Vertrauen Sie Ihren Sicherheitsmaßnahmen. Vertrauen Sie Ihren Mitarbeitern. Mit Lenovo.

So schützen Sie Ihre Mitarbeiter in einer dynamischen Cybersicherheitsumgebung

Smarter technology for all

Lenovo

Die endgültige Umstellung auf hybride Arbeitsmodelle hat ein schwieriges Umfeld für die Cybersicherheit geschaffen.

Die meisten Mitarbeiter müssen heute für hybride Arbeitsmodelle ausgestattet sein. Daher muss der Schutz vor Bedrohungen auf mehrere Clouds und unterschiedliche Plattformen ausgeweitet werden.

So entsteht ein komplexes digitales Umfeld, in dem sich unbekannte Bedrohungen verbergen können. Die Durchsetzung von einheitlichen Sicherheitsrichtlinien für verschiedene Geräte und digitale Ebenen ist eine sehr anspruchsvolle Aufgabe. Sie bereitet denjenigen, die für die Sicherheit zuständig sind, häufig schlaflose Nächte.

Die Sicherheitslösung für Hardware und Cloud – eine einzigartige Partnerschaft: Das Ergebnis der einzigartigen Partnerschaft von Lenovo und Microsoft ist die Kombination von ThinkShield Hardware mit Microsoft Cloud Security Services.

Sicherheit durch Design mit Lenovo ThinkShield

Wir bei Lenovo wissen, wie dringend ein umfassender Schutz benötigt wird. Mit unserem ThinkShield Sicherheitskonzept, das auf bewährten Schutzmaßnahmen basiert, wollen wir unser Geräteportfolio durch Design noch sicherer machen.

Dies erstreckt sich vom Schutz der Lieferketten bis hin zur Entwicklung neuer sicherer Lenovo Produkte von den Herstellern der weltweit zuverlässigsten Business-PCs.

Unser einzigartiges ThinkShield Portfolio mit Hardware, Services, Software und Prozessen bietet Schutz auf allen Ebenen des Unternehmens. Unsere Zusammenarbeit mit branchenführenden Sicherheitsanbietern ermöglicht umfassende Abwehrmaßnahmen zur Abschottung und Eindämmung von Bedrohungen sowie zur Förderung einer Zero-Trust-Strategie, unterstützt durch die Sicherheitslösungen von Microsoft.

Zero Trust. Die Cybersicherheit der Zukunft geht neue Wege.

Zero Trust unterscheidet sich stark von traditioneller Netzwerksicherheit, bei der es eine „Unternehmensgrenze“ gibt oder Geräte über ein VPN verbunden sind, was heute mehr oder weniger die Norm ist.

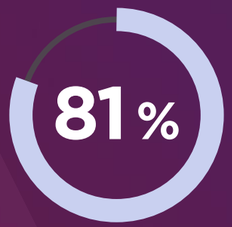
Die Leitprinzipien von Zero Trust lauten: „Niemals vertrauen. Immer überprüfen.”

In der heutigen hybriden Arbeitswelt sollten Geräte nicht automatisch als vertrauenswürdig eingestuft werden, selbst wenn sie mit einem „zugelassenen” Netzwerk verbunden sind.

Zero Trust geht davon aus, dass sich ein Angreifer innerhalb des Netzwerks befindet. Vertrauen wird **kontextbezogen** hergestellt, z. B. aufgrund von **Identität und Standort des Benutzers, des Sicherheitsstatus des Geräts** und der **angeforderten Anwendungen oder Dienste**. Bei jedem Schritt erfolgen Richtlinienkontrollen.

Dadurch wird gewährleistet, dass nur **die richtigen Personen mit den richtigen Ressourcen auf sicheren Geräten auf Ihre Daten zugreifen können**.

Zero Trust war noch nie so dringend notwendig wie heute:

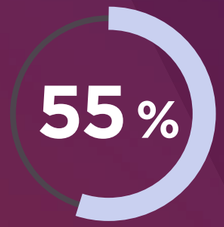


der Unternehmen haben mit der Umstellung auf hybride Arbeitsmodelle begonnen[1]

geringeres Risiko einer Datensicherheitsverletzung[3]

1.070 %

mehr Ransomware zwischen Juli 2020 und Juni 2021[4]



der Unternehmen geben an, in den letzten 18 Monaten einen Phishing-Angriff festgestellt zu haben[2]

weniger Anrufe bei IT- und Helpdesk-Analysten[3]

