Whitepaper

Unified Endpoint Management

Effektive Geräte-Sicherheit für die hybride Arbeitswelt

Leitfaden für IT-Entscheider:innen

vodafone business

Together we can

Vorwort

Laut Digitalverband Bitkom arbeitet jede:r zweite Beschäftige in Deutschland am Computer, Smartphone oder Tablet. Mit mobilen Geräten nehmen Mitarbeitende am kompletten Geschäftsprozess teil.

Für die IT-Mitarbeitenden bedeutet das Geräte-Management viel Arbeit. Eine Studie mit unserem Partner IDG Research zeigt: Homeoffice und Remote Work haben Mitarbeitende zur Zielscheibe von Hacker:innen und Cyber-Kriminellen gemacht. Denn sie nutzen kein geschütztes Firmen-Netzwerk. Und durch viele Gerätetypen, Betriebssysteme und Programme wird das Geräte-Management noch aufwändiger.

Sie wollen verschiedenste Geräte schützen und weniger Verwaltungsaufwand? Dann brauchen Sie ganzheitliche Ansätze und Tools. Alle Infos dazu bekommen Sie in diesem Whitepaper.

Alexander Saul
Geschäftsführer Firmenkunden
Vodafone Deutschland

Inhalt

Effektives Geräte-Management für die hybride Arbeitswelt

Insights aus der Studie von IDG Research und Vodafone

Security-Bilanz

56 % der Unternehmen berichten von einem **Anstieg der Hackerangriffe** auf Geräte von Homeoffice-Nutzer:innen, 16 % von einem starken Anstieg. [Seite 6]

43 % der Unternehmen haben durch Hackerangriffe auf Geräte **wirtschaftlichen Schaden** erlitten, bei fast 13 % war der Schaden massiv. [Seite 6]

Endpoint Security Management

66 % der Unternehmen übertragen die Verantwortung für die **Gerätesicherheit** ihrer IT- oder IT-Security-Abteilung, der Rest bevorzugt andere Unternehmensbereiche. [Seite 7]

62 % der Unternehmen sehen ihre Gerätesicherheit durch **Cloud-Dienste** gestärkt, 17% berichten von einer erheblichen Stärkung. [Seite 12]

63 % der Unternehmen nutzen zumindest teilweise einen **Managed Security Provider (MSSP)**, weitere 18 % haben das vor. [Seite 10]

Hybride Arbeit definiert Geräte-Management neu

Möglichkeiten schaffen Tatsachen. Starke Mobile Geräte und cloudbasierte Anwendungen haben Arbeit ortsunabhängig gemacht.

Mitarbeitende wollen von überall aus arbeiten – mit Geräten ihrer Wahl. Konzepte wie Bring Your Own Device (BYOD) und Choose Your Own Device (CYOD) sind in vielen Unternehmen Alltag.

Ein Zurück zu einheitlichen Arbeitsgeräten wird es nicht geben. Und auch keine Rückkehr zum Büro als einzigem Arbeitsort. Laut der Umfrage von Bitkom sehen 53 % der Mitarbeitenden ihre Zukunft überwiegend oder ausschließlich im Homeoffice. Unternehmen ohne flexible Arbeitsregelungen finden nur schwer Fachkräfte – und haben mehr Fluktuation bei den Mitarbeitenden.

Wichtig ist Mitarbeitenden auch ihre technische Ausstattung. Schlechte persönliche IT-Ausstattung ist der drittwichtigste Grund, ein Unternehmen zu verlassen. Das ergab eine Studie von Nexthink und Vanson Bourne. Mitarbeitende wollen, dass zukunftsfähige Unternehmen in eine moderne digitale Infrastruktur investieren.

Ihre IT braucht deshalb neue Möglichkeiten und Tools, um die komplexe Geräte-Infrastruktur zu verwalten – mit so wenig Aufwand und so viel Sicherheit wie möglich.

Geräte und ihre Integration

Sie können ein Gerät auf mehrere Arten in den Pool Ihres Unternehmens integrieren. Die 3 häufigsten sind:

