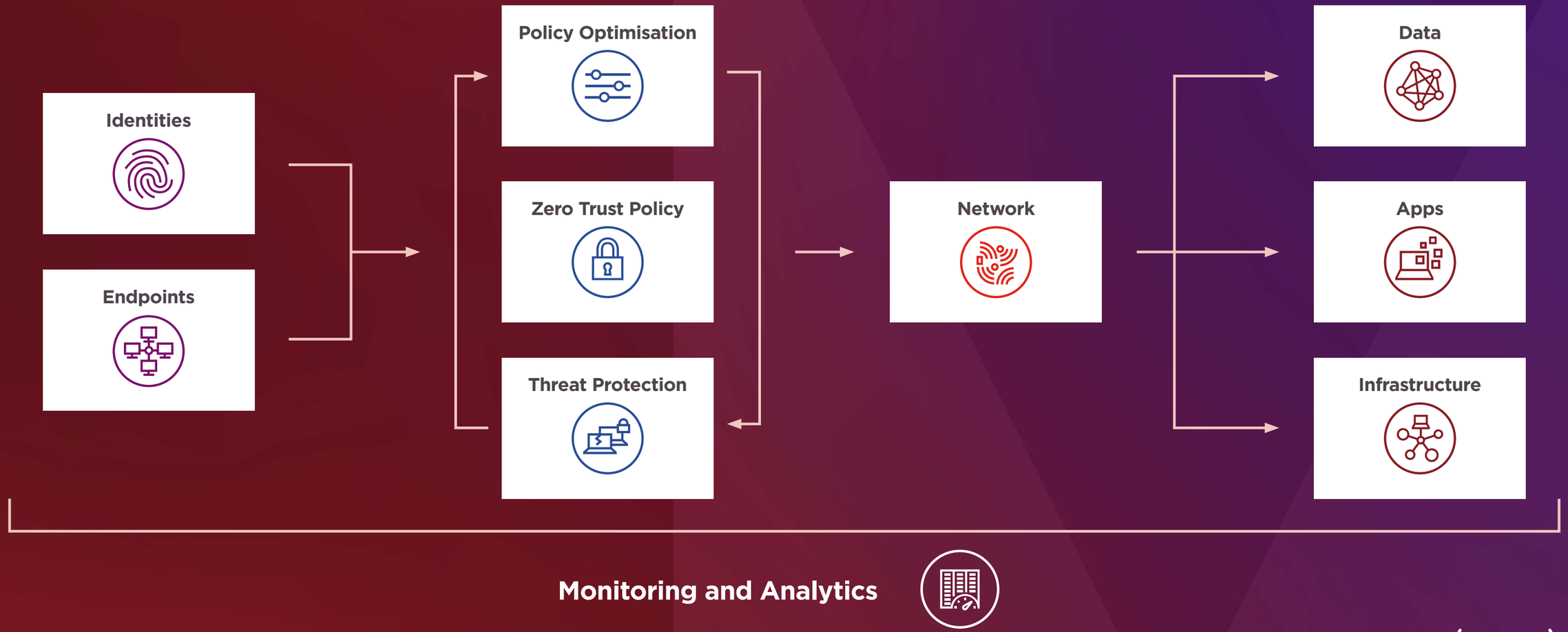
reduction in management time due to improved security processes[3]

Lenovo ThinkShield portfolio and Microsoft Security solutions are specifically and purposefully designed help you implement an **end-to-end Zero Trust strategy** and protect your business at all levels.

[1] Microsoft Zero Trust Adoption Report, 2021
[2] IBM Cost of a Data Breach Report 2021
[3] The Total Economic Impact™ of Zero Trust solutions from Microsoft, December 2021. Study by Forrester Consulting, commissioned by Microsoft.
[4] 1H Global Threat Landscape Report from FortiGuard Labs

This is what Zero Trust architecture looks like.

The concept of Zero Trust is spread across many parts of IT, but protection starts with Windows 11 modern devices, user identities, and endpoint device monitoring.