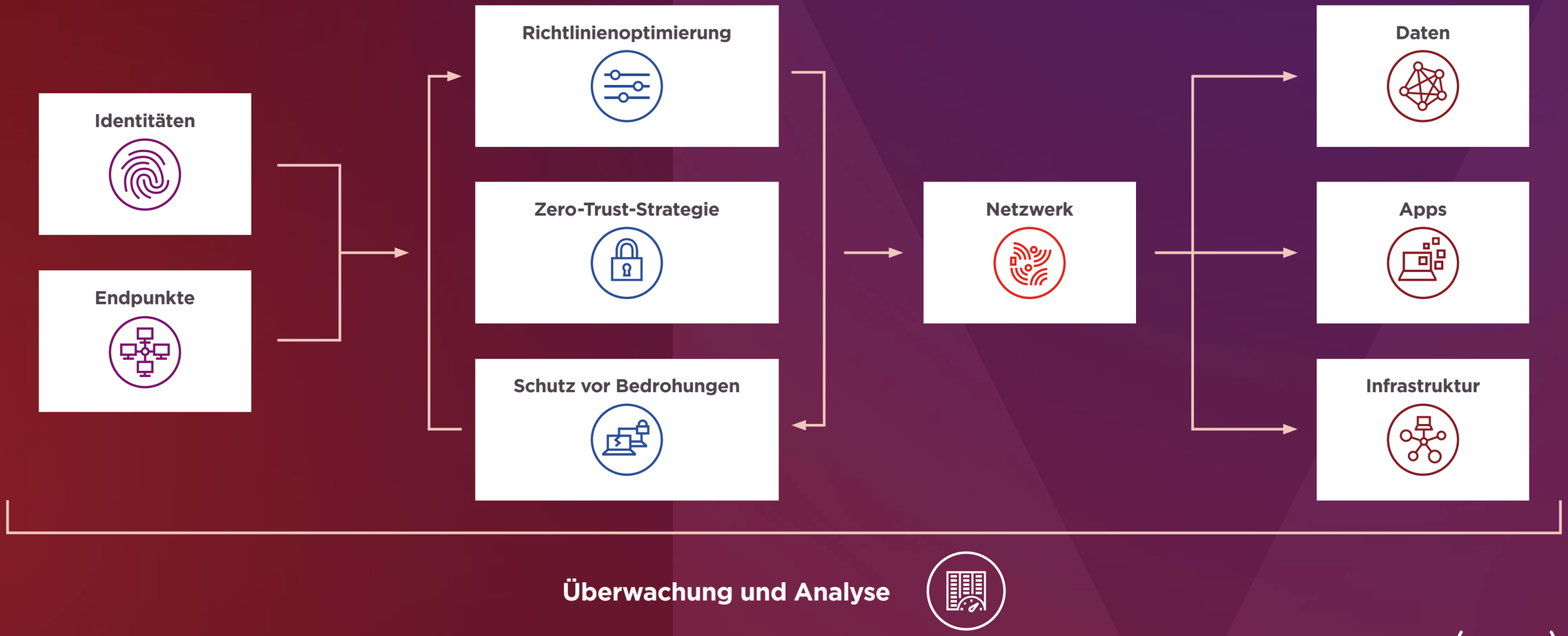
Zeitersparnis für das Management durch bessere Sicherheitsverfahren[3]

Das Lenovo ThinkShield Portfolio und die Sicherheitslösungen von Microsoft sind speziell darauf ausgelegt, Sie bei der Umsetzung einer **umfassenden Zero-Trust-Strategie** zu unterstützen und Ihr Unternehmen auf allen Ebenen zu schützen.

[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, Dezember 2021. Studie von Forrester Consulting im Auftrag von Microsoft.
[4] 1H Global Threat Landscape Report von FortiGuard Labs

So sieht eine Zero-Trust-Architektur aus.

Das Konzept von Zero Trust erstreckt sich über viele Bereiche der IT, der Schutz beginnt jedoch mit modernen Windows 11-Geräten, Benutzeridentitäten und der Überwachung von Endgeräten.



Bieten Sie Ihren Mitarbeitern bessere und sicherere hybride Arbeitsmöglichkeiten mit Windows 11-Geräten von Lenovo

Mit Windows 11 Pro – dem bisher sichersten Windows – können Sie die **Verwaltung** Ihrer hybriden Arbeitsplätze optimieren sowie **Ihre Daten schützen und von überall darauf zugreifen**.

