ivanti

# Der ultimative Leitfaden für Unified Endpoint Management

Wie sich moderne Endpoint-Management-Lösungen auf die Sicherheit und die Erfahrung der Mitarbeitenden auswirken

# Inhalt:



ivanti

01

# Der neue Standard für Endpoint Management nach der Pandemie

Vor fünf Jahren waren die Verwaltung und Sicherheit von Endgeräten noch vergleichsweise einfach.

In den meisten Unternehmen befanden sich die Endgeräte, die für die Arbeit im Unternehmen genutzt wurden, im Büro – eine Umgebung, die kontrolliert werden konnte und ein Ort, an dem die meisten Geräte hoffentlich leicht gefunden und von den IT- und Sicherheitsmitarbeitenden vor Ort verwaltet werden konnten.

Dann brachte die Coronapandemie das traditionelle Büroleben in den eigenen vier Wänden durcheinander.

Ausnahmen vom Standardansatz des „Walled Garden“ gab es sicherlich auch schon vor der Pandemie – Firmenlaptops und mobile Geräte wurden über verwaltete Wi-Fi-Netzwerke betrieben, bevor 2020 alle in eine permanente Remote-Position versetzt wurden!

Die sofortige Anweisung, zu Hause zu bleiben, um die Ausbreitung des Coronavirus einzudämmen, veranlasste IT- und Sicherheitsteams auf der ganzen Welt dazu, aus den vorhandenen Technologien und Geräten die bestmöglichen Arbeitsvorkehrungen zusammenzuschustern.

Ausnahmen von der Regel waren nun für alle die Regel.

Jetzt, da Corona als globale Bedrohung zurückgeht, ermutigen viele Arbeitgeber ihre Mitarbeitenden dazu, ins Büro und zum früheren technologischen Status quo zurückzukehren. Untersuchungen von Ivanti haben ergeben, dass nur 13 % der Wissensarbeiter es vorziehen, ausschließlich im Büro zu arbeiten, während 56 % der Führungskräfte der Meinung sind, dass die Mitarbeitenden im Büro sein müssen, um produktiv zu sein. (Ivanti)

Diese Diskrepanz zwischen den Wünschen der Mitarbeitenden und dem Gefühl ihrer Manager, wo ihre Mitarbeiter effektiv arbeiten würden, hat die IT- und Sicherheitsabteilung in eine äußerst unangenehme – und offen gesagt unhaltbare – Lage gebracht.

Diese Spannung wird noch verstärkt, wenn eine vollständige Rückkehr zum Vor-Ort-Management und den „Walled Garden“-Netzwerken von 2019 sowohl unwahrscheinlich als auch unklug erscheint:

> Zwei Drittel aller Mitarbeitenden würden lieber kündigen, als für eine ganze Arbeitswoche ins Büro zurückzukehren, so eine Umfrage der globalen Stellenausschreibungsseite Monster.com aus dem Jahr 2022 – und 40 % aller Befragten gaben an, dass sie kündigen würden, wenn sie gezwungen wären, regelmäßig für nur einen von fünf Arbeitstagen in einer Arbeitswoche zurückzukehren. (Shumway)

> In einem Ultimatum vom November 2022 forderte Twitter-CEO Elon Musk die Mitarbeitenden auf, entweder für 40 Stunden pro Woche in ihr lokales Büro zurückzukehren oder zu kündigen. (Yang) Hunderte von Arbeitern durchschauten seinen Bluff und kündigten. (Bond) Bis Anfang Januar 2023 schrumpfte die Zahl der Vollzeitmitarbeiter von Twitter von etwa 7.500 Mitarbeitenden um über 80 % auf etwa 1.300 – mit weniger als 550 Vollzeit-Entwicklern. (Kolodny)

> Als Amazon-CEO Andy Jassy seinen Mitarbeitenden befahl, im Februar 2023 in Vollzeit ins Büro zurückzukehren, wehrten sie sich. Schließlich lenkte er ein und erklärte, dass sie nur drei Tage pro Woche im Büro sein müssen. (Palmer)

Für diejenigen, die glauben, dass die Rückkehr zur Büroarbeit die Produktivität verbessert, sagt die Forschung etwas anderes:

- Während der Pandemie verzeichnete Gallup mit 40 % das höchste Engagement der Mitarbeitenden aller Zeiten; seitdem ist es auf weniger als ein Drittel gesunken. (Smith)
- In der ersten Jahreshälfte 2022 ist ein Rekordeinbruch bei der Produktivität zu verzeichnen, der mit dem zunehmenden Druck der Unternehmen korreliert, von allen Mitarbeitenden zu verlangen, dass sie in Vollzeit ins Büro zurückkehren. (Tsipursky)

Diese Trends zeigen uns, dass, selbst wenn die Unternehmen sehen, dass ihre Mitarbeitenden die Anordnungen zur Rückkehr ins Büro einhalten, sie möglicherweise einfach stillschweigend kündigen: Sie tun das Nötigste, während sie nach neuen Möglichkeiten suchen, die ihnen die flexiblen Arbeitsregelungen ermöglichen, die sie während des Pandemie-Notfalls am attraktivsten fanden. (Tsipursky)

Die offensichtliche Lösung? Mitarbeitende zu ermutigen, weiterhin remote, vor Ort oder in einer Kombination zu arbeiten, die für jeden einzelnen Nutzer am besten geeignet ist, wann immer dies möglich ist.

Tatsächlich geben Mitarbeitende, die in einer hybriden oder Remote-Umgebung arbeiten, an, 21,8 % produktiver, 20,7 % zufriedener und 50,8 % engagierter zu sein, wie eine Umfrage des Integrated Benefits Institute aus dem Jahr 2022 ergab. (Bonner)

Natürlich stellt diese neue Anforderung sowohl die IT- als auch die Sicherheitsteams vor neue Schwierigkeiten – und genau hier können einheitliche Endpunktverwaltungslösungen helfen.

Denn selbst wenn Ihr Unternehmen der Meinung ist, dass es sich um eine reine Vor-Ort-Arbeitsumgebung handelt, in der es keinerlei Überlegungen zur Remote-Arbeit gibt – oder auf dieses Ziel hinarbeiten möchte –, weiß Ihr Team, dass eine hunderprozentige Einrichtung für die Arbeit im Büro und für die Sicherheit nicht ausreicht; man muss gewisse „Ausnahmen“ von der Anwesenheits-Regel berücksichtigen, wie wir in diesem Leitfaden erläutern.

**Mitarbeitende, die in einer hybriden oder Remote-Umgebung arbeiten, sind:**

- **50,80 %** mit ihrem Arbeitgeber stärker verbunden
- **21,80 %** produktiver
- **20,70 %** zufriedener in ihren Rollen

# Hybrid- und Remote-„Ausnahmen“ von Ihrer In-Office-Regel

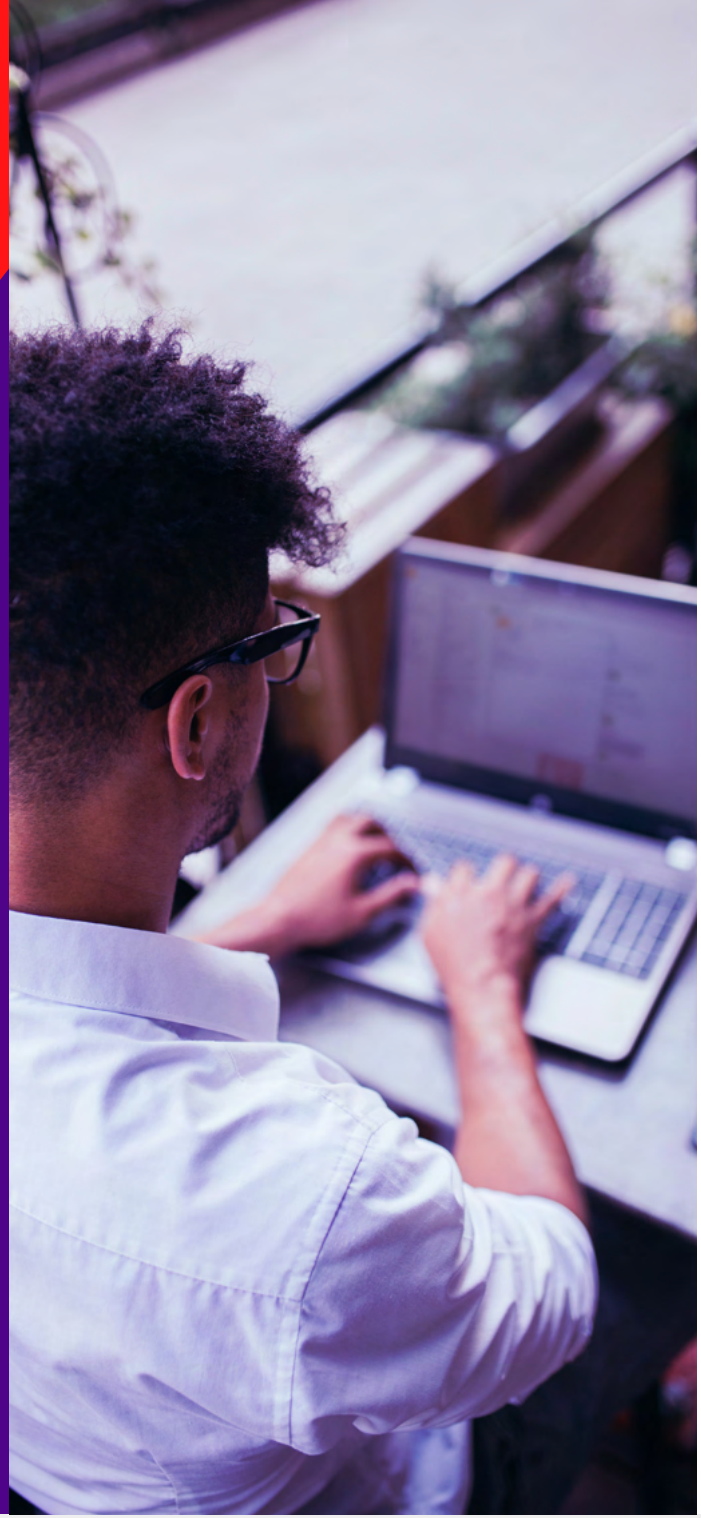
Ihr Unternehmen betrachtet sich vielleicht als vollständig im Büro anwesend – und benötigt daher nur die traditionellen Endpunktverwaltungs- und Sicherheitslösungen, die vor der Pandemie beliebt waren. Aber wird wirklich 100 % vor Ort gearbeitet?

Nein, natürlich nicht!

IT- und Sicherheitsteams müssen alle Abweichungen von den Standardverfahren berücksichtigen. Das macht eine hybride Strategie für Technologiemanagement und Sicherheit robuster als die Annahme des Managements, dass die einzigen Arbeitsumgebungen, die gesichert und verwaltet werden müssen, in den Büros liegen.

Zum Beispiel würden hybride IT-Management- und Sicherheitsstrategien diese „Ausnahmen“ von reinen Bürolösungen abdecken:

- **Bereitschaftsdienste im Gesundheitswesen** für das Wochenende, die auf Patientenakten zugreifen müssen, um auf einen Anruf zu reagieren.
- **Lehrkräfte** die zu Hause Arbeiten benoten oder nach Feierabend die E-Mails der Eltern beantworten.
- **Finanzberater**, die nur auf einem sicheren Server auf ihre E-Mails zugreifen können sollten … aber möglicherweise eine App installiert haben, mit der sie auf ihren persönlichen Geräten darauf zugreifen können.
- **Eltern,** die versuchen, von zu Hause aus zu arbeiten, während sie sich um ein krankes Kind kümmern.
- **Mitarbeitende von Behörden** die an Konferenzen teilnehmen oder auf Reisen sind, um Vorfälle zu beheben, aber dennoch von zu Hause aus Zugriff auf die Netzwerke der Behörde benötigen.
- **Führungskräfte,** die aus Bequemlichkeit aufgrund ihres Dienstalters Ausnahmen beantragen.
- **Mitarbeitende im Außendienst.**



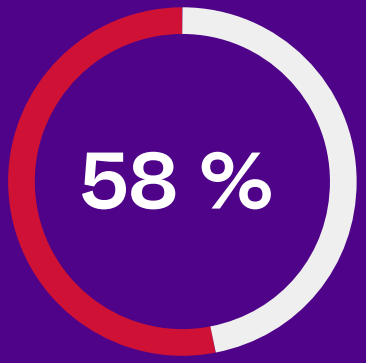
Selbst wenn ein Arbeitsplatz angeblich „zum Büro zurückgekehrt“ ist, werden diese Endbenutzer und andere wie sie den Fernzugriff auf Arbeitsdaten und Anwendungen von mobilen Geräten über jedes Netzwerk erwarten, das sie erreichen können.

