Best Practices für ein einfaches, sicheres Endgerätemanagement

Mobile Produktivität für Ihr Unternehmen.
Wahlfreiheit für Ihre Mitarbeiter.
Umfassende Sicherheit und Kontrolle
für die IT.

Die Wahlfreiheit von Mitarbeitern ist zu einem Grundpfeiler moderner IT-Strategien geworden. Indem Organisationen es ihren Mitarbeitern erlauben, die besten Endgeräte für ihre Bedürfnisse zu wählen, können sie die Produktivität und Flexibilität und sogar die Zufriedenheit bei der Arbeit erhöhen. Mit der richtigen Strategie kann die IT passende Richtlinien und Technologien implementieren, um Unternehmensdaten zu schützen. Gleichzeitig werden Kosten verringert und ein erstklassiger Benutzerkomfort sichergestellt.

Ihre Strategie sollte Ihrer Organisation folgende Vorteile bieten:

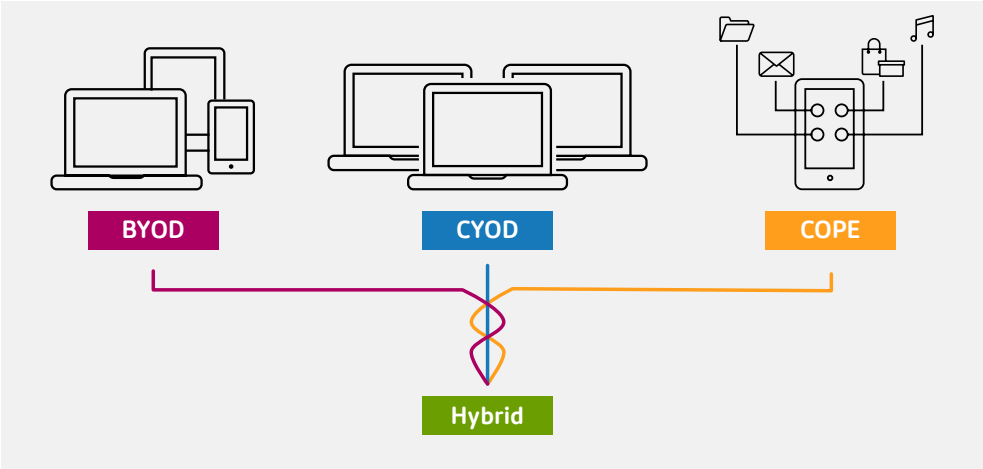
- **Ermöglichen Sie Mitarbeitern**, auch eigene Endgeräte zu nutzen, um so Produktivität, Zusammenarbeit und mobiles Arbeiten zu verbessern.
- **Schützen Sie vertrauliche Informationen** vor Verlust und Diebstahl unter Einhaltung von Sicherheitsstandards, einschließlich Datenschutz, Compliance und Risikomanagement.
- **Reduzieren Sie Kosten und Administrationsaufwand** durch Benutzer-Self-Service und automatisiertes Management und Monitoring.
- **Vereinfachen Sie die IT** mit einer zentralen, umfassenden Lösung für das sichere Management von Daten, Apps und Endgeräten.

Hier sind acht Best Practices zur Entwicklung einer Strategie, die Mitarbeitern das Arbeiten erleichtert und der IT effektive Sicherheits-, Kontroll- und Managementfunktionen bietet:

1. Auswahl einer Richtlinie

Im Zuge des Wandels, den die IT aufgrund von Mobility und Konsumerisierung erlebt, wurden mehrere Richtlinien entwickelt, die die Wahlfreiheit mit einer gesteigerten Kontrolle für die IT verbinden:

- Bring-Your-Own-Device (BYOD): Mitarbeiter können private Endgeräte für die Arbeit nutzen.
- Choose-Your-Own-Device (CYOD): Das Unternehmen bietet Mitarbeitern eine Reihe von Endgeräten zur Auswahl. Diese können sich für ein Endgerät entscheiden, das sie für die Arbeit verwenden.
- Corporate Owned, Personally Enabled (COPE): Mitarbeiter dürfen ein Endgerät aus einer vom Unternehmen genehmigten Liste auswählen und anschließend private sowie geschäftliche Apps darauf installieren.
- Hybrider Ansatz: Es können mehrere Strategien gleichzeitig genutzt werden, um verschiedenen Anwendern und Gruppen das jeweils beste Mobility-Erlebnis zu bieten. Beispielsweise kann COPE gleichzeitig mit CYOD oder BYOD genutzt werden.



Die genauen Details der einzelnen Richtlinien können variieren, jedoch sind die grundlegenden Prinzipien des zentralen Endgerätemanagements (Unified Endpoint Management, UEM) bei allen gleich. Dies gilt auch für ihre Auswirkungen auf die Sicherheit. Die größten Unterschiede gibt es bezüglich der Kosten.

BYOD-Nutzer bezahlen für ihre eigenen Endgeräte und Datentarife. Dafür werden sie in manchen Fällen teilweise oder vollständig vom Unternehmen vergütet. Im Falle von COPE und CYOD bezahlt das Unternehmen für das Endgerät und die Datennutzung. Eine BYOD-Richtlinie muss zudem weitere Faktoren außerhalb des Rahmens von COPE und CYOD berücksichtigen, z. B. ob Mitarbeiter einen Überstundenzuschlag für das Abrufen von E-Mails außerhalb der Arbeitszeiten oder am Wochenende erhalten sollten.

2. Gültigkeit und Registrierung

Sie sollten klar kommunizieren, wer persönliche Endgeräte nutzen darf und ob dies eine kurzfristige Nutzung zur Ergänzung des unternehmenseigenen Endgeräts, ein dauerhafter Ersatz für ein unternehmenseigenes Endgerät oder eine Kombination dieser beiden Optionen sein soll. Dies kann als Privileg angesehen werden, für das man sich qualifizieren muss, als Reaktion auf einen Mitarbeiterwunsch, als Anforderung für bestimmte Benutzerrollen, als zu großes Risiko für einige wenige Anwendungsbereiche oder aber sehr wahrscheinlich als eine Kombination aus diesen Punkten.

Eine Möglichkeit, die jeweils geeignete Strategie zu wählen, ist die Anwendung von Kriterien, wie zum Beispiel Mitarbeitertyp, Reisetätigkeit, Leistung oder die Frage, ob ein Mitarbeiter Offline-Zugriff auf vertrauliche Daten benötigt. Die Teilnahmevoraussetzungen werden zwar auf breiter Basis ermittelt, die Vorgesetzten sollten jedoch grundsätzlich das letzte Wort haben, wenn es darum geht, welche Teammitglieder einen Zuschuss erhalten sollten. Manager können zudem angewiesen werden, BYOD, COPE oder CYOD im Kontext mit anderen Incentives, Privilegien und Motivationsmaßnahmen auf Abteilungsebene einzuführen.

Externe Auftragnehmer sind in der Regel optimale Kandidaten für BYOD. Viele Organisationen erwarten bereits von ihren externen Auftragnehmern, dass diese ihre eigenen Endgeräte mitbringen, und sehen dies auch als Teil ihrer Compliance-Richtlinien.

3. Unterstützte Endgeräte

Ihr Unternehmen kann eine begrenzte Anzahl an Endgerätetypen genehmigen, um eine nicht mehr zu managende Vielfalt an Endgeräten zu verhindern. Es hängt von den Anforderungen der Anwender, möglichen Sicherheitsrisiken und verfügbaren Support-Ressourcen ab, wie granular Sie diese Richtlinien gestalten müssen. Je granularer Ihre Richtlinie bezüglich der Anzahl von Endgerätetypen, Betriebssystemversionen und Modellen ist, desto mehr Ressourcen benötigen Sie grundsätzlich, um alle spezifizierten Endgeräte angemessen zu testen und zu unterstützen.