Es wurde für moderne, sicherheitsoptimierte Geräte entwickelt und bietet Ihnen die neuesten Vorteile eines **hardwarebasierten Schutzes**, der nahtlos in die Software integriert ist. Windows 11 Pro wurde speziell für die **Sicherheit in der hybriden Arbeitswelt entwickelt** und bietet einen **höheren Grad an Sicherheit als Windows 10**. Dies umfasst auch neue Anforderungen an den Schutz – er ist integriert und standardmäßig aktiviert.

ThinkPad X1 Carbon

Verbessern Sie die Sicherheit Ihres Lenovo ThinkShield Geräts mit Windows 11 Pro durch Cloudmanagement

Der Schutz von Identitäten und Endgeräten ist der erste wichtige Schritt bei der Einführung einer Zero-Trust-Strategie. Identitäten und Geräte stellen die beiden Hauptangriffsflächen für Identitätsdiebstahl, Phishing-Mails, Ransomware und andere Arten von Malware sowie die neuesten Bedrohungen dar.

Kombinieren Sie für die Einführung einer Zero-Trust-Strategie Windows 11-Geräte von Lenovo mit Microsoft Cloud-Sicherheitslösungen.

Identitätsverwaltung

- Ermöglicht die Multifaktor-Authentifizierung (MFA), die 99,9 % der Angriffe auf Identitäten stoppen kann.
- Über eine „intelligente" Richtlinien-Engine für den bedingten Zugriff können Sie spezifische Regeln für die Benutzeranmeldung festlegen. In Kombination mit MFA ist so ein ausgewogenes Verhältnis von Sicherheit und Benutzerproduktivität möglich.

Endpunktverwaltung

- Stellen Sie mit Mobile Access Management (MAM) sicher, dass Anwendungen den Sicherheitsprotokollen Ihres Unternehmens entsprechen.
- Sorgen Sie dafür, dass Geräte den Sicherheitsprotokollen Ihres Unternehmens genügen, indem Sie Mobile Device Management (MDM) entweder auf unternehmenseigenen Geräten oder BYOD einsetzen.

Kontrolle, Schutz und Verwaltung durch Nutzung der Vorteile von Security Cloud-Lösungen

Identitätsverwaltung mit Azure Active Directory

- Azure Active Directory ist ein einfacher und effizienter cloudbasierter Dienst für die Identitäts- und Zugriffsverwaltung, der Multifaktor-Authentifizierung und bedingten Zugriff bietet.
- Kombiniert wichtige Verzeichnisdienste, die Zugriffsverwaltung für Anwendungen und Identitätsschutz in einer einzigen Lösung.
- Ermöglicht Ihren Mitarbeitern den sicheren Zugriff auf externe Ressourcen wie Microsoft 365, das Azure-Portal und Tausende anderer SaaS-Anwendungen.
- Schützt interne Ressourcen, wie zum Beispiel ein Intranet, und von Ihrem Unternehmen entwickelte Cloud-Anwendungen.

Microsoft Defender for Endpoint

Diese branchenführende cloudbasierte Sicherheitslösung für Endpunkte bietet Folgendes:

- Sie trägt zum Schutz vor Ransomware, dateiloser Malware und anderen raffinierten Angriffen auf Windows, Mac OS, Linux, Android und iOS bei.
- Sie deckt versteckte Bedrohungen durch kontinuierliche Echtzeit-Überwachung des Code-Verhaltens und der Angreifertechniken auf und ermöglicht so eine schnelle Erkennung und Reaktion.
- Sie bietet rund um die Uhr eine automatische Reaktion auf Vorfälle sowie Abhilfemaßnahmen – damit können Sicherheitsteams im Falle von Warnungen sofort mit der KI-gesteuerten Behebung beginnen.
- Verwalteter Service zur Bedrohungserkennung durch Microsoft-Experten on demand.

Microsoft Endpoint Manager

Erhalten Sie Endgeräteverwaltung und -sicherheit in einer einheitlichen Verwaltungsplattform:

- Schutz, Einrichtung und Verwaltung aller Benutzer, Anwendungen und Endgeräte, ohne die bestehenden Arbeitsabläufe zu stören.
- Unterstützt die Bereitstellung moderner Arbeitsplätze und einer modernen Verwaltung, um Daten in der Cloud und vor Ort zu schützen.
- Kombiniert Dienste, die Sie möglicherweise kennen und bereits nutzen, wie Microsoft Intune, Configuration Manager, Desktop Analytics, Co-Management und Windows Autopilot.

