Microsoft

Der Schlüssel zu sicherer Produktivität in zwei Schritten

Wie eine Zero Trust-Grundlage produktive Arbeitserfahrungen ermöglicht

Inhalt

Einleitung

Halten Sie sich nicht mit der wachsenden Bedrohungslandschaft auf, sondern seien Sie ihr voraus

Die heutige Bedrohungslandschaft wächst schnell. Ausgefeilte Bedrohungen wie Identitätsangriffe, Ransomware und Endpunktangriffe gefährden Daten und die IT-Infrastruktur. Die Realität der modernen Arbeitswelt hat den Druck auf die IT-Teams erhöht, die oft überfordert sind, wenn es darum geht, eine wachsende Zahl von Sicherheitslücken zu schließen.

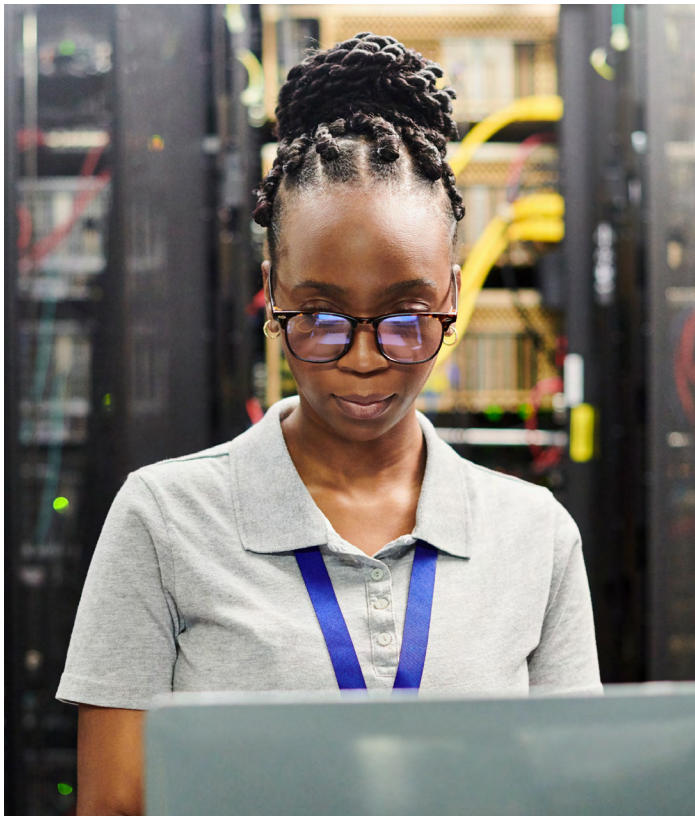
67 % der IT-Expert*innen geben an, dass sie mit der Verwaltung von Remote-Arbeitsplätzen überfordert sind. Daher ist es entscheidend, den Bedrohungen zuvorzukommen, um kostspielige Sicherheitsverletzungen und Ausfallzeiten zu vermeiden.[1] Die Ausdünnung der IT-Teams macht es Angreifenden leichter, erfolgreich zu sein, was schwerwiegende finanzielle und rufschädigende Folgen haben kann.

Der Schlüssel zum Erfolg in dieser wachsenden Bedrohungslandschaft liegt nicht darin, noch mehr von den IT-Teams zu verlangen, sondern vielmehr darin, eine solide Sicherheitsgrundlage in Form eines Zero Trust-Sicherheitsmodells zu schaffen. Diese Sicherheitsgrundlage entlastet die IT-Teams und trägt dazu bei, das Risiko und die Schwere von Angriffen zu verringern. Und genau hier beginnen die Vorteile.

Dieses E-Book untersucht die gängigen Sicherheitsbarrieren in der heutigen Zeit und erörtert, wie die Implementierung von Zero Trust Security Unternehmen hilft, diese zu überwinden. Wir werden auch die positiven Auswirkungen eines Zero Trust-Sicherheitsmodells auf die Produktivität des Teams und die KI-Bereitschaft diskutieren.