Enhance and secure the hybrid working experience for your employee with Lenovo Windows 11 Pro devices

Windows 11 Pro - the most secure Windows yet - helps you **streamline management** of your hybrid workplace while you **protect data and access** anywhere.

Designed for modern devices optimized for security, it gives you the latest benefits of **hardware-based protection**, tightly integrated with software. Windows 11 Pro is purpose-built for **secure hybrid work** with a **higher security baseline than Windows 10.** This includes new requirements for protection - built-in and enabled by default.

ThinkPad X1 Carbon

Enhance the security of your Lenovo Windows 11 Pro ThinkShield Device with cloud management

Protecting identities and endpoint devices is the first critical step in setting up a Zero Trust strategy. Identities and devices are the two main areas targeted by ID credential thieves, phishing mails, ransomware, other types of malware and advanced threats.

Combine Lenovo Windows 11 devices with Microsoft Cloud security solutions to roll out a Zero Trust Strategy.

Identity Management

- Enables Multifactor Authentication (MFA) which can stop 99.9% of identity attacks.
- Delivers a Conditional Access ‘intelligent’ policy engine that allows you to set specific rules for user ‘sign-in’. When paired with MFA it enables a muscular balance between security and user productivity.

Endpoint Management

- Ensure apps comply with your company’s security protocols using Mobile Access Management (MAM).
- Ensure devices comply with your company’s security protocols using Mobile Device Management (MDM) either on company owned devices or BYOD.

Control, Protect and Manage by leveraging the benefits of Security Cloud solutions

Identity Management with Azure Active Directory

- Azure Active Directory is a simple and efficient cloud-based identity and access management service that provides Multifactor Authentication and Conditional Access.
- Combines core directory services, application access management, and identity protection into a single solution.
- Helps your employees securely access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications.
- Secures internal resources such as an intranet and cloud apps developed by your organisation.

Microsoft Defender for Endpoint

This industry-leading cloud powered endpoint security solution:

- Helps to secure against ransomware, file-less malware, and other sophisticated attacks on Windows, Mac OS, Linux, Android, and iOS.
- Discovers hidden threats by continually monitoring, in real time, code behavior and attacker techniques, enabling rapid detection and response.
- 24/7 automated incident response and remediation – helps security teams immediately go from alerts to AI driven remediation.
- Managed threat hunting service from ‘on demand’ Microsoft experts.

Microsoft Endpoint Manager

Get endpoint device management and security in a unified management platform:

- Secures, deploys, and manages all users, apps, and endpoint devices without disrupting existing working processes.
- Helps deliver the modern workplace and modern management to keep data secure, in the cloud and on-premises.
- Combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot.

Right device, right place, right time with Lenovo Zero Touch deployment solution

Secure, modern technology is key to ensuring the success of any business. But the traditional manual approach to deployment is complex, time-consuming and prone to error.

Now there's an easier way to ensure your hybrid and remote employees hit the ground running – **Lenovo Zero-Touch deployment with autopilot**.

It will galvanise hybrid working, increase productivity and free your IT teams to focus on innovation to drive the business.

With **Windows Autopilot**, IT departments no longer need to re-image or set up new devices manually. It's all done remotely. Lenovo Windows 11 devices come with Autopilot pre-configured. IT managers can customise user and apply configurations from any location.

- **Ready to go out of the box** – User simply turns on device and with a few simple clicks, its business ready.
- **Simple profile management** – Create manage and assign up to 350 different profiles to determine a user's settings and PC experience.
- **Effortless transition to the cloud** – Autojoin devices to Azure Active Directory and enroll them in mobile device management.
- **Problem free provisioning** – Personalised and streamlined set up.
- **Track progress** – Using Autopilot users can track the progress of device configuration.
- **Product registration** – Devices automatically registered to Autopilot Cloud Deployment service.