Das richtige Gerät am richtigen Ort zur richtigen Zeit – mit der Lenovo Zero-Touch Deployment Lösung

Sichere, moderne Technologie ist für den Erfolg jedes Unternehmens entscheidend. Doch der herkömmliche manuelle Bereitstellungsansatz ist komplex, zeitaufwändig und fehleranfällig.

Jetzt gibt es einen einfacheren Weg, um sicherzustellen, dass Ihre Mitarbeiter in hybriden und ortsunabhängigen Arbeitsmodellen sofort einsatzbereit sind – **Lenovo Zero-Touch Deployment mit Autopilot**.

Es fördert hybride Arbeitsweisen, steigert die Produktivität und entlastet Ihre IT-Teams, damit sie sich auf Innovationen konzentrieren können, um das Geschäft voranzutreiben.

Mit **Windows Autopilot** müssen IT-Abteilungen für neue Geräte keine neuen Images mehr erstellen oder sie manuell einrichten. Alles erfolgt remote. Windows 11-Geräte von Lenovo sind mit Autopilot vorkonfiguriert. IT-Manager können von jedem beliebigen Standort aus Benutzer anpassen und Konfigurationen anwenden.

- **Sofort einsatzbereit** – das Gerät muss nur eingeschaltet werden und kann nach ein paar einfachen Klicks voll genutzt werden.
- **Einfache Profilverwaltung** – Sie können bis zu 350 verschiedene Profile erstellen, verwalten und zuweisen, um Einstellungen und Nutzungserfahrung festzulegen.
- **Müheloser Übergang in die Cloud** – Windows Autopilot kann Geräte automatisch mit Azure Active Directory verbinden und für die Mobilgeräteverwaltung registrieren.
- **Reibungslose Bereitstellung** – Personalisierte und optimierte Einrichtung.
- **Fortschrittsverfolgung** – Mit Autopilot können Benutzer den Fortschritt der Gerätekonfiguration verfolgen.
- **Produktregistrierung** – Geräte werden automatisch beim Autopilot Cloud Deployment Service registriert.

Entscheiden Sie sich für einen „Better Together“-Ansatz

Sicherheit von Anfang an

- **Schutz, der im Kern ansetzt**, mit der siliziumgestützten Sicherheit eines TPM 2.0 sowie Schutzmaßnahmen für Daten und Identität.
- Einfache und sichere Anmeldung mit **passwortlosen Authentifizierungsmethoden** wie Windows Hello for Business.
- Trägt zur Blockierung von Schadsoftware bei, da der **integrierte Schutz bereits aktiviert ist**.
- Damit Sie von **Anfang an sicher sind, verhindert** Windows 11, dass beim Hochfahren Malware geladen wird.
- Der Schutz von Daten und Netzwerk wird durch vertrauenswürdige **Hardware unterstützt**, die zur Aufrechterhaltung und Überprüfung der Integrität des Geräts beiträgt.

Schutz vor neuen Bedrohungen

- Schützen Sie Ihre Anmeldedaten mit dem **erweiterten Phishing-Schutz** von Microsoft Defender Smartscreen.
- Loggen Sie sich freihändig über den **Anwesenheitssensor** ein – er meldet Sie an, wenn Sie sich nähern, und sperrt das Gerät, wenn Sie sich entfernen.
- Schützen Sie Ihre sensibelsten Daten mit **Secured-Core-PCs von Lenovo**.
- Nutzen Sie den hardwarebasierten Schutz von Anmeldeinformationen mit **Microsoft Pluton**.
- Profitieren Sie von **intelligenter Bedrohungserkennung und schnellen Reaktionen** auf der Grundlage von 43 Billionen Sicherheitssignalen, die täglich analysiert werden.
- Mit der Verschlüsselung durch BitLocker können Sie **Ihre Geschäftsdaten sogar auf verlorenen oder gestohlenen Geräten schützen**.
- **Schützen Sie sich besser vor nicht vertrauenswürdigen Quellen** – öffnen Sie Dateien und Websites in einem isolierten Container mit Microsoft Defender Application Guard.