Daher müssen IT- und Sicherheitsteams Strategien entwickeln, die es den Mitarbeitenden ermöglichen, sowohl im Büro als auch außerhalb erfolgreich zu sein, d.h. Geräte und Netzwerke effektiv zu verwalten. Es bedeutet, dass alle Endgeräte und deren Benutzer an jedem Ort und in jedem Netzwerk gesichert werden müssen – für alle Unternehmensdaten.

Aber diese neue Anforderung, Endgeräte in einem de facto hybriden Arbeitsplatz zu verwalten und zu sichern – unabhängig vom offiziellen Status der Rückkehr an den Arbeitsplatz – bedeutet nicht, dass Unternehmen gezwungen sind, sich auf die gleichen panischen Pandemie-Strategien für die Geräteverwaltung zu verlassen, die sie vor einigen Jahren angewendet haben.

Diese Notlösungen haben eine Zeit lang funktioniert, sind aber für die langfristige Verwaltung von Endgeräten und den Schutz vor modernen Risiken und Sicherheitslücken unzureichend. Damit steigt der Bedarf der Unternehmen an einer wirklich einheitlichen Lösung für die Endgeräteverwaltung.

Tatsächlich geben 58 % der CISOs an, dass ihre Unternehmen seit der Umstellung auf Remote-Arbeit mehr Cyberangriffe erlebt haben. (Proofpoint)




**der CISOs geben an, dass ihre Unternehmen mehr Cyberangriffe erlebt haben, seit sie ihren Mitarbeitenden erlauben, von zu Hause aus zu arbeiten**

ivanti

# Was ist Unified Endpoint Management?

Unified Endpoint Management (UEM) ist eine Technologie, die IT- und Sicherheitsteams in die Lage versetzt, mehrere Endpunkte – d.h. Geräte, Hardware und andere Technologien – von einer einzigen Plattform oder einem Dashboard aus zu finden, zu verwalten und abzusichern. Dabei wird eine Vielzahl von Betriebssystemen (OS) und Gerätetypen von verschiedenen Herstellern und Entwicklern abgedeckt.

Im Kern ist UEM die jüngste Weiterentwicklung von Endpoint-Management-Lösungen, die wiederum aus den ersten MDM-Technologien (Mobile Device Management) hervorgegangen sind.

- **Mobile device management (MDM) –** heute oft in „modernes“ Gerätemanagement oder Device Management umbenannt – war der erste Versuch der Technologiebranche, die Probleme bei der Verwaltung, Durchsetzung und Sicherheit der ständig wachsenden Geräteflotten anzugehen. Diese Lösungen ermöglichten es der IT-Abteilung, Richtlinien, Konfigurationen und Software auf Smartphones, Tablets und anderen Endgeräten, die MDM-APIs unterstützen, zu kontrollieren, zu sichern und durchzusetzen, waren aber häufig auf Geräte mit bestimmten Betriebssystemen beschränkt.

- **Enterprise mobile management (EMM)** übernahm die MDM-Technologie und verschmolz sie mit Lösungen zur Verwaltung von Softwareanwendungen wie Mobile App Management (MAM), Mobile Content Management (MCM) und Mobile Information Management (MIM), um den Lebenszyklus der Software auf dem Gerät, die Daten auf bestimmten Apps und den Zugriff auf Unternehmensdaten zu verwalten.

Der kombinierte Endpunktverwaltungsansatz war jedoch immer noch nicht robust genug, um die traditionellen PCs, Server und andere wichtige Unternehmensendpunkte sowie viele der zunehmenden Edge-Use-Fälle in modernen Unternehmensumgebungen zu berücksichtigen – einschließlich IoT-Geräte und „robustere“ oder spezialisierte Geräte, die in bestimmten, aber häufigen Arbeitssituationen eingesetzt werden.

IT-Teams in größeren Unternehmen fanden sich in einem Flickenteppich wieder, um mehrere Betriebssysteme zu verwalten: macOS, Windows, iOS und Android, aber auch ChromeOS, Linux und andere spezialisierte oder IoT-fähige Geräte.

Obwohl jeder Betriebssystemhersteller Befehle und Konfigurationen über sein natives MDM unterstützt, gibt es einige wichtige Aufgaben, die nicht in den MDM-APIs enthalten sind:

- Gerätestatus (Jailbreak, Root-Erkennung)
- Standort
- Benachrichtigungen
- Mobile Bedrohungsabwehr

So entstand die Technologie für die einheitliche Endpunktverwaltung aus dem Bedürfnis von Unternehmen, zusätzliche Funktionen und Anwendungskontrollen bereitzustellen und diese gleichzeitig auf mehrere Betriebssysteme und Gerätetypen für die mobile und traditionelle Endpunktverwaltung auszuweiten.

03

# 4 Unternehmensvorteile einer modernen UEM-Lösung

In diesem Abschnitt erfahren Sie, wie UEM:

1. Tech-Stacks konsolidiert.

2. Automatisch unbekannte Assets entdeckt.

3. Die Compliance der Benutzenden verbessert.

4. Die digitale Erfahrung der Mitarbeitenden (DEX) verbessert.

ivanti

# Der UEM-Unterschied

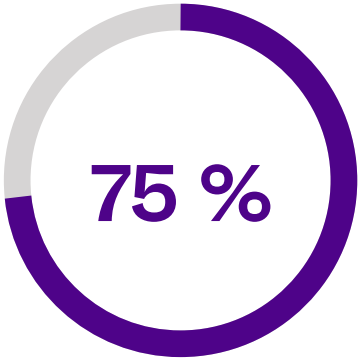
Die meisten Unternehmen verfügen bereits über mindestens eine Lösung, um den Großteil ihrer eigenen und verwalteten Geräte zu verwalten.

Eine Umfrage aus dem Jahr 2022 unter IT-Fachleuten ergab, dass 80 % der Befragten bereits zu einem einzigen Endpunktverwaltungsteam konsolidiert hatten oder dies innerhalb der nächsten zwei Jahre planten. Und 75 % der Befragten haben in irgendeine Art von BYOD-Technologie (Bring your own device) investiert. (Cipolla, Wilson und Silva)

Anstatt in Silos auf Geräteebene zu existieren, machen UEM-Lösungen besseren Gebrauch von modernen KI- und ML-Fähigkeiten, da diese Tools die gleiche Basis an unternehmensweiten Informationen nutzen, um Schlussfolgerungen zu ziehen, anstatt sich auf isolierte Informationsströme von separaten Tools zu verlassen.

## Zu den Vorteilen einer modernen UEM-Lösung gehören:

1. **„Single pane of glass"-Dashboards oder -Portale**, die den ohnehin dünn besetzten IT- und Sicherheitsteams eine konsolidierte Lösung anstelle mehrerer Nischenprodukte bieten.
2. **Automatische Identifizierung und Behebung unbekannter Geräte und sogenannter** „Schatten-IT" durch dynamische, automatische Asset-Erkennung – sowohl vor Ort als auch über die Cloud.
3. **Bessere Einhaltung aller IT- und Sicherheitsrichtlinien** durch einheitliche Geräteanmeldung und -durchsetzung durch die Endbenutzer.
4. **Verbessertes digitales Mitarbeitererlebnis (DEX)** mit automatischer und proaktiver Behebung von Geräteproblemen, um IT-Teams bei der Linksverschiebung zu unterstützen.




der IT-Fachleute geben an, dass ihr Unternehmen in die BYOD-Fähigkeit investiert hat.

# 1 Ein einheitlicher Ansatz konsolidiert schwerfällige Technologie-Stacks.

Angesichts der zunehmenden wirtschaftlichen Unsicherheit fordern Investoren und Vorstandsetagen weltweit, dass ihre Unternehmen den strategischen Output mit weniger Ressourceninvestitionen optimieren, die Effizienz maximieren und jedes Tool, jeden Mitarbeitenden und jede Zeitspanne optimal ausnutzen.

Im Rahmen dieses Mandats gehen immer mehr Unternehmen dazu über, allgemeinere und integrierte Technologielösungen zu kaufen, anstatt nach Einzellösungen zu suchen, die mehr Personal und Spezialwissen erfordern, als ihre IT- und Sicherheitsteams zuverlässig unterstützen können.

Diese strategische Verlagerung hin zur Konsolidierung des Tech-Stacks ist sinnvoll, insbesondere wenn Unternehmen die weltweiten Trends bei Burnout und technologischen Arbeitskräften berücksichtigen:

- 64,4 % der befragten Mitarbeitenden von IT-Dienstleistungen berichteten in einer weltweiten Umfrage 2019 über Burnout – eine der höchsten Raten aller Branchen. Auch die allgemein im Technologiesektor tätigen Mitarbeitenden berichteten mit einer Quote von 60 % über ein erhöhtes Burnout-Niveau. (Paychex)
- 68 % der befragten Einsatzkräfte geben an, dass sie in der Regel zwei oder mehr Vorfälle auf einmal zu bewältigen haben, wobei jeder Vorfall durchschnittlich zwei bis vier Wochen in Anspruch nimmt. 64 % dieser Einsatzkräfte haben auch schon medizinische Hilfe in Anspruch genommen, um Burnout und Angstzustände zu behandeln. (Morning Consult und IBM)
- Das größte Hindernis auf dem Weg zu exzellenter Cybersicherheit für Unternehmen auf der ganzen Welt ist die „Komplexität des Tech-Stacks“, gefolgt von einer „Qualifikationslücke“ bei den derzeitigen Mitarbeitenden im Bereich IT-Sicherheit. Dies ergab eine globale Umfrage unter Sicherheitsexperten im Jahr 2022. (Ivanti)

Wie ein CISO dem Wall Street Journal sagte:

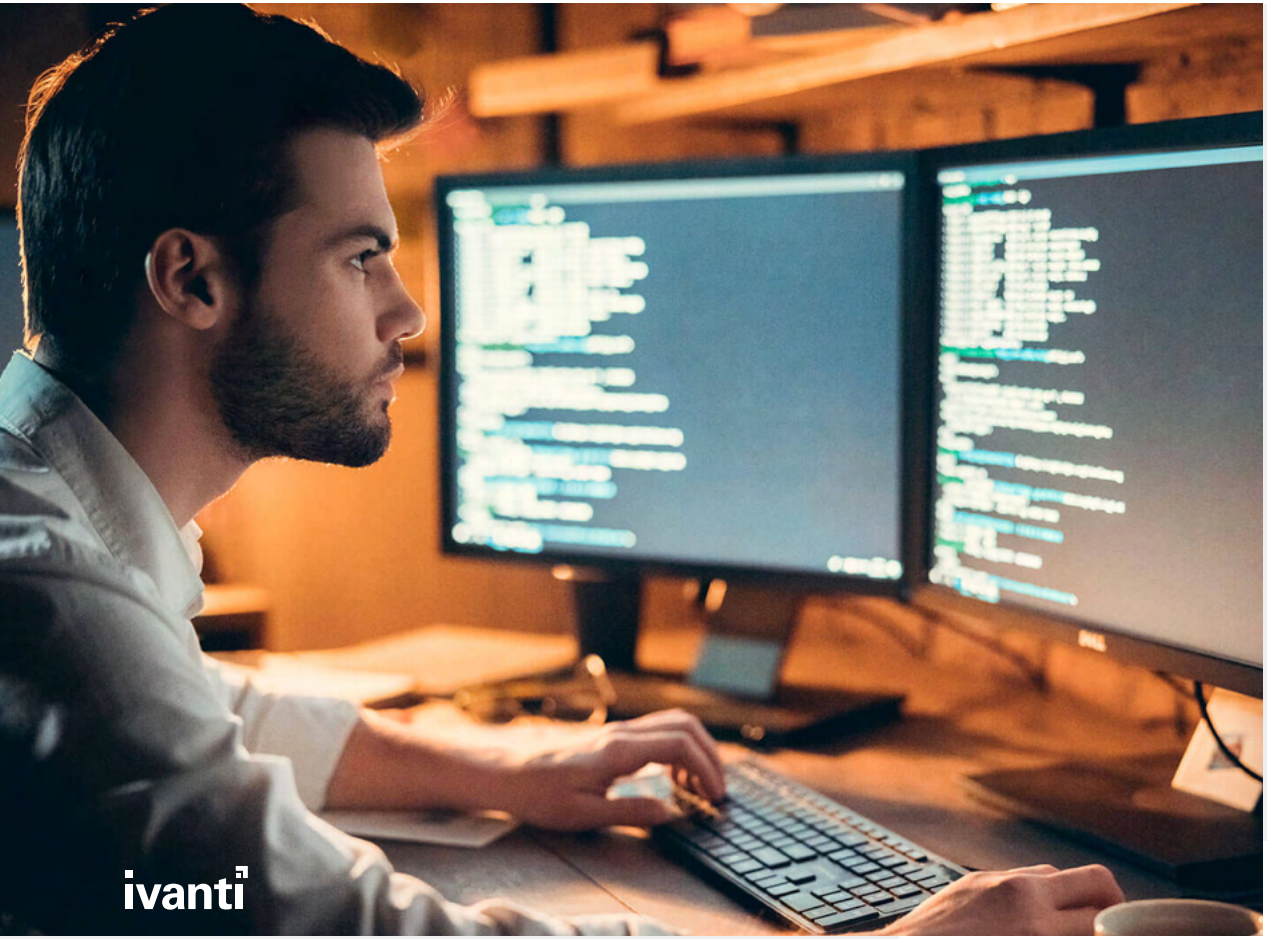
„Wenn ich eine Lösung bekomme, die nur fünf oder sechs Dinge ziemlich gut, aber vielleicht nicht exzellent macht, dann nehme ich diese Lösung gerne. Sie ist einfacher zu verwalten, sie ist günstiger für das Budget, und ich bekomme mehr für mein Geld.”

**Adam Glick**
CISO at SimpliSafe, Inc. (Rundle)

Einfach ausgedrückt? Es gibt einfach zu wenige Mitarbeiter, die über die erforderlichen Fähigkeiten verfügen, um jedes Gerät, jede Anwendung und jeden Vorfall zu verwalten, der in den Einzellösungen auftritt.

Richtig konfiguriert und implementiert, bieten moderne UEM-Plattformen sowohl IT- als auch Sicherheitsteams den bestmöglichen Überblick über die gesamte Endpunktumgebung ihres Unternehmens und liefern dynamisch Berichte über Folgendes:

- Nutzung und Verwaltung von Geräten auf Abteilungs- und Benutzerebene.
- Zugriff und Aktivitäten einzelner Benutzer, um die Gesamtproduktivität und mögliche Sicherheitsbedenken zu bewerten.
- Der Sicherheitsstatus eines Endpunkts, einschließlich aktuell installierter Patches und Anwendungsfälle.
- Die Gesamtkosten eines Geräts für den Betrieb unter Berücksichtigung der historischen Wartungs- und Lizenzkosten.




Jeder dieser Punkte kann durch Einzellösungen für einen bestimmten Gerätetyp oder ein bestimmtes Betriebssystem berücksichtigt werden, mit noch größerer Granularität und Detailgenauigkeit für die optimalsten Prozesse.

Doch nur eine moderne UEM-Lösung kann diese miteinander verbundenen, aber dennoch unterschiedlichen Anforderungen in einem einzigen, leicht zu verwaltenden Dashboard vereinen, das überlastete IT- und Sicherheitsteams in ihren persönlichen Arbeitsabläufen nutzen können.

# 2 Die automatische Erkennung von Assets findet versteckte Kosten mit minimalem Arbeitsaufwand.

Genauso wie die Verwendung mehrerer Technologielösungen zur Verwaltung von Endgeräten die Gesamtkosten erhöht, kann eine unzureichende Asset-Erkennung zu einem höheren Aufwand und höheren Kosten für Unternehmen führen – Kosten, die letztlich das IT-Team trägt, unabhängig davon, wo die Lecks auftreten.

IT-Teams sind sich zunehmend der Gefahr früherer, unentdeckter (und daher nicht verwalteter) Hardware und Software bewusst, die gemeinhin als Schatten-IT bezeichnet wird:

- 36 % der IT-Profis geben an, dass Schatten-IT-Probleme eine große Herausforderung für die Modernisierung ihrer IT-Infrastruktur darstellen. (Insight Enterprises & CIO)
- Schatten-IT ist nach Ransomware-Angriffen und Angriffen auf die Lieferkette eine der größten Sorgen, die von den befragten CIOs für die Kontinuität der Organisation genannt wurden. (NASCIO)
- 41 % der befragten IT-Entscheider sagen, dass „dezentrale“ IT und Schatten-IT einer der größten Trends ist, der sich in naher Zukunft auf globale Unternehmen auswirken wird. (Vanson Bourne für Nutanix)

Warum sind die Überlegungen zur Schatten-IT in den Fokus der IT-Abteilungen gerückt? Mehr hybride Arbeitsplätze und BYOD-Richtlinien (Bring your own device) bringen mehr Geräte und Anwendungen mit sich, die von Endbenutzern verwendet werden, aber nicht unbedingt direkt im Besitz des IT-Teams sind oder von ihm verwaltet werden.

Laut einer Umfrage unter IT-Entscheidungsträgern (Bitwarden) sagen ihre Endbenutzer, dass sie Schatten-IT aus folgenden Gründen nutzen:

1. Ihre tägliche Arbeit ist mit den Schatten-IT-Optionen ihrer Wahl schneller oder einfacher als mit den vom Unternehmen bereitgestellten Ressourcen (63 %).
2. Sie haben nicht die richtigen internen Berechtigungen, um Geräte oder Apps zu nutzen, die sie für ihre Aufgaben zu benötigen glauben (48 %).
3. Die IT-Abteilung ist zu langsam bei der Beantwortung ihrer Anfragen für den Zugriff auf Apps oder Geräte oder zu kompliziert, um sich damit zu befassen (38 %).

## Auswirkungen in der Praxis

### Einsparungen bei Technik und Lizenzkonsolidierung mit UEM

Laut einer von Forrester Consulting im Auftrag von Ivanti durchgeführten Total Economic ImpactTM -Studie erzielte ein Unternehmen, das 10.000 Endpunkte verwaltet und jährlich um 5 % wächst, durch die Implementierung von Ivanti Neurons for UEM innerhalb von drei Jahren einen ROI von 261 %.

36 % des in der TEI-Studie geschätzten Nutzens für das gemischte Unternehmen ergab sich aus der Abschaffung einzelner Endpunktverwaltungslösungen und der Reduzierung der Ausgaben für Softwarelizenzen von nicht genutzten Anwendungen. (Forrester Consulting TEI-Studie)

Für weitere Informationen lesen Sie bitte den Total Economic ImpactTM von Ivanti Unified Endpoint Management (UEM) Lösungen.

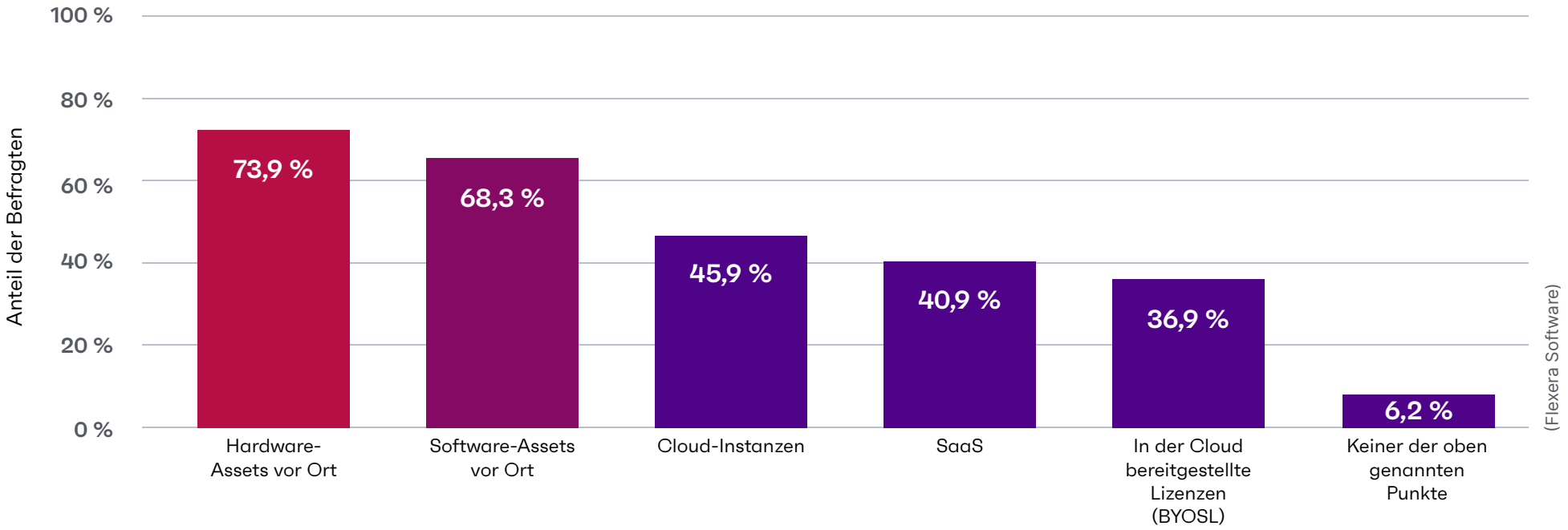
Um diesem Schatten-IT-Problem noch mehr Nahrung zu geben, haben IT-Teams die Asset-Transparenz für herkömmliche On-Premises-Implementierungen besser im Griff als für Remote- oder Cloud-basierte Assets. (Flexera Software)

Diese weltweiten Umfragen und Studien decken sich mit den anekdotischen Erfahrungen von Ivanti mit Kunden, die nach der Einführung einer UEM-Lösung mit aktiver Asset-Erkennung in der Regel 25-30 % bisher unbekannte Geräte im Unternehmensnetzwerk finden.

Die automatische Erkennung von Assets über eine zentralisierte UEM-Plattform ermöglicht es IT-Teams:

- Alle Geräte zu erkennen, wenn sie sich mit der Infrastruktur und den Netzwerken des Unternehmens verbinden.
- Das Risiko zu verringern, dass vorübergehend genutzte Geräte ohne Abhilfe oder Segmentierung online sind.
- Geräte aus der Ferne zu scannen, ohne dass ein Mitarbeiter benötigt wird.
- Potenziell gefährliche, unbekannte Geräte zu segmentieren und unter Quarantäne zu stellen und gleichzeitig die Flexibilität einer BYOD-Richtlinie zu gewährleisten.

Q: Haben Sie das Gefühl, dass Sie einen genauen Überblick über die folgenden Umgebungen haben?



# 3 Die automatische Registrierung von Geräten beschleunigt das Onboarding und die Konformität der Endbenutzer.

Zu einer de facto hybriden Arbeitsstrategie gehört es, die Einarbeitung neuer Mitarbeiter zu berücksichtigen – einschließlich der Bereitstellung neuer Geräte mit der entsprechenden Software und Zugriffsberechtigungen für Endbenutzer, die möglicherweise nie einen Fuß ins Büro setzen!

UEM-Lösungen bieten vorkonfigurierte Benutzer- und Geräteprofile, so dass die Bereitstellung so einfach ist, wie wenn der Personalverantwortliche ein Self-Service-Portal für Anforderungen und Berechtigungen aufruft, ohne dass sich das IT-Team unnötig einmischen muss.