Adopt a “Better together” approach

Security out-of-the-box

- **Protect at the core** with TPM 2.0 silicon-assisted security, and data and identity safeguards.
- Simpler and more secure sign-in using **passwordless authentication** methods like Windows Hello for Business.
- Helps block malicious software with **built-in protection already enabled**.
- To help **keep you secure from the start**, Windows 11 prevents malware from loading when you boot.
- Data and network protection supported by **hardware-based root-of-trust** that helps maintain and verify device integrity.

Protect against evolving threats

- Protect credentials with **enhanced phishing protection** in Microsoft Defender Smartscreen.
- Sign in hands free with **presence sensing** – logs you in when you approach, locks when you leave.
- Protect your most sensitive data with **Secured-core PCs from Lenovo**.
- Get hardware-based credential protection with **Microsoft Pluton**.
- Take advantage of **intelligent threat detection and rapid responses** informed by 43 trillion security signals analysed daily.
- BitLocker encryption helps **protect your business information**, even on lost or stolen devices.
- Get more **protection from untrusted sources** – open files and websites in an isolated container with Microsoft Defender Application Guard.

Modern security management

- **Keep security features up to date** with Windows Update for Business.
- Enable the adoption of **Zero-Trust security** frameworks.
- **Ensure policy compliance for onsite and remote employees** with Microsoft Endpoint Manager.
- Deploy devices **preconfigured with corporate security policies** using Windows Autopilot and zero-touch deployment.
- Gain security and visibility by enabling **secure single sign-on** across all your apps with Azure Active Directory.
- **Cloud-first design enables easy extensibility** with Microsoft 365, Microsoft Defender for Cloud, and Microsoft Defender for Endpoints.
- Help **prevent malicious code** and protect against malware and other untrusted software with Windows Defender Application Control.

Lenovo – your trusted partner for Zero Trust Strategy implementation and hybrid working

Why choose Lenovo?

Experience, expertise, enterprise-strength capability and a dedicated team of experts to support your cloud adoptions, security policy definition and implementations.
As a Microsoft Cloud Solutions Provider-authorised partner (CSP), Lenovo offers the full portfolio of Microsoft Cloud services, including Microsoft 365 and Azure services.

Microsoft Partner

Microsoft

2022 Partner of the Year Winner
Device Award

Microsoft Gold Partner and Device Partner of the Year

Lenovo meets Microsoft's strict requirements to be recognised as a Gold Partner which confirms that Lenovo have the expertise and capabilities to provide you with high-end and secure solutions for your remote working.

In addition to that, Lenovo has received the prestigious Microsoft Device Partner of the Year Award. This recognises excellence in building, marketing, or selling devices and IT solutions that champion Microsoft-based technology.

The award came on the back of Lenovo's track record in delivering integrated solutions and services, consistently, flexibly, and predictably, to meet its customers' current digital transformation demand and future-proof their businesses.

Our cloud strategy: everything from one vendor

Lenovo's goal is a true hybrid organisation, able to deploy on-premises, private and public cloud, meeting our customers' needs for storage, software and solutions. That ties in with our ability to offer hardware, services, software, device-as-a-service, and support – all from one vendor.

Here's how we make your Zero Trust Strategy solution work for your business

Lenovo's Managed and Professional Services put you on track for a smooth, problem-free, upgrade to Zero Trust defenses.

- From solution design to onboarding to final migration Lenovo has all your needs covered.
- If you have a Microsoft 365 license, we simply refresh Windows 11 devices and Microsoft 365 and include Azure Active Directory, Microsoft Defender, and Endpoint Manager.
- Premier support – dedicated user hotline, 24/7, 365 days a year.
- Dedicated experts – locally-based experts primed to support your move to secure hybrid working.
- Enterprise grade security – top cyber security defenses that beat back the swelling tide of malware and targeted attacks.

Contact us today to see how Lenovo can support you in building your organisation's Zero Trust security strategy.

Book a meeting

Microsoft 365

Smarter technology for all

Lenovo