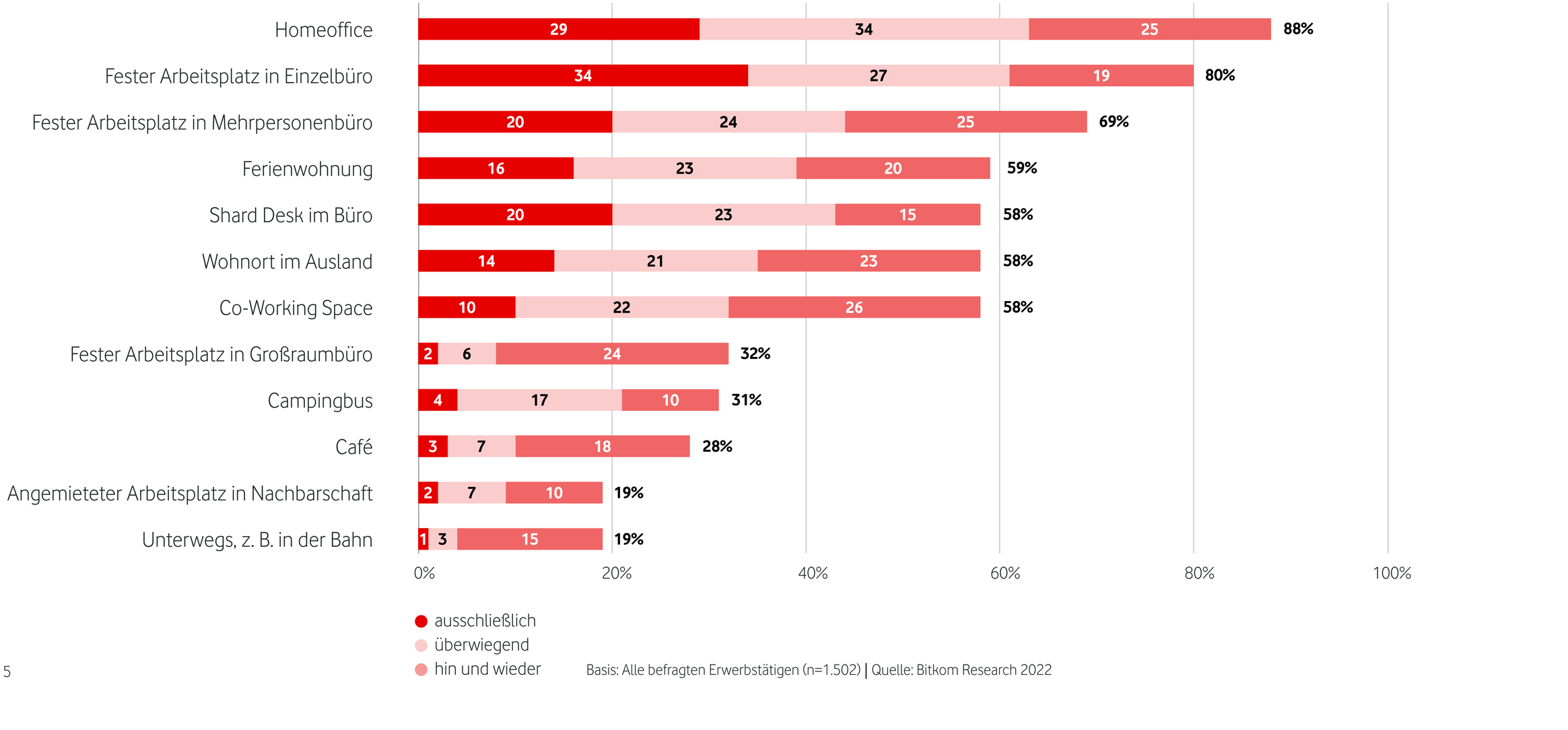
- **BYOD,** Bring your own device: Mitarbeitende dürfen ihre privaten Geräte beruflich nutzen. Die IT prüft die BYOD-Geräte auf Sicherheitsrisiken und gibt sie dann frei.

- **COBO,** Company-owned, business only: Das Unternehmen schafft die Geräte an. Sie sind dann nur für den beruflichen Gebrauch zugelassen. Die IT kümmert sich um die komplette Administration. Mitarbeitende dürfen das Gerät nicht privat nutzen.

- **COPE,** Company-owned, personally enabled: Das Unternehmen gibt den Mitarbeitenden Geräte aus einem hauseigenen Pool. Sie dürfen die Geräte privat nutzen – oft aber mit Einschränkungen.

9 von 10 Mitarbeitenden sehen ihre Zukunft im Homeoffice

An welchem Ort möchten Sie arbeiten?



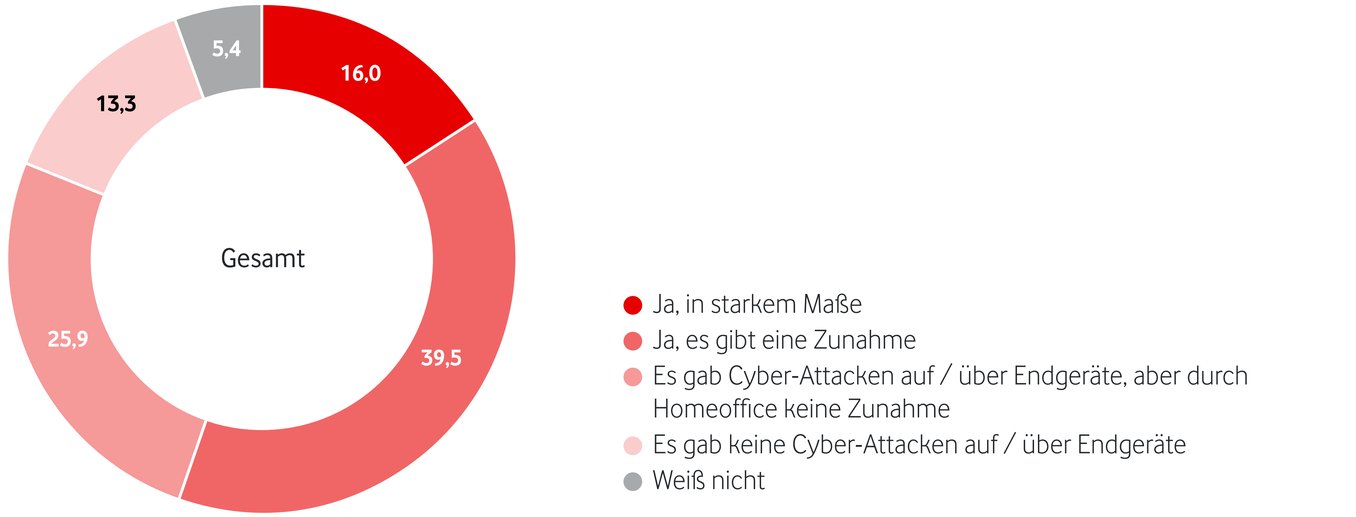
Basis: Alle befragten Erwerbstätigen (n=1.502) | Quelle: Bitkom Research 2022