Mit der automatischen Registrierung von Endgeräten können neue Geräte und Benutzerprofile mit minimaler Unterbrechung der regulären Aufgaben des IT-Personals oder der normalen Arbeitsabläufe der Mitarbeitenden registriert werden.

Automatisch durchgesetzte Richtlinien und Gerätekonfigurationen von der primären UEM-Lösung sorgen außerdem für eine durchgängige Einhaltung der Richtlinien.

Und schließlich sind Unternehmen durch den Einsatz einer UEM-Lösung nicht mehr darauf angewiesen, dass sich die Endbenutzer für benötigte Updates oder Sicherheitsanwendungen entscheiden. Die von UEM verwalteten Geräte melden sich automatisch für den jeweiligen Aktualisierungsplan oder die Anwendungsinstallation an – keine Benutzerinteraktionen oder Berechtigungen erforderlich!

## Auswirkungen in der Praxis

### Statt 2-3 Tagen oder mehr nur noch 5-10 Minuten für die Installation und Konfiguration der Software

In Interviews für eine von Forrester Consulting im Auftrag von Ivanti durchgeführte TEI-Studie schätzte ein Integrationsentwickler eines Schuhhändlers, dass sein Team früher zwei bis drei Tage pro Gerät mit der Installation und Konfiguration von Software verbrachte. (Forrester Consulting TEI-Studie)

Nach der Implementierung von Ivanti Neurons for UEM erklärte der Befragte jedoch: „Sobald das Gerät abgebildet ist, installieren sie einfach Ivanti und ziehen das Gerät in alle Softwareaufgaben. Das ist in fünf bis zehn Minuten erledigt, und am Ende des Tages wird nur noch überprüft, ob alle Anwendungen vorhanden sind. Das spart definitiv Zeit beim Onboarding-Prozess.“ (Forrester Consulting TEI-Studie)

FORRESTER®

# 4 Endbenutzer berichten von besseren digitalen Erfahrungen und erhöhter Produktivität.

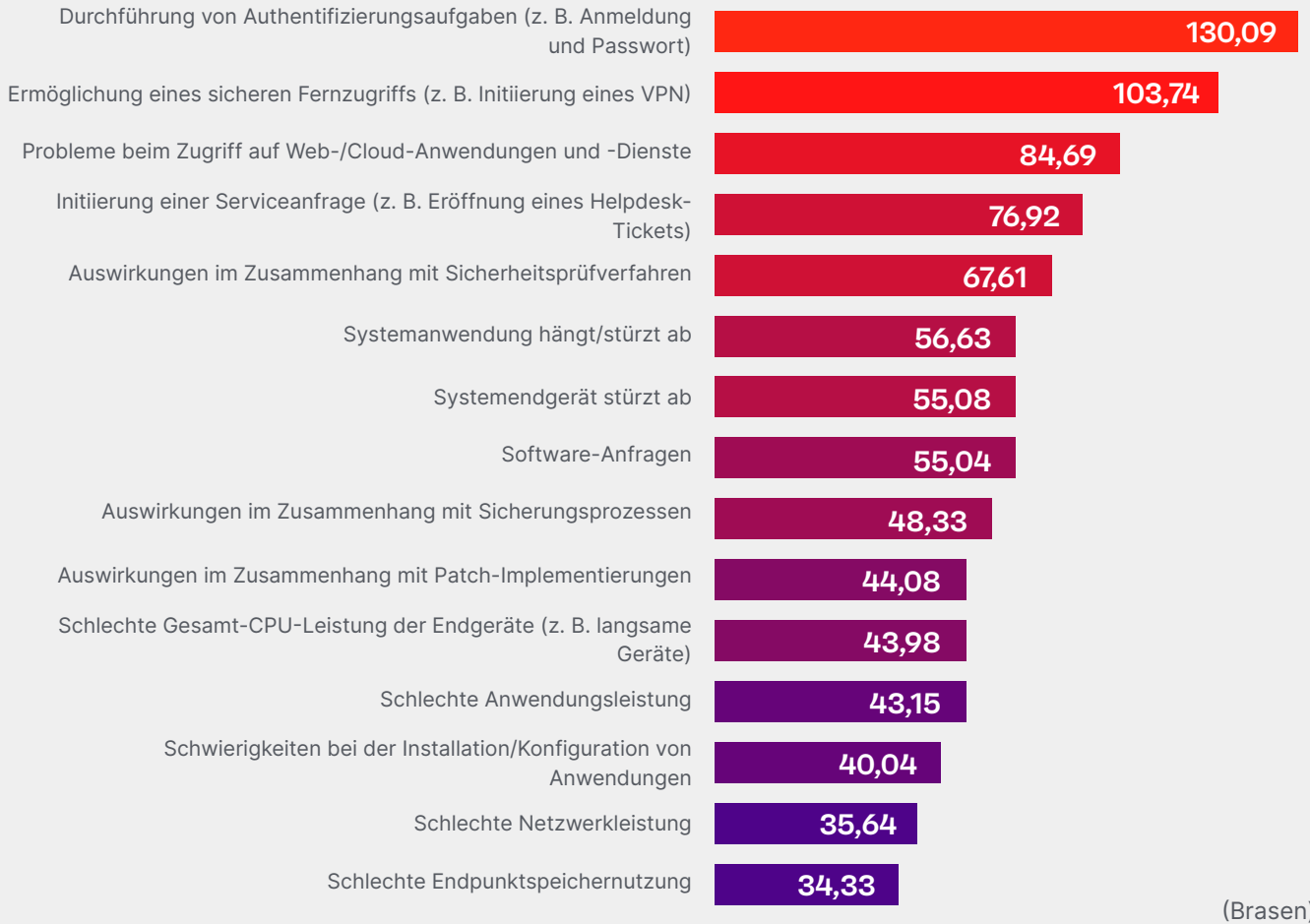
Jedes IT- und Sicherheitsteam wird dieser einfachen Tatsache zustimmen: Die digitale Erfahrung der Mitarbeiter (DEX) ist wichtig.

Jüngste DEX-Forschungen bestätigen diese fast instinktive Wahrheit:

- 26 % der befragten Mitarbeitenden – und 31 % der IT- und Sicherheitsexperten – haben zumindest teilweise in Erwägung gezogen, ihren Job wegen Schwierigkeiten mit der Technologie aufzugeben. (Ivanti)
- Ein durchschnittlicher Mitarbeiter ist jedes Jahr mit 919 Problemen bei der Endpunktverwaltung konfrontiert, was fast vier Problemen pro Arbeitstag entspricht. (Brasen)
- Ein Benutzer benötigt bis zu 20 Minuten, um jede Unterbrechung zu überwinden, die durch schlechtes Endpunktmanagement und technische Probleme verursacht wird. (Brasen)

DEX ist sogar so wichtig, dass die Analysten von Gartner vorhersagen, dass bis 2025 50 % der IT-Organisationen eine DEX-Strategie, ein DEX-Team und ein begleitendes Management einrichten werden – im Jahr 2022 waren es nur 15 %. (Wilson, Cipolla und Paulman)

**Durchschnittliche Anzahl von digitalen Problemen pro Jahr, die jeder Nutzer laut den befragten Unternehmen hat**




(Brasen)

Natürlich ist die Umsetzung einer geeigneten DEX-Strategie in fast jeder Situation eine Herausforderung. Besonders schwierig wird es jedoch, wenn nur 20 % der befragten C-Suite-Führungskräfte aktiv planen, im kommenden Jahr Budgets für die Verbesserung der Erfahrungen ihrer Mitarbeitenden einzusetzen. (Ivanti)

UEM-Lösungen können IT-Teams jedoch einen schnellen Überblick über das Gerät und die Benutzeraktivitäten verschaffen. So können vielbeschäftigte Techniker Probleme auf einen Blick beurteilen oder tiefer in robuste Analysen eintauchen, um die Ursache von Benutzerfrustrationen zu ermitteln und schneller zu reparieren.

Moderne UEM-Lösungen – mit benutzerdefinierten Geräte- und Benutzeraktivitätswarnungen sowie vorprogrammierten Service-Level-Vereinbarungen und Playbooks – können sogar viele dieser mangelhaften Endpunktmanagement-Technologien automatisch erkennen und proaktiv reparieren.

Auf diese Weise stellen ordnungsgemäß konfigurierte und robuste UEM-Lösungen eine der grundlegendsten und wichtigsten Komponenten einer robusten DEX-Strategie dar. Sie helfen IT-Teams dabei, ihr Service-Management nach links zu verlagern, indem sie Geräteprobleme beheben, bevor ihre Benutzer ein Ticket zur Unterstützung einreichen.

Überall können IT- und Sicherheitsteams durch proaktive Technologieplattformen wie UEM-Lösungen wertvolle Zeit und Geld sparen – auch wenn die Führungsetagen die Bedeutung von DEX-Investitionen erst noch begreifen müssen.


**Nur 20 % der Führungskräfte planen, spezifische Budgets für die Verbesserung der Mitarbeitererfahrung bereitzustellen.**

ivanti

04

# 4 Anwendungsfälle für Endgerätesicherheit mit UEM-Lösungen

In diesem Abschnitt erfahren Sie, wie Ihre UEM-Lösung Ihr Sicherheitsteam bei Folgendem unterstützt:

1. Anreize für gutes Sicherheitsverhalten.

2. Sicherung einer wachsenden hybriden Arbeitsumgebung.

3. Automatische Durchsetzung von Richtlinien.

4. Einfache Integration mit Patching oder Lösungen zur Abwehr mobiler Bedrohungen.

# Warum UEM-Benutzer auch die Endpunktsicherheit berücksichtigen müssen

Vielleicht haben Sie bemerkt, dass wir in diesem Leitfaden häufig sowohl auf die IT- als auch auf die Sicherheitsteams verweisen - und das ist kein Zufall.

Unabhängige Analysten sind der Meinung, dass – in Anbetracht der Tatsache, dass das Arbeiten von jedem Ort nach der Pandemie mehr Remote- und hybride Ansätze umfasst und nicht nur Büroarbeit vor Ort – UEM-Lösungen mehr Anwendungsfälle für die Endpunktsicherheit für eine „proaktive und widerstandsfähige Verteidigung“ gegen moderne Angreifer einbeziehen werden. (Cipolla, Wilson und Silva)

Es ist daher keine Überraschung, dass die Sicherheit von Endgeräten für Unternehmen weltweit nach wie vor eine der wichtigsten Investitionsprioritäten im Bereich der Cybersicherheit ist – nur noch übertroffen von Cloud-Sicherheitstools und internen Benutzerschulungen. (PwC)

(Und wenn die vorgeschlagene UEM-Lösung dazu beitragen könnte, Cloud-Anwendungen zu sichern, dann wäre das ein Bonus für alle Beteiligten!)

UEM-Lösungen bieten einen einzigartigen Ausgangspunkt für IT- und Sicherheitsteams, um mit denselben Basisinformationen – den Geräten, Benutzerprofilen und Netzwerkaktivitäten ihres Unternehmens – zu arbeiten und alle Endgeräte ordnungsgemäß zu verwalten, abzusichern und zu warten.

1. **Investitionen in ein DEX-fokussiertes Technologiepaket**, um Anreize für ein gutes Sicherheitsverhalten der Endbenutzer zu schaffen.

2. **Um die schnell wachsende Angriffsfläche eines Unternehmens zu sichern**, müssen Sicherheitsteams eine größere Vielfalt an Bedrohungsvektoren als je zuvor angehen, von IoT-Geräten bis hin zu unbekannten Internetverbindungen.

3. **Durchgesetzte Sicherheitsrichtlinien und überwachtes Benutzer-, Geräte- und App-Verhalten** können seitliche Bewegungen im Unternehmensnetzwerk von einem kompromittierten Endpunkt aus verhindern und erste Eindringlinge oder potenzielle Insiderbedrohungen melden, bevor Schaden entsteht.

4. **Sicherheitstools wie Patch Management oder Lösungen zur Abwehr mobiler Bedrohungen lassen sich problemlos** in moderne UEM-Lösungen integrieren und bieten Sicherheitsteams eine einfache und schnelle Methode zur Beseitigung priorisierter Risiken, ohne die regulären Benutzer- oder IT-Administrationsabläufe zu beeinträchtigen.