Modernes Sicherheitsmanagement

- **Halten Sie Sicherheitsfunktionen** mit Windows Update for Business auf dem neuesten Stand.
- Ermöglichen Sie die Einführung von **Zero-Trust-Sicherheitssystemen**.
- Gewährleisten Sie mit Microsoft Endpoint Manager **die Einhaltung von Richtlinien für Mitarbeiter vor Ort und außerhalb**.
- Stellen Sie mithilfe von Windows Autopilot und Zero-Touch Deployment Geräte bereit, die mit den **Sicherheitsrichtlinien des Unternehmens vorkonfiguriert sind**.
- Steigern Sie Sicherheit und Transparenz, indem Sie mit Azure Active Directory eine **sichere einmalige Anmeldung** für alle Ihre Anwendungen ermöglichen.
- **Dank Cloud-First-Design ist eine mühelose Erweiterung** mit Microsoft 365, Microsoft Defender for Cloud und Microsoft Defender for Endpoints möglich.
- **Verhindern Sie mit Windows Defender Application Control bösartigen Code** und schützen Sie sich vor Malware und anderer nicht vertrauenswürdiger Software.

Lenovo – Ihr zuverlässiger Partner für die Umsetzung einer Zero-Trust-Strategie und hybride Arbeitsmodelle

Warum Lenovo?

Erfahrung, Fachwissen, Kompetenz auf Unternehmensniveau und ein engagiertes Expertenteam, das Sie bei der Einführung der Cloud, der Festlegung von Sicherheitsrichtlinien und der Implementierung unterstützt. Als autorisierter Microsoft Cloud Solutions Provider (CSP) bietet Lenovo das gesamte Portfolio der Microsoft Cloud Services an, einschließlich Microsoft 365 und Azure Services.

Microsoft Partner

Microsoft

2022 Partner of the Year Winner
Device Award

Microsoft Gold Partner und Device Partner of the Year

Lenovo erfüllt die strengen Anforderungen von Microsoft für die Anerkennung als Gold Partner. Lenovo verfügt also nachweislich über die nötigen Fachkenntnisse und Fähigkeiten, um Ihnen hochwertige und sichere Lösungen für ortsunabhängiges Arbeiten zu bieten.

Darüber hinaus wurde Lenovo mit dem angesehenen Microsoft Device Partner of the Year Award ausgezeichnet. Damit werden herausragende Leistungen bei der Entwicklung, der Vermarktung oder dem Verkauf von Geräten und IT-Lösungen ausgezeichnet, die Microsoft-basierte Technologien nutzen.

Die Auszeichnung wurde auf Basis der Erfolgsbilanz von Lenovo in Bezug auf die einheitliche, flexible und berechenbare Bereitstellung integrierter Lösungen und Services verliehen, die den aktuellen Bedarf der Kunden an digitaler Transformation decken und ihre Unternehmen zukunftssicher machen.

Unsere Cloud-Strategie: alles aus einer Hand

Lenovo möchte sich zu einem echten Hybridunternehmen wandeln, das in der Lage ist, On-Premises, Private und Public Cloud bereitzustellen und den Bedarf der Kunden an Speicherprodukten, Software und Lösungen zu decken. Dies knüpft an unsere Fähigkeit an, Hardware, Services, Software, Device as a Service und Support anzubieten – alles aus einer Hand.

So unterstützen wir Sie bei der erfolgreichen Umsetzung Ihrer Lösung für eine Zero-Trust-Strategie in Ihrem Unternehmen

Mit den verwalteten und professionellen Services von Lenovo sind Sie auf dem besten Weg zu einem unkomplizierten und reibungslosen Upgrade auf Zero-Trust-Abwehrmechanismen.

- Vom Lösungsdesign über das Onboarding bis hin zur endgültigen Migration deckt Lenovo alle Ihre Anforderungen ab.
- Wenn Sie über eine Microsoft 365-Lizenz verfügen, aktualisieren wir einfach Windows 11-Geräte und Microsoft 365 und beziehen Azure Active Directory, Microsoft Defender und Endpoint Manager mit ein.
- Premier Support – spezielle Benutzer-Hotline, rund um die Uhr, das ganze Jahr.
- Engagierte Experten – Fachkräfte vor Ort, die Sie bei der Umstellung auf sichere hybride Arbeitsmodelle unterstützen.
- Sicherheit auf Unternehmensniveau – erstklassige Cybersicherheit gegen die wachsende Flut von Malware und gezielten Angriffen.

Smarter technology for all

Lenovo

Setzen Sie sich noch heute mit uns in Verbindung und erfahren Sie, wie Lenovo Sie bei der Entwicklung einer Zero-Trust-Sicherheitsstrategie für Ihr Unternehmen unterstützen kann.

Termin vereinbaren

Microsoft 365