Remote Worker im Visier von Hackerangriffen

Die Kehrseite der dezentralen Arbeitswelt ist spürbar. Fast 56 % der befragten IT- und Business-Verantwortlichen beobachten mehr Angriffe auf Geräte von Homeoffice-Nutzer:innen. 16 % sogar einen starken Anstieg. Das ist das Ergebnis der Studie Endpoint Security – die IDG zusammen mit uns durchgeführt hat (siehe Grafiken). 43 % der befragten Unternehmen erlitten durch solche Angriffe einen wirtschaftlicher Schaden. Für fast 13 % war der Schaden massiv.

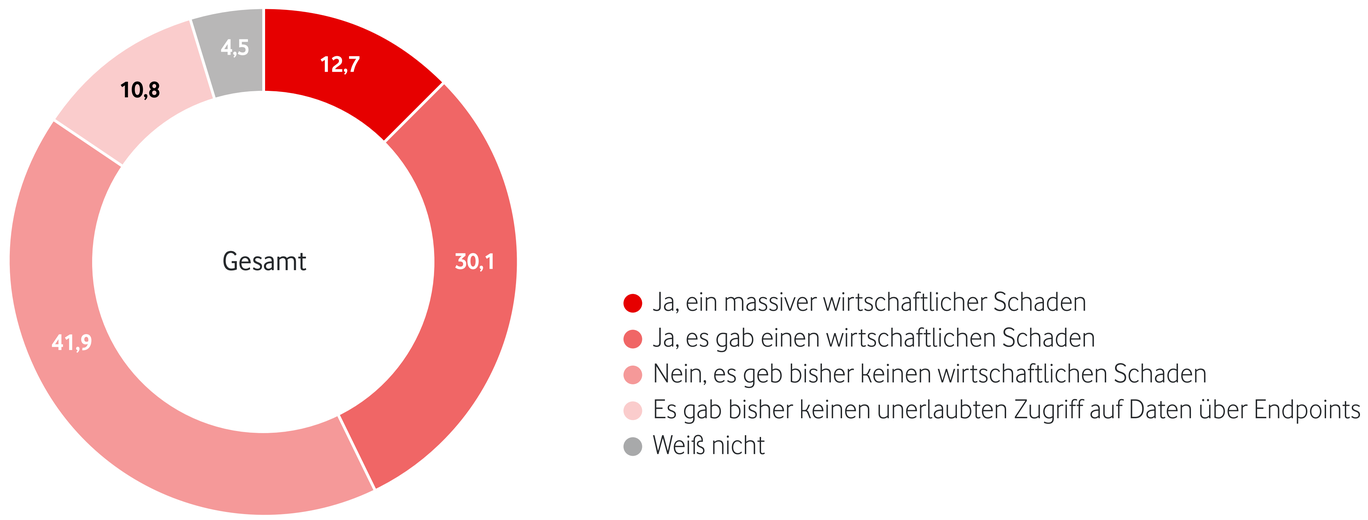
Registriert Ihr Unternehmen eine Zunahme von Attacken auf Endgeräte, seitdem Mitarbeitende vermehrt von Zuhause arbeiten?

Angaben in Prozent. Basis n = 332



Ist in Ihrem Unternehmen durch einen Cyber-Angriff über Endpoints schon einmal ein wirtschaftlicher Schaden entstanden?

Angaben in Prozent. Basis n = 332



Geräte-Management wird zur Top-Priorität der IT

Sichere und gut gemanagte Geräte sind für die IT eine Top-Priorität. So minimieren Sie die Risiken von Remote Work. Deshalb steigen die Budgets für IT-Security. Das zeigt eine aktuelle Umfrage des CIO. Die Geräte lassen sich nicht mehr rein manuell verwalten. Dafür haben Unternehmen zu viele und zu unterschiedliche Geräte. Auch ältere Lösungen für das Mobile Device Management (MDM) reichen selten aus.