Zwar bieten die UEM-Automatisierungen für die Geräteeinführung und die Richtlinienkontrollen einige grundlegende Schutzmaßnahmen für die Cyber-Hygiene, und die Protokolle der Geräte- und Benutzeraktivitäten bieten eine zuverlässige Überwachung, die von den Sicherheitsteams mit Begeisterung genutzt werden kann, doch die meisten Plattformen benötigen zusätzliche Kontrollen und Tools, um ihr volles Potenzial als zentrale Anlaufstelle für die gesamte Endpunktsicherheit eines Unternehmens auszuschöpfen. (Verizon)

# 1 Die Beteiligung der Sicherheit an UEM beginnt mit DEX.

Wie kaum eine andere Abteilung außerhalb der IT selbst werden Sicherheitsteams Investitionen in eine proaktivere DEX-Technologie – einschließlich UEM-Lösungen – unterstützen, insbesondere da die Risiken der Schatten-IT und der immer größer werdenden Angriffsflächen für Endgeräte in einem hybriden Arbeitsplatz nach der Pandemie immer weiter zunehmen.

- CIOs nennen Schatten-IT-Lösungen oder -Produkte als eine der Hauptsorgen für die Kontinuität von Regierungen in aller Welt. (NASCIO)
- 12,8 % der Cloud-basierten Cyberangriffe im Jahr 2022 betrafen Schatten-IT. (Shackleford)
- Nur 52 % der befragten Sicherheitsexperten berichten von einem „hohen“ Grad an Asset-Transparenz in ihrem Unternehmen – und 10 % gaben an, dass sie überhaupt kein Asset-Ermittlungs-Tool verwenden.

Und Hacker nutzen diese Lücke zwischen dem, was das Sicherheitsteam zu schützen weiß, und dem, was die Benutzer getan haben, um ihren Arbeitstag zu erleichtern, bereits aus.

**12,8 %** **aller Cloud-basierten Cyberangriffe im Jahr 2022 betrafen Schatten-IT.**

## Auswirkungen in der Praxis

# Als schlechtes DEX fast dazu führte, dass Hacker eine Petrochemieanlage in die Luft jagten

Im Jahr 2017 hackten Angreifer das saudi-arabische Petrochemieunternehmen Triconex. Das Sicherheitsteam bemerkte erst, dass sein System durchbrochen worden war, als sechs Controller ausfielen und einen Alarm auslösten.

Die Einsatzkräfte fanden schnell heraus, dass jemand aus der Ferne auf die Systeme zugegriffen hatte, um Malware einzuschleusen – aber das schien unmöglich!

Schließlich waren die Sicherheitssysteme der Anlage so konzipiert, dass sie Angriffe aus der Ferne vereiteln konnten, da ein Mitarbeiter einen physischen Schlüssel an der Konsole der Anlage einstecken musste, um Konfigurationsänderungen vorzunehmen.

Durch die räumliche Anordnung der Anlage war der Controller jedoch vom Kontrollraum getrennt, so dass die Bediener von einem Raum zum anderen gehen mussten, um Änderungen vorzunehmen. Ein Mitarbeiter hatte seinen physischen Schlüssel in der Konsole des Controllers aufbewahrt, damit er – und die Hacker – aus der Ferne auf den Code für Updates zugreifen konnten.

Hätten andere redundante Sicherheitssysteme die Mitarbeitenden der Anlage nicht auf die kritischen Ausfälle aufmerksam gemacht, die durch die Aktivitäten des Hackers ausgelöst wurden, hätten die kompromittierten Controller von Triconex alle Sicherheitssysteme abschalten und die Mitarbeitenden der Anlage töten können, entweder durch das Austreten von Chemikalien oder durch regelrechte Explosionen.

Dieser Cyberangriff könnte einer der ersten Hacks gewesen sein, bei dem ein Mensch ums Leben kam – und das alles wegen eines müden Mitarbeitenden und des Versäumnisses des Sicherheitsentwicklers, menschliches Verhalten bei der Entwicklung „narrensicherer“ Sicherheitssysteme zu berücksichtigen. (Rhysider)

2

# Sichern Sie mehr verschiedene Arbeitsumgebungen und IoT-Endpunkte über UEM-Clients.

Bei Remote-Arbeiten denkt man an Mitarbeiter, die in einem Café arbeiten, mit eingesteckten Kopfhörern, die nichts von dem anderen „Kunden“ mitbekommen, der darauf wartet, dass sie die Toilette aufsuchen, um geschützte Dateien herunterzuladen und ihren ungesperrten Laptop zu benutzen.

Auch wenn menschliches Versagen in gewissem Umfang immer vorhanden sein wird, werden Endpunktsicherheitslösungen und -richtlinien, die von der UEM-Plattform des IT-Teams durchgesetzt werden, dazu beitragen, einige der Risiken zu beseitigen, die durch einen geografisch vielfältigeren Arbeitsplatz entstehen.

Lassen Sie uns über zwei der häufigsten Risiken für die Endpunktsicherheit sprechen: die Verbreitung des Internets der Dinge (IoT) und Man-in-the-Middle-Angriffe in öffentlichen Netzwerken.

(Spoiler-Alarm: Beide Szenarien lassen sich durch eine ordnungsgemäße Erkennung von Assets, Netzwerksegmentierung und Geräteüberwachung beheben – all dies kann durch UEM-Lösungen mit den richtigen sicherheitsorientierten Konfigurationen und unterstützenden Funktionen durchgeführt werden).

# Auswirkungen in der Praxis

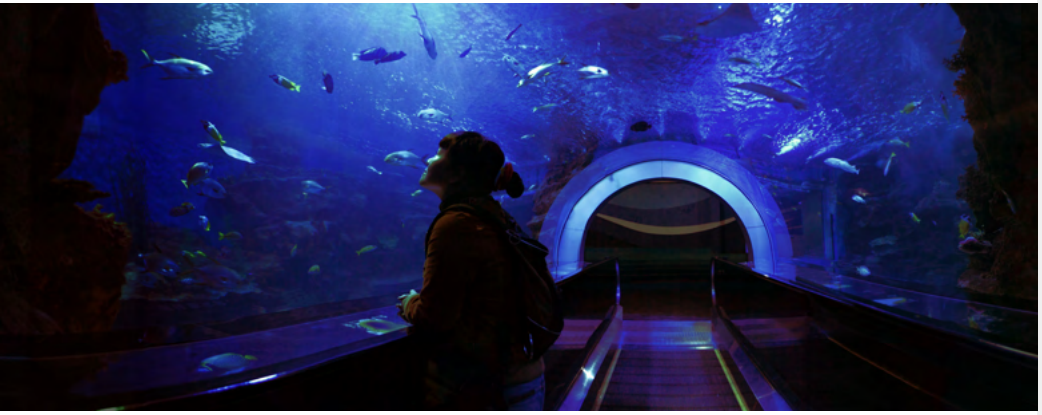
## Unerwartete Angriffe über das Internet der Dinge (IoT)

IoT-Angriffe machten im Jahr 2021 mehr als 12 % aller weltweiten Malware-Angriffe aus – gegenüber weniger als 1 % aller Malware-Angriffe im Jahr 2019. (IBM Security)

Dennoch gaben 47 % der befragten IT-Experten an, dass ihr Unternehmen keine IoT-Compliance-Richtlinie hat. (SAM)

IoT-fähige Geräte sowohl in Unternehmen als auch an entfernten Arbeitsplätzen können durch relativ einfache Netzwerksegmentierung und aktive Scan-Funktionen geschützt werden.

Viele dieser Geräte sind jedoch solche, die Unternehmen und Endbenutzer nicht unbedingt in ihre Risikoanalyse einbeziehen würden, bis es zu spät ist – wie diese Unternehmen festgestellt haben.



### Thermometer für Aquarien

Ein nordamerikanisches Kasino erlebte, welchen Schaden ein nicht verwaltetes IoT in seinem Betrieb anrichten kann, als Hacker eine Sicherheitslücke im Aquarium-Thermometer der Kasinolobby ausnutzten. Da dieser IOT-fähige Tank im Netzwerk des Casinos nicht ordnungsgemäß segmentiert war, konnten die Hacker seitlich in die Cloud-Infrastruktur des Casinos eindringen und ihren Angriff fortsetzen. (Wei)

### Medizinische Geräte

Der WannaCry Ransomware-Angriff im Jahr 2017 veranlasste Hersteller und Behörden, Sicherheitslücken von mit dem Internet verbundenen medizinischen Geräten – einschließlich Insulinpumpen und Herzschrittmachern – zu überdenken. (Chase, Coley und Connolly)

### Fahrzeuge

**2015:** Hacker haben einen Jeep Cherokee gekapert und den Motor während der Fahrt auf der Autobahn abgeschaltet. (Greenburg)

**2023:** Ein Tesla-Fahrer fand heraus, dass die offizielle Tesla-Mobil-App ihm erlaubte, ein Fahrzeug zu betreten – und zu fahren -, das ihm nicht gehörte. (Day)

**Nach 2023:** Regierungsbeamte warnen, dass es „derzeit kein umfassendes Konzept für die Cybersicherheit gibt“, weder für Elektrofahrzeuge noch für deren Ladegeräte (SANDIA) – Fahrzeuge, mit denen die Mitarbeitenden von Unternehmen zu Büros oder Meetings außerhalb des Unternehmens fahren und mit denen sie ihre Firmengeräte per Bluetooth verbinden werden.

## Auswirkungen in der Praxis

# Der (beinahe) Man-in-the-Middle-Hack von Equifax

Einer der häufigsten Angriffe auf mobile Geräte und Endpunkte ist der Man-in-the-Middle-Angriff (MitM). Wenn Mitarbeitende über ein unsicheres Netzwerk oder eine unsichere Internetverbindung auf vertrauliche Informationen zugreifen, können sich Hacker mitten in den Datenfluss einklinken und geschützte Informationen „abfangen".

Die Aussicht auf einen MitM-Angriff war der Grund, warum Equifax, ein amerikanisches Unternehmen für Verbraucherkredite, 2017 seine Apps sowohl von Apple als auch von Google heruntergenommen hat.

Nachdem das Unternehmen in berüchtigter Weise die persönlichen Daten von 143 Millionen Kunden monatelang Hackern preisgegeben hatte, die in seinem Netzwerk lauerten, weil es versäumt hatte, eine bekannte Sicherheitslücke (Khandelwal) zu schließen, wurde der Sicherheitsforscher Jerry Decime neugierig: Hatte Equifax nach diesem Verstoß die Sicherheit im gesamten Unternehmen verstärkt?

Decime untersuchte die mobilen App-Versionen der Equifax-Software und stellte zu seiner Überraschung fest, dass die Apps nach der anfänglichen Authentifizierung in einer Reihe von kritischen Bereichen keine HTTPS-Protokolle mehr verwendeten. (Decime)

Alle Informationen, die nach der Authentifizierung zwischen dem Gerät des Benutzers und den Equifax-Servern übertragen wurden – einschließlich weiterer persönlicher Daten und finanzieller Transaktionen! – hätten von einem cleveren Hacker, der erkannt hat, dass die Sicherheit nur oberflächlich ist, abgefangen und exfiltriert werden können.

Es ist Equifax hoch anzurechnen, dass sie innerhalb einer Stunde auf die Mitteilung von Decime reagierten und die unsicheren Apps sowohl vom Apple- als auch vom Google-App-Marktplatz entfernten. (Weissman)

Dieses klassische Beispiel eines MitM-Angriffs unterstreicht jedoch, wie wichtig eine sichere Kommunikation zwischen einem Benutzer und dem Server eines Unternehmens ist – oder zwischen Ihren Mitarbeitern und den sensiblen Informationen und Netzwerken Ihres Unternehmens.