Die größten Sicherheitsherausforderungen

Cyberkriminelle werden immer raffinierter und organisierter, wobei böswillige Akteur*innen fortschrittliche Tools und Taktiken einsetzen, um Schwachstellen zu finden und auszunutzen. Wenn Cyberkriminelle erfolgreich sind, kann der Schaden für den Ruf und die Finanzen des Opfers schwerwiegend sein – vor allem, wenn die Verletzung sensible oder persönliche Daten betrifft. Extern kann der Verlust des Vertrauens von Kunden, Partnern und Investoren zu einem Rückgang des Marktanteils, der Kundenabwanderung und zu niedrigeren Bewertungen führen. Intern stören Cyberangriffe den Betrieb und verursachen Ausfallzeiten, Produktivitätseinbußen und Umsatzeinbußen.



Der wachsende finanzielle Schaden durch Cyberkriminalität

23,84 Billionen USD

Die geschätzten Kosten der weltweiten Cyberkriminalität werden bis 2027 voraussichtlich **23,84 Billionen USD betragen.** [2]

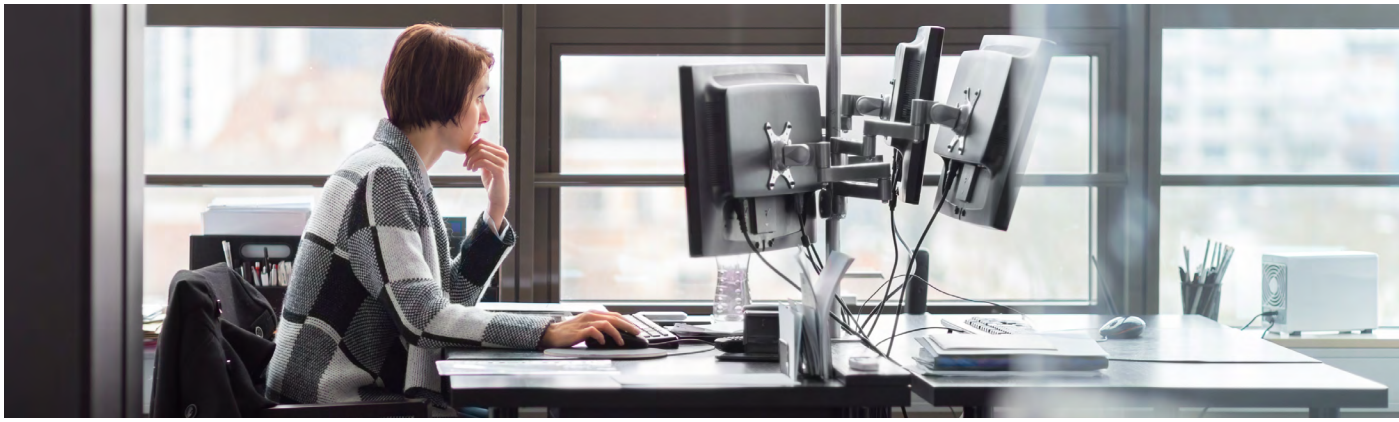
Die wichtigsten Sicherheitsprobleme der modernen Arbeitswelt

Angesichts dieser schwerwiegenden Folgen sehen sich IT-Teams mit mehreren wichtigen Herausforderungen konfrontiert.

Verifizieren der Identität
Die Angreifenden verwenden verschiedene Techniken wie Phishing, Malware und Domain-Spoofing, um Anmeldedaten von Benutzer*innen zu erlangen. Diese Anmeldeinformationen (Kennwörter, Benutzer-IDs, E-Mails usw.) werden dann verwendet, um Zugang zu Unternehmensressourcen zu erhalten, Daten zu stehlen oder Konten zu kompromittieren.