Zum Glück ist der Markt für Geräte-Management und Endpoint Security rund um Anbieter wie Microsoft, Ivanti oder VMware innovativ und dynamisch. Sein aktuelles Volumen liegt zwischen 2 und 4,5 Milliarden US-Dollar. Und für die nächsten 5 Jahre sagen Expert:innen mehr als 30 % Wachstum voraus. Laut einer aktuellen Forrester-Umfrage wollen 28 % der Unternehmen in ihr Geräte-Management (UEM) investieren.

Wer in Ihrem Unternehmen ist federführend verantwortlich für Endpoint Security?

	Gesamt	Mittelstand	
Geschäftsführer/CEO	11,4 %	4,1 %	
COO/CFO/ kaufmännische Leitung	7,2 %	10,8 %	
CTO/ Technik-Vorstand	11,7 %	13,5 %	
CIO / CDO / IT-Vorstand	33,7 %	43,2 %	IT-Funktionen
Administrator	9,0 %	6,8 %	
CISO / CSO	5,4 %	5,4 %	
Security-Manager	17,8 %	16,2 %	

Nur in 66 % der befragten Unternehmen verantworten die IT oder spezielle Security-Funktionen die Gerätesicherheit. Im Mittelstand mit 500 bis 999 Mitarbeitenden sind es immerhin 71 %. Und immer mehr Unternehmen übertragen die Aufgabe an die IT. Denn Geräte-Management ist komplex und Tools dafür werden immer besser.

Quelle: IDG-Studie "Endpoint Security 2022"

Eine Verwaltung für alle Devices

Die meisten Tools zur Geräte-Verwaltung kommen aus dem Mobile Device Management, MDM. Mit dieser Software verwalten Sie Smartphones. Denn Handys haben eigene Betriebssysteme und werden anders genutzt als Computer. Deshalb brauchen sie auch spezielle Software-Suiten: MDM für die Verwaltung der Geräte – und MAM, Mobile Application Management, für den Zugriff auf Anwendungen Ihres Unternehmens.

Längst sind auch Notebeooks üblich in Unternehmen. Und Mitarbeiter:innen arbeiten nicht mehr nur im Büro. Deshalb verwalten Sie mit den Tools auch Windows-, macOS- und Linux-Rechner. Dazu kommen neue Security-Funktionen. Damit können Sie auch auch auf Business-Anwendungen zugreifen. Diese Art von Software für das einheitliche Geräte-Management heißt **Unified Endpoint Management, UEM**. Sie dominiert heute das Geräte-Management und läuft meistens über eine Cloud.

Die Entwicklungsstufen von MDM, EMM und UEM

Enterprise Mobility Management (EMM)

Mobile Device Management (MDM)

für Tablets und Smarphones: Gerätemanagement, Anbindung an Mailserver und Cybersecurity (Sicherheitsfunktionen).

Mobile Application Management (MAM)

Verwaltet automatisch Software des Unternehmens. Und stellt sie im App Store bereit.

Unified Endpoint Management (UEM)

- Weiterentwicklung und Erweiterung von EMM
- Alle Dienste plattformübergreifend und einheitlich für mobile und Desktop-Geräte (Unified-Ansatz)
- Alle Endgeräte-Dienste auch für „Bring Your Own Device“ (BYOD) verfügbar.

Quelle: IDG-Studie ”Endpoint Security 2022”

Vorteile von Unified Endpoint Management

Was UEM leistet

- Richtet Betriebssysteme und Anwendungssoftware automatisch ein
- Inventarisiert Ihre Geräte und die installierte Software
- Sie verwalten Software-Lizenzen und Mobilfunk-Verträge zentral
- Installiert Updates und Patches automatisch auf allen Geräten
- Onboarding und Offboarding neuer Mitarbeiter:innen – mit personalisierten Geräten, Passwörtern und Zugriffsrechten
- Schützt Geräte gegen Diebstahl, z.B. über Geofencing
- Sie können Ihre Geräte per Fernzugriff überwachen und deaktivieren
- Ihr Support kann remote auf die Geräte zugreifen
- Sichert Daten und stellt sie bei Schäden automatisch wieder her