UEM-Lösungen und Sicherheitstools von Partnern können die Anfälligkeit für diese Arten von Angriffen proaktiv begrenzen:

- Robuste Benutzerzugriffsprofile.
- Automatische Deprovisionierung von Zugangsdaten.
- Sichere Datenzugriffs- und Kommunikationskanäle, wie VPNs oder Zero Trust-Kontrollen – ebenfalls über UEM-Lösungen bereitgestellt und überwacht.

3

# Durchgesetzte Sicherheitsrichtlinien und Geräteaufzeichnungen verhindern, dass Hacker in Unternehmensnetzwerken Fuß fassen können.

Proaktive Cybersicherheitsstrategien versuchen nicht nur, Hacker davon abzuhalten, in Unternehmensnetzwerke einzudringen, sondern berücksichtigen auch, was passiert, wenn es bösen Akteuren gelingt, einzudringen.

Nehmen Sie den einfachen USB-Stick. Es kann große Dateien wie Präsentationen, Videos und Musik speichern und auf neuen Computern verwenden, ohne auf eine Netzwerkverbindung warten zu müssen, um Material hoch- oder herunterzuladen.

Wenn USB-Laufwerke große Dateien für legitime Zwecke transportieren können, dann können sie natürlich auch Malware transportieren.

UEM-Lösungen können standardmäßig automatisch Richtlinien für Wechseldatenträger bereitstellen und durchsetzen. Durch solche Richtlinien müssen die Endbenutzer Ihres Unternehmens eine spezielle Erlaubnis für die Verwendung von speicherintensiven Geräten mit ihren firmeneigenen Computern beantragen, anstatt alle Geräte und Endpunkte automatisch diesen Angriffen auszusetzen.

## Auswirkungen in der Praxis

# Stuxnet: Die berühmteste USB-Stick-Malware der Welt

Stuxnet ist der Name eines Computervirus, der angeblich von bestimmten Geheimdiensten entwickelt wurde, um das iranische Programm zur nuklearen Anreicherung zum Scheitern zu bringen.

Die Anlage wurde unter strengsten Sicherheitsvorkehrungen betrieben – was bedeutete, dass sie von jeglichem Internet- oder Netzwerkzugang von außen abgeschirmt war. Die einzige Möglichkeit, wie Malware in die Einrichtung gelangen konnte, war, dass ein bereits vertrauenswürdiger Insider sie persönlich an einen Computer im Netzwerk der Einrichtung anschloss.

Die Angreifer erstellten also einen Computervirus, der nur die industriellen Kontrollsysteme angriff, die die iranische Anlage für die Zentrifugen verwendete, und luden das gesamte Malware-Paket auf USB-Sticks.

Die manipulierten Datenträger wurden in der Region verteilt, damit die Atomwissenschaftler sie finden würden – vielleicht auf Konferenzen, vielleicht einfach von vertrauenswürdigen Kollegen aus der Region ausgehändigt.

Schließlich machte ein Wissenschaftler den fatalen Fehler und steckte einen USB-Stick mit der Stuxnet-Malware ein... und das Programm beschädigte schätzungsweise 1.000 Zentrifugen und verschwendete Material, was dazu beitrug, die iranische Führung unter Druck zu setzen, das iranische Atomabkommen von 2015 zu unterzeichnen.

**Wenn Sie mehr über Stuxnet erfahren möchten, sehen Sie sich diese Ressourcen an:**

- „Ep 29: Stuxnet" von Jack Rhysider
- "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon" von Kim Zetter

Die Geräte- und Benutzerprotokolle, die eine UEM-Plattform aufzeichnet, können auch für Sicherheitszwecke verwendet werden.

Wenn das Unternehmen Grund zu der Annahme hat, dass ein Mitarbeiter eine Insider-Bedrohung darstellen könnte, können die Sicherheitsteams die Aufzeichnungen eines Geräts auf Anzeichen dafür überprüfen, dass Tools auf Systemadministrator-Ebene wie PowerShell illegal auf dem Gerät eines Benutzers installiert und verwendet wurden.

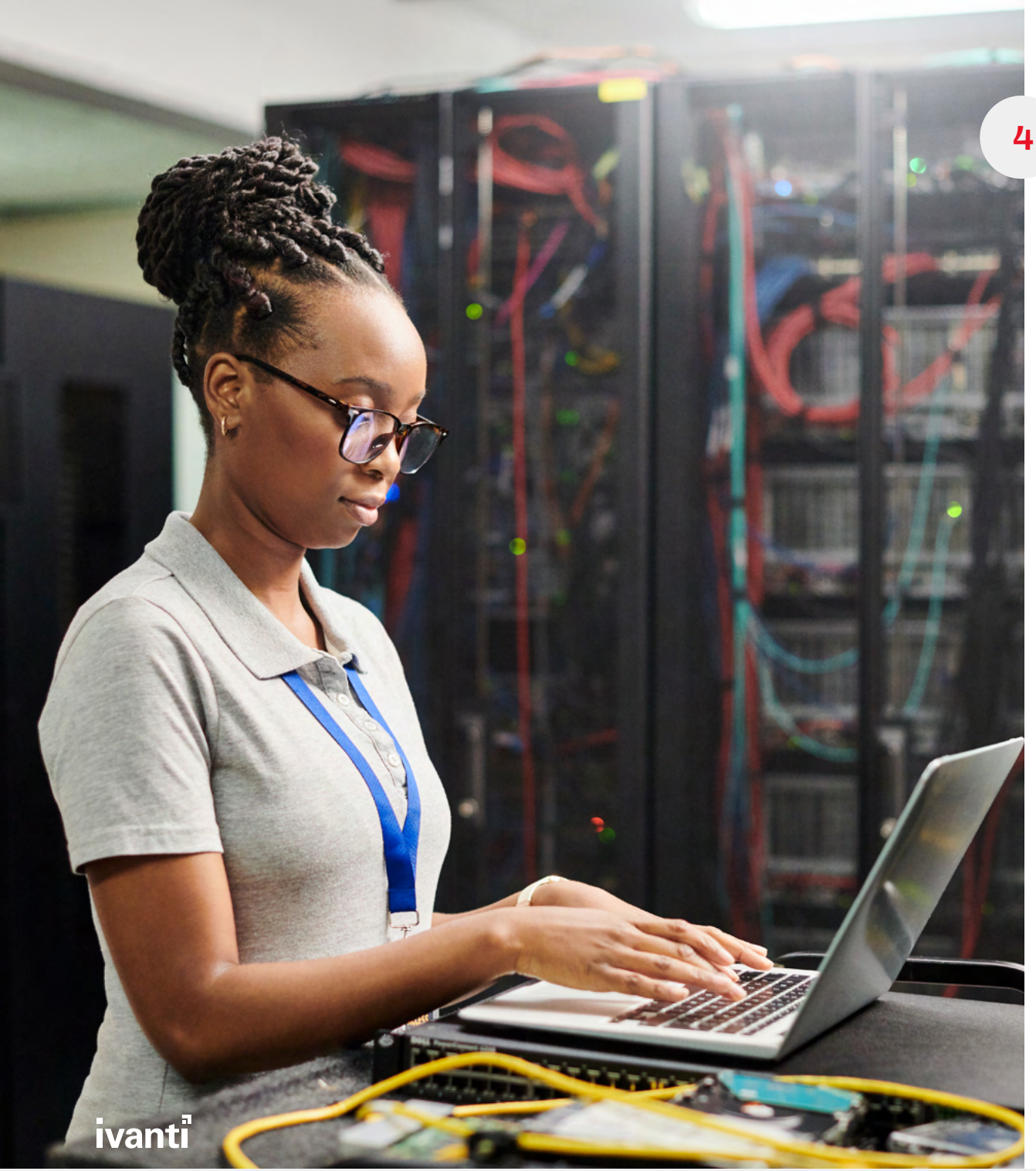
Oder das System eines Unternehmens warnt vor der Aktivität eines gewöhnlichen „Benutzers“, der plötzlich fortgeschrittene Netzwerktechniken auf dem verwalteten Gerät des Unternehmens ausführt.

Solche Aktivitäten können ein Zeichen dafür sein, dass es sich gar nicht um den autorisierten Benutzer handelt, sondern um einen Hacker, der sich hinter den authentischen (aber kompromittierten) Anmeldedaten dieses Benutzers versteckt und versucht, seine Privilegien im Unternehmensnetzwerk zu erweitern.

Mit den richtigen Konfigurationen, Warnmeldungen und Sicherheitstools können diese Aktivitäten auf einem Endgerät oder einem mobilen Gerät erkannt werden, lange bevor der Hacker sich im Netzwerk des Unternehmens bewegt oder Administratorrechte erhält.

Und da steigende Cyberversicherungspreise die ohnehin schon angespannten Unternehmensfinanzen weiter belasten, könnte es sich für IT- und Sicherheitsteams durchaus lohnen, strengere Richtlinien für entfernbare Medien und Warnmeldungen zu Benutzeraktivitäten durchzusetzen, um proaktiv Risiken zu beseitigen und Versicherungsprämien zu senken. (Breg)

ivanti



4

# Einfache Integrationen bieten einfache, einmalige Sicherheitsimplementierungen.

Eine gut integrierte UEM-Plattform bietet zwar grundlegende Möglichkeiten der Cyberhygiene, kann aber nicht das A und O Ihrer Endpunkt-Sicherheitslösungen sein.

UEM-Lösungen bieten jedoch eine hervorragende Ausgangsposition für andere Tools – wie Patch-Management oder Lösungen zur Abwehr mobiler Bedrohungen. Schließlich hat das UEM selbst einen Client, der direkt auf jedem eigenen und verwalteten Gerät des Unternehmens installiert ist.

Mit nur wenigen Mausklicks können andere Sicherheitstools über den UEM-Client mit demselben Gerät verbunden werden. So können Sie Ihre Endpunkt-Sicherheitsmaßnahmen sofort verstärken, ohne die DEX-Funktionalität Ihres Unternehmens oder die Produktivität der Endbenutzer zu beeinträchtigen.

# UEM + Risikobasiertes Patch-Management

UEMs können beispielsweise mit risikobasierten Lösungen zur Verwaltung von Patches und Sicherheitslücken kombiniert werden, um eine nahtlose proaktive Risikoreaktion zu ermöglichen und aktiv ausgenutzte Sicherheitslücken in Ihrer aktuellen Umgebung zu beheben.

1 **Das Sicherheitsteam analysiert aktuelle Bedrohungsdaten,** indem es aktuell ausgenutzte Sicherheitslücken auf die derzeit verwendeten Geräte und Anwendungen Ihres Unternehmens anwendet.

- Die aktiven Scan-Funktionen des UEM stellen sicher, dass kein Gerät und keine Anwendung bei dieser ersten Prüfung übersehen wird!

2 **Das Sicherheitsteam depriorisiert oder beschleunigt aktuelle ungepatchte Sicherheitslücken**, je nach Risikoumfeld und Prioritäten Ihres Unternehmens. Sie können folgendes in Betracht ziehen:

- Prioritätsstufe der potenziell betroffenen Geräte, Benutzer, Betriebssysteme und unternehmenskritischen Funktionen.
- Ob eine Sicherheitslücke aktiv von bekannten Angreifern ausgenutzt wurde.
- Welche Art von Zugriff oder Berechtigungen ein Angreifer durch einen Exploit erhalten könnte.
- Wie oft die potenziell betroffenen Geräte oder Anwendungen von der Organisation genutzt werden, entweder passiv oder aktiv.
- Wie schwierig es sein wird, einen Patch aufzuspielen, oder ob andere Abhilfemaßnahmen erforderlich sind (Quarantäne, Segmentierung usw.).

3 **Das IT-Team erhält eine Liste der priorisierten Patches,** zusammen mit:

- Informationen darüber, warum diese Patches auf der Grundlage der einzigartigen Risikofaktoren des Unternehmens implementiert werden sollten – was dem IT-Team die Gewissheit gibt, dass die Sicherheitsbehörden nicht von ihnen verlangen, einfach alle möglichen Sicherheitslücken zu patchen!
- Bestimmte Geräte oder Benutzer für das Rollout von Patches in einem festgelegten Rhythmus.
- Bekannte mögliche Interferenzen mit aktuellen Softwarepaketen oder Arbeitsabläufen.