1.287
kennwortbasierte Angriffe pro Sekunde.[3]

31 Millionen
Die Zahl der Phishing-Angriffe stieg im vergangenen Jahr auf **31 Millionen** pro Monat.[4]



Schutz einer modernen Belegschaft
Die Arbeitsmodelle vieler Unternehmen haben sich in den letzten Jahren rasant verändert: **12,7** % der Vollzeitbeschäftigten arbeiten jetzt von zu Hause aus und **28,2 %** nutzen ein Hybridmodell.[5] Diese Mitarbeitenden treffen nicht immer die richtigen Vorkehrungen zur Abwehr von Bedrohungen, was Cyberkriminellen weitere Schwachstellen eröffnet. Die Arbeit mit veralteter Hardware und nicht verwalteten Geräten, die nicht konform sind, erhöht die IT-Komplexität und macht Unternehmen anfälliger für Angriffe.

80–90 %
der erfolgreichen Ransomware-Angriffe erfolgen über nicht verwaltete Geräte.[6]

71 %
der Mitarbeitenden infizieren sich häufiger auf einem nicht verwalteten Gerät.[7]

86 %
der Sicherheitsverantwortlichen sagen, dass veraltete PC-Hardware Unternehmen verwundbarer macht.[8]

Schutz von Informationen

Cyberkriminelle versuchen, sich einen Wettbewerbsvorteil zu verschaffen, indem sie den Betrieb eines Unternehmens stören oder geistiges Eigentum wie Geschäftsgeheimnisse, Patente, Marken und Urheberrechte stehlen. Der Diebstahl von geistigem Eigentum kann durch finanziellen Gewinn, Wirtschaftsspionage oder Industriesabotage motiviert sein. Je mehr Sicherheitsprobleme ein Unternehmen zu bewältigen hat – Software- und Firmware-Patches, Hardware-Upgrades sowie interne und externe Sicherheitslücken –, desto weniger Zeit und Arbeit können eingesetzt werden, um sich auf Angriffe auf kritische Daten vorzubereiten.

70 %

der Unternehmen wurden durch nicht zugelassene Software, Anwendungen und Dienste kompromittiert.[9]

62 %

der Mitarbeitenden investieren nicht genug Zeit in strategische Aufgaben wie Sicherheitsstrategie oder die Vorbereitung auf raffinierte Angriffe.[10]

Unternehmen müssen einen proaktiven und widerstandsfähigen Ansatz für die Cybersicherheit wählen, um sich in dieser komplexen und sich ständig weiterentwickelnden Bedrohungslandschaft zurechtzufinden. Heute bedeutet dies, dass wir von einem traditionellen, reaktiven Rahmen zu einem proaktiven Zero Trust-Rahmen übergehen müssen.

Schritt 1
Schaffung einer Zero Trust-Sicherheitsgrundlage

Zero Trust ist ein Sicherheitsmodell, das nach dem Motto **„Never trust, always verify“** funktioniert. Es geht davon aus, dass Vertrauen eine Schwachstelle ist, die ausgenutzt werden kann, um Angriffspunkte zu finden, und verlangt, dass Sie Leitplanken aufstellen, die sicherstellen, dass Cyberkriminelle nicht unbeabsichtigt durch Ihre Verteidigungsmaßnahmen gelangen können.

Never trust

Vertrauen Sie niemals implizit einer Entität, weder intern noch extern.

Always verify

Überprüfen Sie kontinuierlich Identitäten, Geräte, Daten und Netzwerke.

Zero Trust-Prinzipien

Anstatt davon auszugehen, dass alles, was sich hinter der Unternehmensfirewall befindet, vertrauenswürdig ist, geht Zero Trust Security davon aus, dass jede (interne oder externe) Einheit, die versucht, auf Unternehmensressourcen zuzugreifen, eine potenzielle Bedrohung darstellt. Diese Annahme macht es notwendig, drei Prinzipien anzuwenden: explizite Überprüfung, Implementierung des am wenigsten privilegierten Zugriffs und Annahme einer Verletzung.