Wie die IT von UEM profitiert

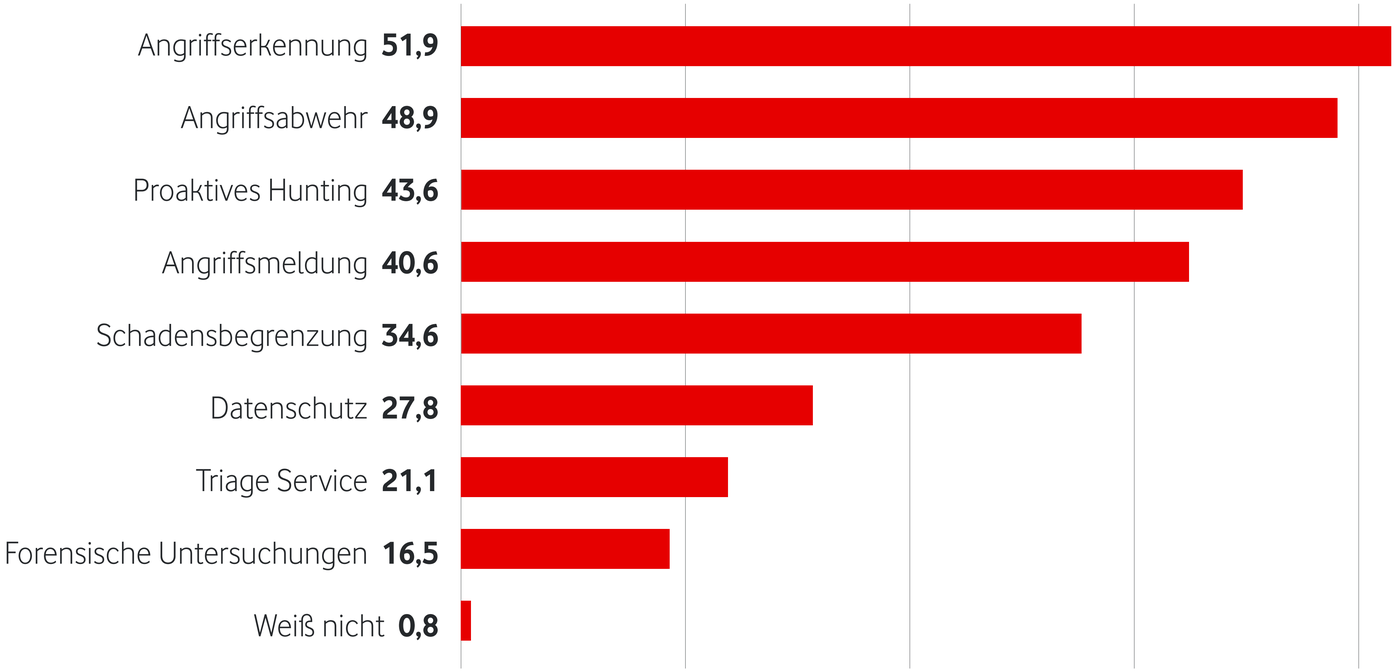
- Arbeit ist flexibler geworden. Deshalb brauchen Sie eine Methode, mit der Sie Geräte einfach verwalten können – und bei der Ihre IT wenig Support leisten muss
- Das Konsolidieren von Endpoint Management und Endpoint Security führt zu zusätzlichen Effizienzen im Geräte-Management.
- In das Endpoint Management sind Digital Experience Tools integriert. So analysieren Sie, wie nutzerfreundlich und effizient Ihre Geschäftsprozesse und Anwendungen sind.
- Analysieren Sie, wie benutzerfreundlich und effizient Ihre Geschäftsprozesse sind – mit Digital Experience Tools, die sie ins Endpoint Management integrieren.
- Viele IT-Prozesse und -Aufgaben des Geräte-Managements laufen automatisch. Ihre IT muss keine Routineaufgaben mehr erledigen – und Sie sparen beim IT-Budget.

Geräte-Management und -sicherheit als Dienstleistung

Geräte-Management wird immer komplexer – und viele IT-Abteilungen haben nur knappe Ressourcen. Trotzdem wollen Ihre Mitarbeitenden flexibel arbeiten und brauchen sichere Geräte. Deshalb übertragen immer mehr Unternehmen das Geräte-Management komplett an externe Partner.

Was genau haben Sie an einen Dienstleister ausgelagert?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, die Endpoint Security teilweise oder komplett an einen Dienstleister ausgelagert haben. Basis n = 133

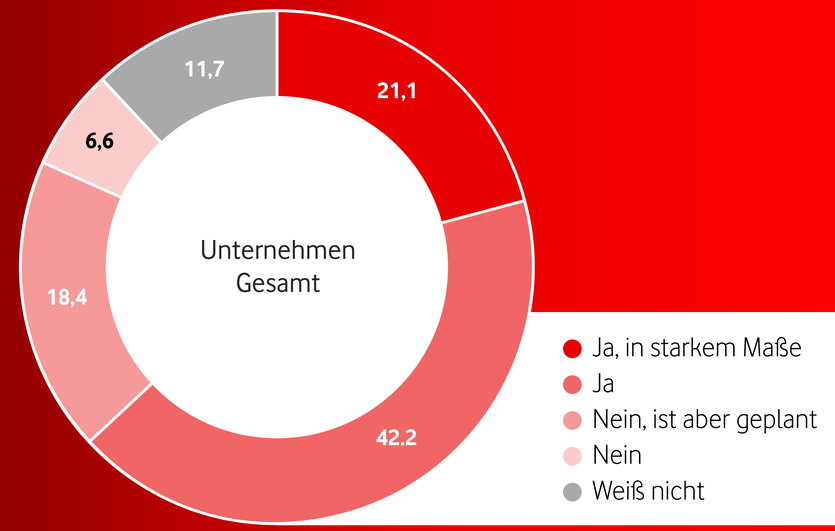


Die meisten Unternehmen nutzen schon Security Services. Die populärsten kümmern sich um Angriffserkennung und -abwehr.