4 **Das IT-Team verteilt automatisch Patches über die UEM-Plattform auf die identifizierten Geräte und Endpunkte.** Dabei werden die Updates so geplant, dass die Produktivität der Endbenutzer möglichst wenig beeinträchtigt wird, und es wird auf merkwürdige Aktivitäten geachtet, die darauf hinweisen, dass ein Patch die regulären Arbeitsabläufe beeinträchtigt hat.

Weitere Informationen zu risikobasierten Patching- und Abhilfestrategien finden Sie in The Ultimate Guide to Risk-Based Patch Management.

# UEM und Mobile Threat Defense

Jeder ist anfällig für Phishing – sogar die Profis!

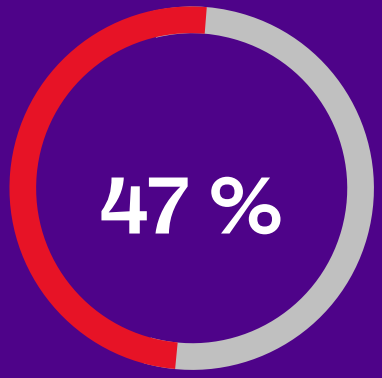
Phishing-Kampagnen sind ein bekannter Einstiegspunkt für Ransomware-Banden und machen bis 2020 54 % aller Ransomware-Übertragungsmethoden aus. (Datto)

Spezialisierte „Whaling"-Phishing-Angriffe – von Hackern erstellte E-Mail-Kampagnen, die speziell auf Führungskräfte in großen Unternehmen abzielen – führten dazu, dass amerikanische Unternehmen im Jahr 2021 schätzungsweise 2,4 Milliarden US-Dollar verloren. (Verizon)

Neue Forschungen haben gezeigt:

- 47 % der IT-Profis geben zu, auf einen Phishing-Angriff hereingefallen zu sein. (Ivanti)
- Nur 43 % der Sicherheitsexperten geben an, dass ihre Unternehmen in den letzten 24 Monaten einen Phishing-Angriff erlebt haben (Ivanti) – obwohl andere Branchenberichte feststellen, dass 83 % der Unternehmen im Jahr 2021 einen erfolgreichen Phishing-Angriff erlebt haben (Verizon).
- Mehr als ein Drittel der Führungskräfte gibt zu, auf einen Phishing-Link geklickt zu haben – das ist viermal so viel wie bei anderen Mitarbeitenden im Büro. (Ivanti)

**Zwischen der Zahl der Phishing-Angriffe, von denen die Sicherheitsteams glauben, dass sie in ihren Unternehmen vorkommen, und der Zahl der tatsächlichen Phishing-Angriffe klafft eine Lücke von 40 Punkten.**




**der IT-Experten sind Opfer von Phishing-Angriffen geworden.**

Also, wenn:

- IT-Spezialisten auf Phishing-E-Mails hereinfallen
- Sicherheitsspezialisten nicht erkennen, dass ihre Unternehmen Phishing-Angriffen ausgesetzt sind
- Ältere Führungskräfte immer häufiger zum Ziel von Angriffen werden – und immer häufiger auf diese Angriffe herein fallen

... dann reichen Sicherheitsschulungen und Spam-Filter in den Posteingängen von Unternehmen nicht aus, um Benutzer davon abzuhalten, die Sicherheit von Unternehmen durch Phishing-Kampagnen zu gefährden.

Die Konfigurationen und Einstellungen eines UEM können zwar dazu beitragen, den anfänglichen Schaden zu begrenzen, der durch das Anklicken eines Phishing-Links entsteht – vor allem, wenn es mit einer Patching-Lösung gekoppelt ist, die die Möglichkeiten der Hacker, ihre Privilegien zu erweitern oder sich im Netzwerk zu bewegen, stark einschränkt –, aber es ist nicht annähernd so effektiv, wenn es nicht mit einer speziellen Lösung zur Abwehr mobiler Bedrohungen (MTD) gekoppelt ist.

Die besten MTD-Lösungen können über den UEM-Client eines angemeldeten Geräts ausgeführt werden – entweder im Besitz des Unternehmens oder als Teil eines BYOD-Programms – ohne die regulären Benutzeraktivitäten zu beeinträchtigen oder zusätzlichen Speicher zu verbrauchen.

Wenn die MTD Lösung Folgendes erkennt:

- **Ein eingehender Phishing-Link:** Das System blockiert sofort die Bewegung und stellt sicher, dass die Aktion vom Benutzer nicht abgeschlossen wird.
- **Potentiell bösartige Aktivitäten:** Die MTD- und UEM-Lösungen führen dann je nach Aktivität und potenzieller Bedrohung automatisch verschiedene Abhilfemaßnahmen durch – bis hin zum Entzug des Benutzerzugriffs auf alle Unternehmensanwendungen, auch auf einem persönlichen Gerät!  – bis der Benutzer die Anwendung entfernt oder das Problem anderweitig behoben hat.
- **Ein nicht installiertes Betriebssystem-Update:** Das System bietet dem Benutzer höflich eine Push-Benachrichtigung an, die ihn auffordert, das Update zu installieren. Wenn der Benutzer sein Gerät weiterhin nicht aktualisiert, werden immer mehr Abhilfemaßnahmen ergriffen – bis hin zur Quarantäne von Unternehmensanwendungen oder dem Zugriff von einem veralteten Gerät.

04

# Wie Sie Ihre UEM-Lösung auswählen

Es gibt viele leistungsstarke UEM-Lösungen auf dem Markt. Die meisten bieten die in diesem Leitfaden beschriebenen grundlegenden Funktionen an, aber jeder Anbieter bietet auch einzigartige Funktionen.

Wie wählen Sie also den richtigen UEM-Anbieter für Ihr Unternehmen aus? Eine, die Sie dort abholt, wo Sie gerade sind – die aber auch skalierbar ist und neue Möglichkeiten für immer bessere Kontrollen und Sicherheit bietet, wenn die Anforderungen Ihres Unternehmens wachsen?

**Ihre einheitliche Endpunktverwaltungslösung sollte:**

- ☐ Unterstützen Sie die gesamte Palette der Geräte und Betriebssysteme, die Ihr Unternehmen derzeit verwendet – oder in Zukunft verwenden könnte – einschließlich macOS, iOS, iPadOS, Windows, ChromeOS, Android und Linux.
- ☐ Bieten Sie ein einheitliches Dashboard an, das Informationen über Geräte und Benutzeraktivitäten enthält, damit IT- und Sicherheitsteams mit denselben Daten arbeiten können.
- ☐ Unterstützen Sie sowohl On-Premises- als auch Cloud-Implementierungen, einschließlich Cloud-nativer Anwendungen – selbst wenn ein Unternehmen glaubt, dass alle „nur“ vom Büro aus arbeiten!
- ☐ Fassen Sie Benutzer- und Geräteinformationen zusammen und erstellen Sie klare Berichte, um umfassendere Strategien für IT-Assets und Sicherheitsendpunkte wie Softwarelizenzvereinbarungen oder risikobasierte Patching-Strategien zu entwickeln.
- ☐ Erleichtern Sie die einfache, automatische Registrierung und Bereitstellung von Geräten.
- ☐ Sie laufen so leise und „unsichtbar“ wie möglich und sorgen für ein positives Technologieerlebnis bei den Endbenutzern, während sie proaktiv Probleme beheben und es den IT-Teams ermöglichen, sich strategischeren Initiativen zu widmen als der Bearbeitung von einfachen Helpdesk-Tickets.
- ☐ Integrieren Sie nativ verwandte Endpunktsicherheitstools wie risikobasierte Lösungen zur Verwaltung von Sicherheitslücken und zur Abwehr mobiler Bedrohungen, denn eine UEM-Plattform kann nicht alles alleine machen – und lassen Sie sich von keinem Anbieter etwas anderes einreden!
- ☐ Implementieren Sie Standard-Automatisierungen, Service-Level-Vereinbarungen und Warnmeldungen wie Deprovisioning-Protokolle, Onboarding-Verfahren, Aktivitätsspitzen oder Lags, Jailbreaking-Verhalten von bösartigen Anwendungen, genehmigte Patch-Rollouts usw.

## Auswirkungen in der Praxis

# Die Total Economic Impact™ Studie für Ivanti Neurons for UEM

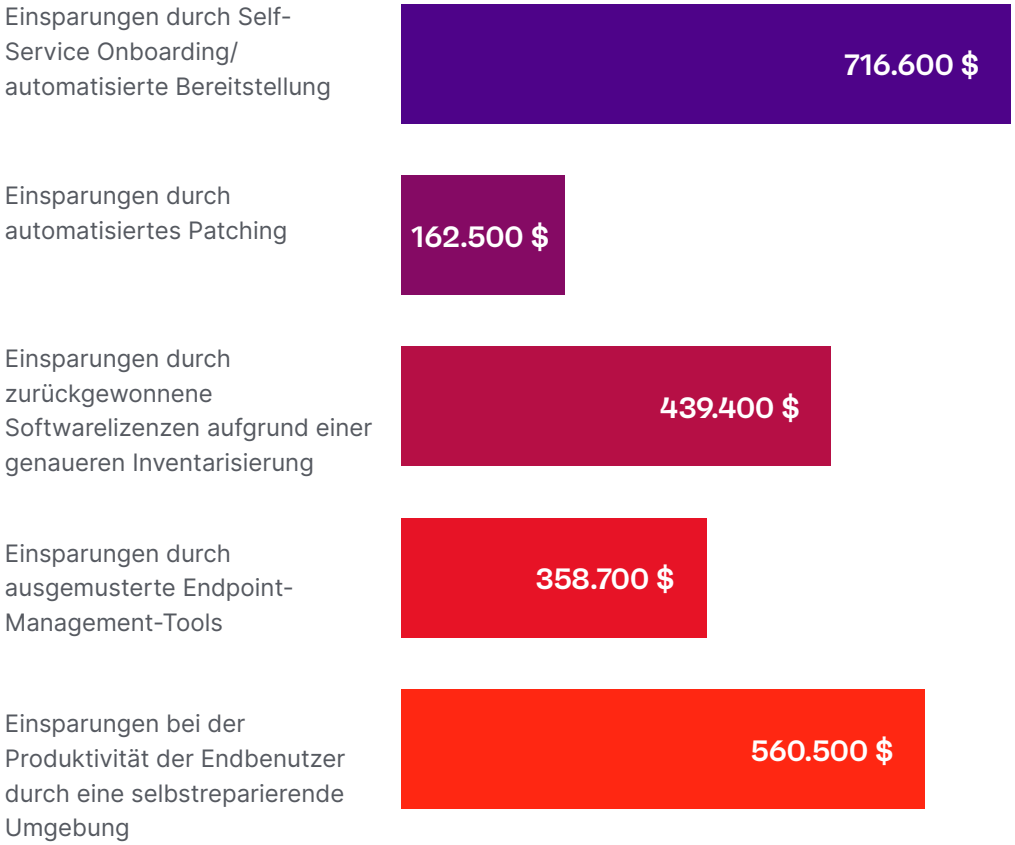
Eine im Juli 2022 von Forrester Consulting im Auftrag von Ivanti durchgeführte Total Economic ImpactTM -Studie ergab, dass ein Unternehmen, das 10.000 Endpunkte verwaltet und jährlich um 5 % wächst, durch die Implementierung von Ivanti Neurons for UEM über einen Zeitraum von drei Jahren Vorteile in Höhe von 2,24 Millionen US-Dollar gegenüber Kosten in Höhe von 619.000 US-Dollar erzielte. (Forrester Consulting TEI-Studie)

Diese Vorteile summierten sich zu einem Nettogegenwartswert (NPV) von 1,62 Mio. USD und einem dreijährigen ROI von 261 %, wobei sich die Anfangsinvestition der Verbundorganisation innerhalb von sechs Monaten nach der Installation amortisierte. (Forrester Consulting TEI-Studie)

Laut der ebenfalls in Auftrag gegebenen TEI-Studie wurden diese Einsparungen erzielt durch:

- Konsolidierung des Tech-Stacks
- Zurückgeforderte Software-Lizenzen
- Automatisiertes Patchen
- Verbesserte Benutzerproduktivität
- Onboarding und Bereitstellung per Self-Service

**Vorteile (drei Jahre) für Gesamtorganisation**



# Laut den Befragten der in Auftrag gegebenen TEI-Studie

**Self-Service Onboarding und automatisierte Bereitstellung**
**716.632 USD Einsparungen über 3 Jahre für die Gesamtorganisation**

„Was wir jetzt mit Ivanti entwickelt haben, ist ein Onboarding-Formular, das ein Vorgesetzter über das Self-Service-Portal einreichen kann. Es schneidet automatisch ein Ticket aus und leitet es an die richtigen Teams weiter. Wir müssen nicht mehr wie früher eine Checkliste abarbeiten."