Explizit überprüfen
Der erste Grundsatz soll sicherstellen, dass die Person, die versucht, auf Ihr Netzwerk zuzugreifen, diejenige ist, die sie vorgibt zu sein. Jede Zugriffsanfrage auf eine Ressource wird auf der Grundlage mehrerer Faktoren authentifiziert und autorisiert, darunter die Identität des Benutzers oder der Benutzerin, das Gerät, der Standort, der Dienst oder die Workload, auf den/die er/sie zugreift, die Datenklassifizierung und alle identifizierten Anomalien oder Risiken. Dadurch wird sichergestellt, dass berechtigte Benutzer*innen und Geräte auf Unternehmensressourcen zugreifen können, während verdächtige Einheiten blockiert oder befragt werden.

Implementierung des Least-Privilege-Zugangs
Dieses Prinzip gewährleistet, dass Benutzer*innen Zugriff auf die Ressourcen erhalten, die sie für die Erledigung ihrer Aufgaben benötigen – und nicht mehr. Dieser Ansatz begrenzt die Offenlegung sensibler Daten und Ressourcen für unbefugte oder kompromittierte Benutzer*innen und Geräte und schränkt das Ausmaß des Schadens ein, den Angreifende im Netzwerk anrichten können. Methoden wie Just-in-Time- und Just-enough-Access-Policies (JIT/JEA), adaptive Policies auf der Grundlage von Risikobewertungen und Datenschutzstrategien helfen bei der Durchsetzung dieses Grundsatzes.

Annahme einer Sicherheitsverletzung
Dieser Grundsatz zielt darauf ab, den Schaden zu minimieren, den eine Sicherheitsverletzung anrichten kann. Die Annahme von Sicherheitsverletzungen beinhaltet die Segmentierung des Zugriffs auf Ressourcen, die Gewährleistung der Verschlüsselung von Daten bei der Übertragung und im Ruhezustand sowie die Verwendung von Analytics zur Transparenz, Erkennung von Bedrohungen und Verbesserung der Verteidigung. Diese Strategie ist von entscheidender Bedeutung, um den Radius eines Angriffs zu verkleinern und zu verhindern, dass sich Angreifende innerhalb des Netzes seitlich bewegen können, falls sie doch Zugang erhalten.

Best Practices für die Umsetzung der Zero Trust-Prinzipien: Schutz von Identitäten und Endpunkten

Der Aufbau einer sicheren Grundlage erfordert eine moderne Produktivitätslösung wie Microsoft 365 E3. Sie umfasst integrierte Zero Trust-, KI- und Automatisierungsfunktionen, um Identitäten schnell zu überprüfen, autorisierten Benutzer*innen Zugriff zu gewähren und plattformübergreifend auf Bedrohungen zu überwachen. Um Zero Trust-Sicherheit zu etablieren, sollten Sie sich nach umfassenden Lösungen umsehen, die diese wichtige Grundlage für den Schutz von Identitäten und Endgeräten bieten, um die bestmögliche – und sicherste – Produktivität für Ihre Mitarbeitenden zu ermöglichen.

Identitäten schützen

Setzen Sie eine mehrstufige Authentifizierung ein: Benutzer*innen müssen ihre Identität über eine zweite Quelle (z. B. ein Telefon oder ein Token) bestätigen, bevor sie Zugang erhalten.

Aktivieren Sie die kennwortlose Authentifizierung: Lassen Sie die Benutzer*innen ihre Identität überprüfen, ohne ein Kennwort einzugeben, indem Sie eine andere Form des Nachweises verlangen, z.B. einen Fingerabdruck oder einen eindeutigen Code.

Implementieren Sie Single Sign-On (SSO): Sie müssen nicht mehr mehrere Anmeldedaten für dieselbe Person verwalten, so dass die Mitarbeitenden bei der Verwendung verschiedener Anwendungen weniger Anmeldeaufforderungen erhalten.

Erweitern Sie Ihre Lösung für die Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM) mit mehr Daten: Geben Sie mehr Daten in Ihre IAM-Lösung ein, um einen besseren Überblick darüber zu erhalten, wer auf Unternehmensressourcen zugreift.