Quelle: IDG-Studie „Endpoint Security 2022“

Nutzt Ihr Unternehmen selbst und/oder Ihr Managed Security Service Provider (MSSP) cloudbasierte Komponenten zur Sammlung und Auswertung der Sicherheitsvorfälle bzw. zum Schutz der Endpoints?

Angaben in Prozent. Basis n = 332



In der Endpoint Security verlagert sich der Schwerpunkt in Richtung Services und Software-as-a-Service.

Quelle: IDG-Studie „Endpoint Security 2022“

Die populärsten UEM-Lösungen

BlackBerry Spark

Mit der Spark Suite von BlackBerry bekommen Sie starkes Unified Endpoint Management – mit Unified Endpoint Security für Android, ChromeOS, iOS, macOS und Windows. Verwalten Sie Geräte je nach Eigentumsmodell, Anwendergruppe oder Betriebssystem. Mit Blackberry Edit bekommen Sie außerdem einen Editor für Office-Dokumente und einen Viewer für PDF-Dokumente. Zum Paket gehört auch ein Unternehmens-Messenger. Damit kann Ihre IT Mitarbeitende per SMS, Telefon und E-Mail z.B. über Wartungstermine informieren – oder bei Problemen Support anbieten.

Microsoft Intune-Produktfamilie

Intune verwaltet den Benutzerzugriff und vereinfacht die App- und Geräteverwaltung auf Ihren Geräten – einschließlich mobiler Geräte, Desktopcomputer und virtueller Endpunkte. Mit der Lösung integrieren Sie nahtlos viele Microsoft-Dienste. Z.B. Microsoft 365, Configuration Manager, Windows Autopilot und Microsoft Defender for Endpoint. Die Verwaltung von Endpunkten, die lokal, virtualisiert, in der Cloud sowie auf Mobilgeräten und dem Desktop eingesetzt werden, auf Plattformen wie Windows-, Mac-, iOS-, Android- und Linux-Betriebssystemen, wird unterstützt.

VMware Workspace ONE UEM

Der Marktführer für Virtualisierungssoftware hat sein VMware Workspace ONE UEM für physische Geräte und fürs Management virtueller Desktops ausgelegt. Ein Schwerpunkt der Lösung sind auch Rugged Devices – also Geräte für den Einsatz in schwierigen Arbeitsumgebungen. Mit VMware Workspace ONE bekommen Sie auch Single Sign-on, Remote Support, Remote Access, Endpoint. Die Software unterstützt Android, ChromeOS, iOS, Linux, macOS und Windows 10.

Ivanti Neurons UEM

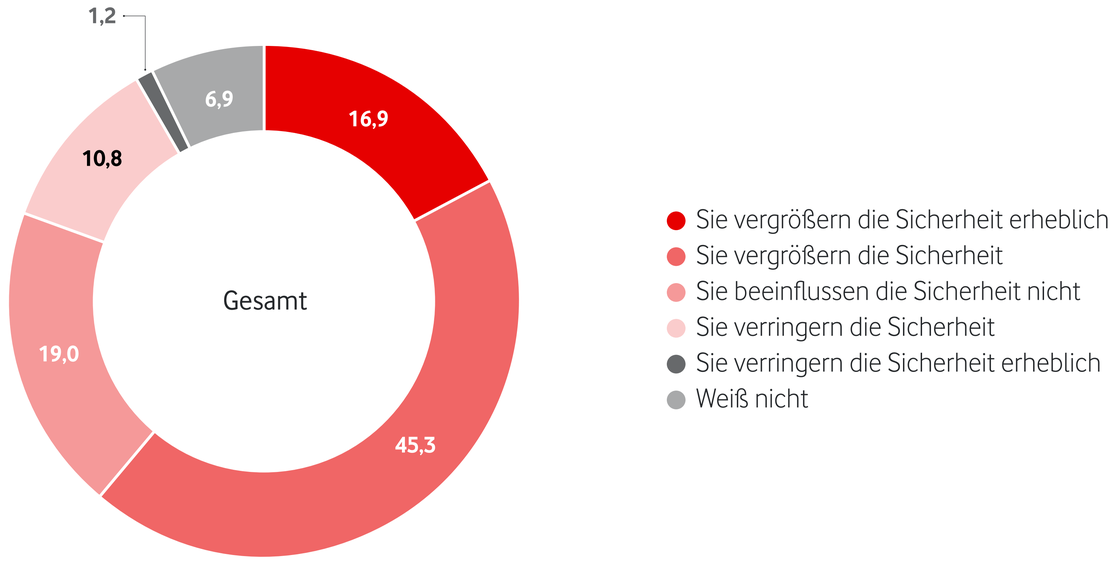
Bei Neurons steht die Zero Trust-Philosophie im Vordergrund. Das heißt, dass sich Anwendende bei jedem Zugriff auf Anwendungen und Daten authentifizieren müssen – auch innerhalb des Firmennetzes. Mit Neurons Tunnel greifen sie mit fast jedem Betriebssystem auf eine VPN-Infrastruktur zurück. Und mit AppConnect SDK und App Wrapper führen Sie mobile Apps in Software-Containern aus. Über die Ivanti Neurons Plattform können Administrator:innen die Digital Employee Experience (DEX) nachvollziehen. MobileIron UEM unterstützt Android, iOS, MacOS und Windows.