(Der Befragte schätzte außerdem, dass die IT-Abteilung 50 % weniger Zeit für den Onboarding-Prozess aufwenden musste).

– IT-Spezialist für eine Regierungsbehörde

**Tech-Stack-Konsolidierung und ausgemusterte Legacy-Tools**
**358.734 USD 3-Jahres-Einsparungen für Gesamtunternehmen**

„Meine Fernsteuerungslösung kostete 75.000 Dollar pro Jahr. Mein [IT Asset Management] (ITAM) kostete weitere 100.000 Dollar. Wissensmanagement kostete weitere 20.000 Dollar pro Jahr ... Wenn ich mich mit einem Anbieter zusammenschließe und all diese Kosten zusammenfasse, kann ich sparen."

– Direktor für IT- und Telekommunikationssupport bei einem Unternehmen für Sterbebegleitung

**Automatisierte Patching-Funktionen und Integrationen**
**162.515 USD Einsparungen über 3 Jahre für die Gesamtorganisation**

„Wir haben einen Monat gebraucht, um zu entwerfen und zu besprechen, wie wir die Patches automatisieren wollten. Seitdem wir die Richtlinie erstellt haben, dauert es weniger als eine Stunde, um ein Rollout-Projekt einzurichten, und dann wird das Patching einfach durchgeführt. Ich muss mich nicht kümmern und ich kann darauf vertrauen, dass das, was ich sehe, korrekt ist."

– Integrationsmanager für ein Schuhhandelsunternehmen

**Zurückgeforderte Software-Lizenzen**
**439.449 USD Einsparungen über 3 Jahre für die Gesamtorganisation**

„Früher war es ein sehr langwieriger Prozess, wenn wir Softwarelizenzen stillegen wollten. Wir mussten die Benutzer erreichen und sie fragen: ‚Hey, Sie haben das schon lange nicht mehr benutzt, können wir die Lizenz zurückholen?' Als wir unsere Softwarelizenzen in die EPM-Lösung [Teil von Ivanti Neurons for UEM] integriert haben, konnten wir die Rückforderung von Software automatisch durchführen [...] Das war wahrscheinlich die größte Ersparnis, die wir damit erzielen konnten."

- Manager für Infrastruktur- und Endpunktlieferdienste für ein Lebensmittelproduktionsunternehmen

**Verbesserte Endbenutzer-Produktivität**
**560.521 USD Einsparungen über 3 Jahre für die Gesamtorganisation**

„Durch die selbstreparierenden Maßnahmen – Aktualisierung alter Profile, Neustart von Computern, die seit sieben Tagen nicht mehr neu gestartet wurden, Patches am Abend – haben wir unseren Endbenutzern geholfen, produktiver zu werden, weil die Computer einen Teil der Ressourcen zurückerhalten, die vorher verbraucht wurden [...] Jede Minute, die sie einsparen können, ist ein finanzieller Vorteil für die Endbenutzer."

– Direktor für IT- und Telekommunikationssupport bei einem Unternehmen für Sterbebegleitung

Für weitere Informationen lesen Sie bitte den Total Economic ImpactTM von Ivanti Unified Endpoint Management (UEM) Lösungen.

# Referenzen


1. Bitwarden. 2022 Password Decisions Survey. November 2021. https://bitwarden.com/images/resources/2022-password-decisions-survey.pdf.
2. Bond, Shannon. Twitter employees quit in droves after Elon Musk's ultimatum passes. 17 November 2022. https://www.npr.org/2022/11/17/1137413251/twitter-employees-quit-elon-musk.
3. Bonner, Carole. Health and Wellbeing for the Remote & Hybrid Workforce. 20 October 2022. https://8926463.fs1.hubspotusercontent-na1.net/hubfs/8926463/Remote%20Hybrid%20Workforce_Formatted.pdf.
4. Brasen, Steve. Evolving Requirements for Digital Employee Experience (DEX). 4 August 2022. https://www.ivanti.com/resources/v/doc/ebooks/ema-iva009a-ivanti-requirements-ebook.
5. Breg, David. Quarterly Cyber Insurance Update. 10 February 2023. https://www.wsj.com/articles/quarterly-cyber-insurance-update-february-2023-62141c19.
6. Chase, Melissa, et al. Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook. 14 November 2022. https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response.
7. Cipolla, Tom, et al. Magic Quadrant for Unified Endpoint Management Tools. 1 August 2022. https://www.gartner.com/doc/reprints?id=1-2AQEK9FU&ct=220802&st=sb.
8. Datto. Datto's Global State of the Channel Ransomware Report. November 2020. https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf.
9. Day, Lewin. Tesla App Unlocks Someone Else's Car, Lets Them Drive Away in It. 14 March 2023. https://www.thedrive.com/news/tesla-app-unlocks-someone-elses-car-lets-them-drive-away-in-it.
10. Decime, Jerry. Settling the score: taking down the Equifax mobile application. n.d. https://www.linkedin.com/pulse/settling-score-taking-down-equifax-mobile-application-jerry-decime/.
11. Flexera Software. 2021 State of IT Visibility Report. June 2021. https://info.flexera.com/ITV-REPORT-State-of-IT-Visibility.
12. Forrester Consulting study commissioned by Ivanti. The Total Economic Impact™ Of Ivanti Unified Endpoint Management (UEM) Solutions. July 2022. https://rs.ivanti.com/reports/forrester-tei-of-ivanti-uem-solutions-2022.pdf.
13. Greenburg, Andy. Hackers Remotely Kill a Jeep on the Highway—With Me in It. 21 July 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
14. IBM Security. X-Force Threat Intelligence Index 2022. February 2022. https://www.ibm.com/downloads/cas/ADLMYLAZ.
15. Insight Enterprises & CIO. Insight intelligent technology report 2022: IT ambions for business transformation. November 2021. https://ca.insight.com/en_CA/content-and-resources/gated-content/insight-intelligent-technology-report-ac1252.html.
16. Ivanti. 2022 Digital Employee Experience Report. 28 June 2022. https://rs.ivanti.com/ivi/2700/4e528f833de3.pdf.
17. —. 9 Must-Know Phishing Attack Trends. 20 July 2021. https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465.
18. —. Getting Started With DEX: Core Areas of Focus to Deliver a Great Digital Employee Experience. 23 Novemer 2022. https://rs.ivanti.com/ivi/2734/f6efbc801083.pdf.
19. —. Government Cybersecurity Status Report. 9 March 2023. https://www.ivanti.com/resources/v/doc/ivi/2747/a856c631661d.
20. —. Press Reset: A 2023 Cybersecurity Status Report. December 2022. https://www.ivanti.com/lp/security/assets/s1/2023-cybersecurity-status-report.
21. Khandelwal, Swati. Equifax Suffered Data Breach After It Failed to Patch Old Apache Struts Flaw. 14 September 2017. https://thehackernews.com/2017/09/equifax-apache-struts.html.
22. Kolodny, Lora. Twitter is down to fewer than 550 full-time engineers. 20 January 2023. https://www.cnbc.com/2023/01/20/twitter-is-down-to-fewer-than-550-full-time-engineers.html.
23. Lutkevich, Ben. Wi-Fi Pineapple. October 2022. https://www.techtarget.com/searchsecurity/definition/Wi-Fi-Pineapple.

# Referenzen


24. Morning Consult and IBM. IBM Security Incident Responder Study. 3 October 2022. https://www.ibm.com/downloads/cas/XKOY5OLO.

25. NASCIO. The 2021 State CIO Survey. October 2021. https://www.nascio.org/wp-content/uploads/2021/10/2021-State-CIO-Survey.pdf.

26. Palmer, Annie. Amazon employees push CEO Andy Jassy to drop return-to-office mandate. 21 February 2023. https://www.cnbc.com/2023/02/21/amazon-employees-push-ceo-andy-jassy-to-drop-return-to-office-mandate.html.

27. Paychex. Feeling the Burn(out): Exploring How Employees Overcome Burnout. 25 February 2019. https://www.paychex.com/articles/human-resources/impact-of-employee-burnout.

28. Proofpoint. 2022 Voice of the CISO: Global Insights Into CISO Challenges, Expectations and Priorities. May 2022. https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-voice-of-the-CISO-report.pdf.

29. PwC. 2022 Global Digital Trust Insights. December 2021. https://www.pwc.se/sv/pdf-reports/cybersecurity/cyber-global-digital-trust-insights-2022.pdf.

30. Rhysider, Jack. Darknet Diaries, Episode 68: Triton. June 2020. https://darknetdiaries.com/transcript/68/.

31. Rundle, James. “Economic Uncertainty Weighs on Cyber Chiefs.” Wall Street Journal 13 January 2023. https://www.wsj.com/articles/economic-uncertainty-weighs-on-cyber-chiefs-11673562985.

32. SAM. IoT Security Landscape Report. July 2022. https://securingsam.com/wp-content/uploads/2022/04/SAM_IOT-Security-Report.pdf.

33. SANDIA. Cybersecurity for Electric Vehicles Charging Infrastructure. July 2022. https://www.osti.gov/servlets/purl/1877784/.

34. Shackleford, Dave. SANS 2022 Cloud Security Survey. March 2022. https://8645105.fs1.hubspotusercontent-na1.net/hubfs/8645105/white-paper/sans-2022-cloud-security-survey.pdf.

35. Shumway, Emilie. Monster: Two-thirds of workers would quit if forced to return to the office five days a week. 26 September 2022. https://www.hrdive.com/news/monster-two-thirds-workers-would-quit-forced-back-to-office/632690/.

36. Smith, Ray A. Quiet Quitters Make Up Half the U.S. Workforce, Gallup Says. 29 September 2022. https://www.wsj.com/articles/quiet-quitters-make-up-half-the-u-s-workforce-gallup-says-11662517806.

37. Tsipursky, Gleb. The return to the office could be the real reason for the slump in productivity. Here’s the data to prove it. 16 February 2023. https://fortune.com/2023/02/16/return-office-real-reason-slump-productivity-data-careers-gleb-tsipursky/.

38. Vanson Bourne for Nutanix. Nutanix Enterprise Cloud Index: Application Requirements to Drive Hybrid Cloud Growth (2019 edition). November 2019. https://www.nutanix.com/content/dam/nutanix/resources/gated/analyst-reports/enterprise-cloud-index-2019.pdf.

39. Verizon. Mobile Security Index 2022. 2022 August 2. https://www.verizon.com/business/resources/reports/2022-msi-report.pdf.

40. Wei, Wang. Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer. 16 April 2018. https://thehackernews.com/2018/04/iot-hacking-thermometer.html.

41. Weissman, Cale Guthrie. Here’s Why Equifax Yanked Its Apps From Apple And Google Last Week. 15 September 2017. https://www.fastcompany.com/40468811/heres-why-equifax-yanked-its-apps-from-apple-and-google-last-week.

42. Wilson, Dan, et al. Market Guide for DEX Tools. 31 August 2022. https://www.gartner.com/doc/reprints?id=1-2B07Z49S&ct=220902&st=sb.

43. Yang, Mary. Elon Musk gives Twitter employees an ultimatum: Stay or go by tomorrow. 16 November 2022. https://www.npr.org/2022/11/16/1137105935/twitter-elon-musk-ultimatum.

# Der ultimative Leitfaden für Unified Endpoint Management

Wie sich moderne Endpoint-Management-Lösungen auf die Sicherheit und die Erfahrung der Mitarbeitenden auswirken

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com