Endpunkte schützen

Blockieren Sie die Legacy-Authentifizierung: Verhindern Sie, dass Anwendungen oder Geräte alte Protokolle verwenden, die keine modernen Sicherheitsfunktionen unterstützen, damit böswillige Akteur*innen nicht mit gestohlenen oder wiederverwendeten Anmeldedaten auf Ressourcen zugreifen können.

Führen Sie Risikobewertungen in Echtzeit durch: Überprüfen und bewerten Sie kontinuierlich das Risikoniveau jeder Zugriffsanfrage mithilfe von KI, Automatisierung und Analytics, um sicherzustellen, dass Anomalien in Echtzeit erkannt und entschärft werden.

Bewerten und optimieren Sie kontinuierlich Ihren Sicherheitsstatus: Seien Sie raffinierten Bedrohungen immer einen Schritt voraus, indem Sie Ihren Identitäts- und Sicherheitsstatus regelmäßig überprüfen, um zu sehen, wie gut Ihre Umgebung mit den aktuellen Best Practices übereinstimmt.

Vorteile der Implementierung eines Zero Trust-Sicherheitsmodells

Wie die Anwendung des „Never trust, always verify"-Modells Sie besser vor Cyberbedrohungen schützt

Verbessern Sie die Sicherheit
Durch die Minimierung der Angriffsfläche und die Blockierung unerlaubter Zugriffe reduziert Zero Trust die Zahl der ausnutzbaren Schwachstellen, die durch den täglichen Betrieb entstehen. Und sollte es böswilligen Akteur*innen gelingen, sich Zugang zu verschaffen, hilft die Zero Trust-Sicherheit, die Anwesenheit zu erkennen und den Schaden, der angerichtet werden kann, proaktiv zu begrenzen.

Verbessern Sie Ihre Fähigkeit, ein modernes Arbeitsproduktivitätsmodell anzupassen
Zero Trust eignet sich gut für hybride Arbeitsmodelle und bietet sicheren Zugang, unabhängig davon, wo und wie die Mitarbeitenden arbeiten. So wird verhindert, dass die Produktivität ins Stocken gerät, weil Mitarbeitende nicht auf Ressourcen zugreifen können, wenn sie an einem anderen Ort arbeiten oder das Gerät wechseln.

Vereinfachtes Sicherheitsmanagement
Zero Trust vereinfacht das Sicherheitsmanagement, indem es eine umfassende Lösung bietet, die Identität, Anwendungen, Geräte, Infrastruktur und Daten unter einheitlichen Sicherheits- und Governance-Richtlinien abdeckt. Durch den Einsatz von KI und die Automatisierung von Aufgaben wie der Überwachung von Bedrohungen und der Risikobewertung vereinfacht Zero Trust die Verwaltung noch weiter und entlastet IT-Teams, sodass diese Zeit haben, sich auf strategische Initiativen und Innovationen zu konzentrieren.

Die Teilnehmenden einer Foundry Zero Trust-Umfrage gaben an, dass die Implementierung eines Zero Trust-Modells Vorteile mit Auswirkungen auf die Produktivität, Risikominderung und Compliance mit sich bringt.[11]

Die wichtigsten von den Befragten genannten Vorteile:

- Kundendaten schützen
- Kontinuierlicher Zugriff und kontinuierliche Authentifizierung
- Verwaltung des Zugriffs auf Cloud-Apps und Geräte
- Erleichterung des Übergangs zur Remote-Arbeit
- Lösung des Mangels an Sicherheitsfachkräften
- Verringerung der Komplexität der Integration
- Verkürzung der Zeit bis zur Entdeckung einer Sicherheitsverletzung Sicherheit und eine hervorragende User Experience für Endbenutzer*innen

Schritt 2
Endpunktverwaltung optimieren

Nachdem Ihr Unternehmen eine Zero Trust-Sicherheitsgrundlage geschaffen hat, können Sie ein vereinfachtes Rahmenwerk einführen, das es IT-Administrator*innen ermöglicht, die Endpunktverwaltung zu optimieren.