Samsung Knox Manage

Mit Samsung Knox Manage bekommen Sie Mobile Device Management für Geräte mit Android-, iOS-, Windows 10- oder Windows 11-Betriebssystemen. Knox Manage nutzt ein cloudbasiertes Command Center. Damit können IT-Administrator:innen fast 300 verschiedene Unternehmensrichtlinien durchsetzen. Der Knox Manage Cloud Connector kann über einen sicheren K anal Daten zwischen Unternehmenssystem und dem Cloud Server von Knox Manage übertragen. Zum Paket gehört auch eine Zertifizierungsstelle. Sie authentifiziert Geräte und Benutzer:innen im WLAN, VPN, beim Exchange-Server und anderen Anwendungen. Mit einem LDAP-Dienst greifen Sie außerdem auf Verzeichnisdienste wie Active Directory zu.

Wie beeinflusst der Einsatz von Cloud Services die Sicherheit von Netzen und Systemen in Ihrem Unternehmen?

Angaben in Prozent. Basis n = 332



Securitybezogene Cloud-Services machen IT-Systeme inklusive Geräte sicherer. Das bestätigt die Mehrheit der befragten IT- und Business-Entscheider:innen in der IDG-Studie.

Quelle: IDG-Studie „Endpoint Security 2022“

3 Tipps zur Auswahl der richtigen UEM-Plattform

Funktionsumfang: Die Plattform sollte alle Hardware-Typen, Betriebssysteme, Bereitstellungsmodelle, Einstellungen und Richtlinien abdecken, die Sie nutzen – oder noch nutzen könnten. Außerdem sollte die Plattform so funktionieren, dass sie keine weiteren Tools brauchen.

Security-Features: Die UEM-Plattform sollte alle Sicherheitseinstellungen der Geräte verwalten können. Automatische Routinen erleichtern Ihrer IT die Arbeit und sparen Geld. So können Sie z.B. automatisch Updates aufspielen. Außerdem sollten Sie mit der Plattform spezielle Security-Tools in die Verwaltung integrieren können.

Monitoring & Analyse: Die Analyse der digitalen Erfahrung der Mitarbeitenden (Digital Employee Experience, DEX) ist eine neue Disziplin. Und sie reicht weit über das Thema Benutzerfreundlichkeit hinaus. Mit DEX-Funktionen oder der Integration von DEX-Tools sammeln Sie wertvolle Erkenntnisse. Sie erfahren mehr darüber, wie Ihre Mitarbeitenden Geräte nutzen – und verbessern dadurch Ihre Prozesse.

Komplementäre Security-Lösungen für UEM

IT-Sicherheit entwickelt sich sehr dynamisch. Deshalb sollten Sie eine Extra-Lösung für Endgeräte-Sicherheit an die UEM-Plattform koppeln.

Microsoft Defender for Business

Eine Endpoint-Security-Lösung für kleine und mittelständische Unternehmen mit bis zu 300 Mitarbeitenden. Sie schützt Geräte mit Windows, macOS, iOS und Android vor Schadsoftware, Ransomware, Phishing und anderen Bedrohungen. Defender for Business ist Teil von Microsoft 365 Business Premium. Sie bekommen es aber auch als eigenständiges Abonnement. Und Sie können es unabhängig vom Microsoft Endpoint Manager einsetzen.

Lookout Mobile Endpoint Security

Eine Mobile Threat Defense-Lösung, die Sie zusätzlich zum jeweiligen EMM- oder UEM-System einsetzen. Sie beurteilt für Sie Risiken für iOS- und Android-Geräte. Die Einschätzungen gibt sie an das EMM/UEM-System weiter. Das setzt dann spezielle Richtlinien um. Bei einer Gefahrenlage kann es den Zugriff auf Unternehmensressourcen unterbinden. So können nur autorisierte Benutzer:innen auf für sie bestimmte Daten zugreifen.