Endgeräte umfassen eine Reihe von Geräten, die im täglichen Arbeitsablauf verwendet werden, darunter Desktop-Computer, Laptops, Tablets, Mobiltelefone, IoT-Geräte und Cloud-Lösungen. Die Anzahl von Endpunkten steigt von Jahr zu Jahr, sodass das durchschnittliche Unternehmen mittlerweile über etwa **135.000** Geräte verfügt.[12] Die Verwaltung und Sicherung all dieser verschiedenen Endgeräte ist eine große (und teure) Aufgabe, denn etwa 30 % der IT-Helpdesk-Kosten entfallen auf die Lösung von Endgeräteproblemen. Der Einsatz einer Cloud-basierten Produktivitätssuite wie Microsoft 365 E3 vereinfacht die Verwaltung von Endgeräten und senkt die IT-Kosten, auch wenn die Zahl der Endgeräte weiter steigt.

Was können Sie mit einer optimierten Endpunktverwaltung erreichen?

Verbessern Sie die Erfahrungen und die Produktivität Ihrer Mitarbeitenden. Bieten Sie Unterstützung für eine breite Palette von Anwendungen, Peripheriegeräten, Geräten und Selbstbedienungsoptionen, damit Mitarbeitende von überall aus effizient arbeiten können.

Verbessern Sie die Kontrolle über Leistung, Zustand und Sicherheit von Endgeräten. Aktualisieren Sie Ihre Geräte mit dem neuesten Betriebssystem und Sicherheitsrichtlinien auf der Grundlage von Identität, Standort, Compliance und Risikofaktoren.

Weniger IT-Komplexität. Steigern Sie die IT-Effizienz, indem Sie die Cloud nutzen, um die Bereitstellung, Konfiguration und Aktualisierung von Geräten und Anwendungen zu vereinfachen. Das Ergebnis ist eine umfassende Verwaltung und Sicherheit für Endgeräte über verschiedene Betriebssysteme, Gerätetypen und Eigentumsmodelle hinweg.

Sobald Sie die beiden Schritte zur Schaffung einer Zero Trust-Grundlage und zur Optimierung der Endpunktverwaltung abgeschlossen haben, rückt das nächste Ziel in den Fokus: ungehinderte Produktivität und Zusammenarbeit.

Microsoft 365 E3: Zero Trust-Sicherheit und einheitliche Endpunktverwaltung für eine leistungsstarke, produktive Belegschaft

In der Vergangenheit mussten Unternehmen ein sorgfältiges Gleichgewicht zwischen Sicherheit und Produktivität finden. Wenn die IT-Abteilung zu viele Sicherheitsvorkehrungen trifft, kann die Produktivität der Mitarbeitenden beeinträchtigt werden, da sie Schwierigkeiten haben, auf die erforderlichen Informationen und Ressourcen zuzugreifen. Andererseits könnte ein einziger erfolgreicher Cyberangriff den gesamten Betrieb zum Erliegen bringen, wenn zu wenig Schutzmaßnahmen ergriffen werden.

Microsoft 365 E3 ist eine Cloud-basierte Produktivitätslösung, die grundlegende Zero Trust-Sicherheit, Geräte- und App-Verwaltung auf Unternehmensebene sowie robuste Tools für die Zusammenarbeit bietet. Dank integrierter KI-Funktionen versteht sie den Kontext Ihrer Daten und Ihres Wissens, um die sichere Produktivität in Ihrem Unternehmen zu fördern, damit Ihre Mitarbeitenden auf jeder Ebene konzentriert, vernetzt und sicher arbeiten können.