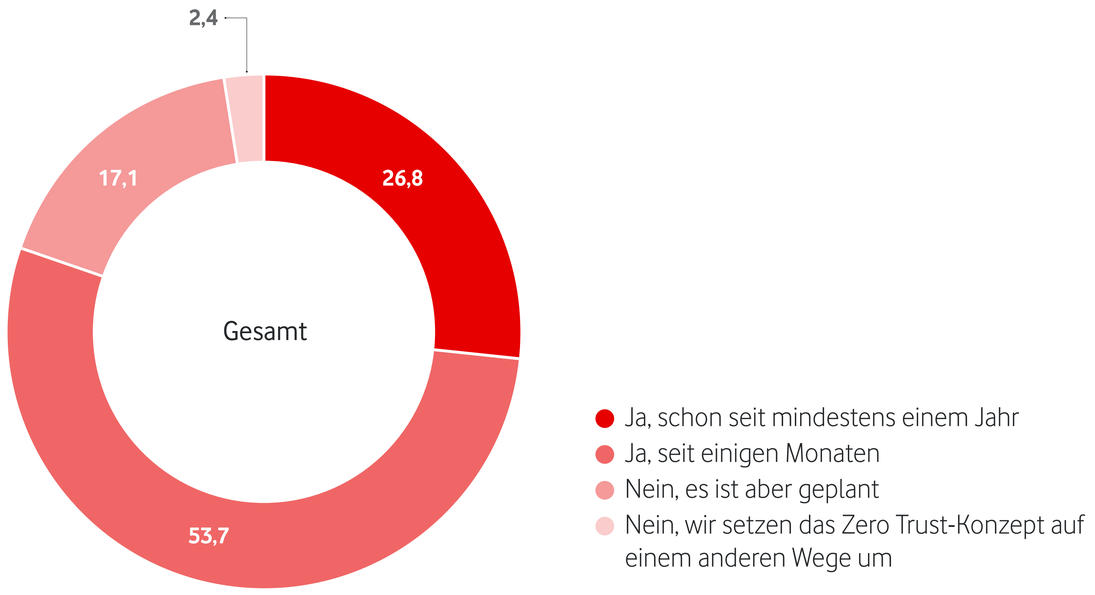
Das Zero Trust-Prinzip

Moderne Security-Infrastrukturen funktionieren nach dem Zero Trust-Prinzip. Nutzer:innen wird nicht pauschal vertraut – Sie haben also über Ihren Log-in nicht Zugriff auf alle Ressourcen. Stattdessen können Mitarbeitende nur Anwendungen und Daten nutzen, die sie für ihre Arbeit brauchen – unabhängig davon, ob die Anwendung in der Cloud oder vom Unternehmensnetz bereitgestellt wird.

Mehr Infos zum Zero Trust-Prinzip finden Sie in unserem Cloud Security Whitepaper. ▶

Setzen Sie im Kontext Endpoint Security auch eine dezidierte Zero Trust-Plattform ein?

Angaben in Prozent. Filter: Unternehmen, die ein Zero Trust-Konzept anwenden. Basis n = 42



Die größte Sicherheit bekommen Sie mit UEM-Tools durch eine Kombination mit Security-Software für mobile Geräte. Diese Software sollte das Zero Trust-Prinzip nutzen.

Quelle: IDG-Studie „Endpoint Security 2022“

UEM als Rundum-sorglos-Paket von Vodafone

Bei uns bekommen Sie umfassenden Service. Wir beraten Sie herstellerunabhängig, um für Sie das beste Produkt zu finden – und unterstützen Sie, bis Ihre Lösung funktioniert. Denn durch unser großes Partnernetzwerk übernehmen wir auch Installation und Migration. Auch im Lifecycle begleiten unsere Expert:innen Ihre Mitarbeitenden und Administrator:innen.

Verwalten Sie Ihre Geräte zentral

Steigern Sie die Produktivität nachhaltig

Legen Sie den Umfang von Sicherheit selbst fest

Mehr Infos im Web: www.vodafone.de/UEM

Über die Studie Endpoint Security

Für die Studie Endpoint Security 2022 wurden 332 IT-Entscheider: innen in der DACH-Region interviewt. Darunter waren strategische Entscheider:innen im C-Level-Bereich und den Fachbereichen – sowie Entscheider:innen und Spezialist:innen aus dem Bereich IT.

Die Stichprobe stammt aus der IT-Entscheider-Datenbank von IDG Business Media sowie zur Erfüllung von Quotenvorgaben aus externen Online-Access-Panels. Sie umfasst alle Branchen.

Verteilung der Stichprobe nach Unternehmensgröße

Weniger als 100 Beschäftigte:	4,2 %
100 bis 499 Beschäftigte:	28,0 %
500 bis 999 Beschäftigte:	22,3 %
1.000 bis 9.999 Beschäftigte:	30,4 %
10.000 Beschäftigte und mehr:	15,1 %

Erhebung: Die Befragung umfasst über 332 abgeschlossene und qualifizierte Interviews in der Zeit von 4. bis 11. Februar 2022. Die persönlichen Einladungen zur Umfrage kamen per E-Mail.

Fragebogenentwicklung: IDG Research Services in Abstimmung mit den Studienpartnern.

Lesen Sie auch: das Cyber Security-Whitepaper

Cyberattacken sind die wohl am schnellsten wachsende Bedrohung für Unternehmen. Und die möglichen Schäden sind gewaltig.

Deshalb brauchen Unternehmen ein starkes und unkompliziertes Konzept für **Cyber Security**.

Mit dem Whitepaper bekommen Sie:

- Komprimiertes Know How zu den Kernbereichen von Cyber Security
- Aktuelle Studienergebnisse zu entstandenen Schäden in Unternehmen
- Insights zu Angriffen von Hacker:innen und ihren Einfallstoren.
- Praxistipps für Schutzkonzepte in Unternehmen

Jetzt downloaden:

vodafone.de/**whitepaper-cyber-security**