Funktionen von Microsoft 365 E3

Identitäts- und Zugriffsverwaltung von einem zentralen Ort
Starke und anpassungsfähige Zugriffsrichtlinien, die es den Nutzer*innen ermöglichen, die benötigten Ressourcen zu erhalten, ohne auf Reibungspunkte zu stoßen

Informationsschutz und Governance
Sorgen Sie dafür, dass Ihre Daten verschlüsselt bleiben, egal ob sie sich im Ruhezustand, bei der Übertragung oder bei der Verwendung befinden, und machen Sie sensible Informationen leicht auffindbar.

Automatisierter Bedrohungsschutz
Automatisieren Sie Updates, um die Software auf dem neuesten Stand zu halten, stellen Sie Patches schnell bereit, um ausnutzbare Schwachstellen zu reduzieren, und verhindern Sie proaktiv, dass Bedrohungen die Geschäftskontinuität stören.

Produktivität steigern: Microsoft Copilot for Microsoft 365

Der Einsatz von KI erfordert eine Vielzahl von Daten, die aus verschiedenen Quellen stammen. Die Implementierung von Zero Trust-Sicherheit und nahtlosem Endpunktmanagement sind entscheidende Schritte, um sicherzustellen, dass all diese Daten sicher und einfach zu verwalten sind. Wenn Sie das geschafft haben, können Sie Ihre Produktivität mit Tools wie Microsoft Copilot noch weiter steigern.

Microsoft Copilot für Microsoft 365 ist ein KI-gestütztes Produktivitätstool, das durch die Automatisierung gängiger Aufgaben wie das Erstellen von Dokumenten, das Planen von Besprechungen und das Verwalten von Projekten stundenlange Arbeit erspart. Durch die frei gewordenen Stunden haben die Mitarbeitenden mehr Zeit und Energie für Aufgaben, die konzentrierte Kreativität und innovative Problemlösungen erfordern.

Mit KI Raum für Kreativität schaffen

70 %

der Befragten würden so viel Arbeit wie möglich an KI delegieren, um ihre Arbeitsbelastung zu verringern.[13]

Total Economic Impact

In einer von Forrester Consulting durchgeführten Auftragsstudie wurde nachgewiesen, dass Microsoft 365 E3 die Sicherheit erhöht, die Produktivität verbessert und die IT-Verwaltung vereinfacht.[14]

Starke Sicherheit

35 %

Verringerung der Wahrscheinlichkeit einer Datenschutzverletzung.

Produktivität

60 h

Sparen Sie mit Microsoft 365 E3 durchschnittlich 60 Stunden pro Jahr.

Vereinfachte IT

25 %

Verringerung des Zeitaufwands für die Bereitstellung und Verwaltung neuer Software um 25 %.

Unterstützen Sie Ihr Unternehmen mit sicherer Produktivität von Microsoft 365.

Weitere Informationen ›

[1] IT Trends Report: Remote Work Drives Priorities in 2021. JumpCloud, 2021.
[2] Grafik: Cyberkriminalität wird in den kommenden Jahren voraussichtlich sprunghaft ansteigen. Statista. 2022.
[3] Microsoft Security Copilot: How does it help you protect your data? Intelequia. April 2023.
[4] Microsoft Entra: 5 Identitätsprioritäten für 2023. Microsoft Security. Januar 2023.
[5] Statistiken und Trends zur Remote-Arbeit (2023). Forbes Advisor. 2023.
[6] Microsoft Digital Defense Report. 2023.
[7] Die Anatomie externer Angriffsflächen. Microsoft Security Insider. Mai 2023.
[8] Microsoft Security Signals Boost SDM Research Learnings. Hypothesis Group. September 2021.
[9] The State of Attack Surface Management 2022. Randori. 2022.
[10] Microsoft Digital Defense Report. 2022.
[11] Zero Trust Adoption Survey. Foundry. März 2022.
[12] Managing Risks and Costs at the Edge. Ponemon Institute. 2022.
[13] Jahresbericht des Work Trend Index: Wird KI die Arbeit erleichtern? Microsoft, Mai 2023.
[14] The Total Economic Impact Of Microsoft 365 E3. Eine bei Forrester Consulting in Auftrag gegebene Studie, Oktober 2022.