Um klare Besitzverhältnisse zu wahren, sollten BYOD-Teilnehmer ermuntert werden, ihre privaten Endgeräte selbst zu erwerben, anstatt diese über die Einkaufsabteilung des Unternehmens zu bestellen. Gegebenenfalls können Mitarbeiterrabatte weitergegeben werden, wenn diese über die Unternehmenslieferanten verfügbar sind.

Einige Mitarbeiter möchten eventuell zusätzliche Peripheriegeräte erwerben, wie z. B. Monitore oder Tastaturen. In diesem Fall sollten Sie eindeutig festlegen, wer diese erwirbt und das Eigentum daran hält.

4. Implementierung

Die richtige Kommunikation ist wichtig für eine erfolgreiche Implementierung. Unterstützen Sie Anwender bei ihrer Entscheidung für oder gegen eine Teilnahme am Programm und bei der Auswahl des richtigen Endgeräts für ihre Bedürfnisse. Sie sollten zudem verstehen, wie auf Daten zugegriffen werden kann, wie und wo Daten gespeichert werden und wie ungemanagte Apps und Services aus dem Consumerbereich für geschäftliche Aufgaben genutzt werden können.

Arbeits- und Unternehmensdaten sollten streng getrennt gehalten werden, um die Anforderungen an E-Discovery und die Richtlinien zur Datensicherung einzuhalten. Analog dazu dürfen berufliche E-Mails niemals von privaten Accounts versendet werden. Eine Nutzungsrichtlinie sollte für private BYO-Endgeräte in demselben Umfang gelten wie für unternehmenseigene Endgeräte.

Es ist zudem wichtig, ein Programm für neue Teilnehmer einzuführen, das sie beim Einstieg und bei der Nutzung unterstützt. Eine Willkommens-E-Mail mit einem Link zu einem Self-Service-Portal hilft Anwendern dabei, schneller produktiv arbeiten zu können.

5. Kostenteilung

Die Kostenreduzierung ist eines der Hauptvorteile von BYOD, da Anwender einen Teil oder die gesamten Kosten für die im Unternehmen genutzten privaten Endgeräte übernehmen. Wenn Unternehmen einen Zuschuss bieten, beträgt dieser üblicherweise 18 bis 20 Prozent der Kosten für das Endgerät. Die Teilnehmer sollten sich darüber im Klaren sein, dass der Zuschuss steuerlich wie ein Einkommen behandelt wird. In Gegenden mit höheren Einkommenssteuersätzen empfiehlt es sich gegebenenfalls, den Zuschuss entsprechend zu erhöhen, um die Höhe des Nettozuschusses für alle Teilnehmer gleich zu halten.

Sollten Sie sich für die Zahlung eines Zuschusses entscheiden, sollte dieser die vollständige Nutzungsdauer der einzelnen Teilnehmer berücksichtigen. Zuschüsse sollten in regelmäßigen Abständen verlängert werden, um so sicherzustellen, dass die Geräte nicht älter werden als dies für ein unternehmenseigenes Endgerät der Fall wäre. Sollte ein Teilnehmer das Unternehmen während eines BYOD-Zyklus verlassen, können Sie gegebenenfalls einen Teil des Zuschusses zurückfordern.

Eine Kostenteilung hat Auswirkungen auf die Einführung eines BYOD-Programms in die Organisation. Eine organisationsweite Einführung kann eine Kostensteigerung zur Folge haben, da sich auch Mitarbeiter anmelden und Zuschüsse beantragen, deren Endgeräte das Ende des Nutzungszyklus noch nicht erreicht haben. Wird das Programm Mitarbeitern erst dann angeboten, wenn ihre Endgeräte ersetzt werden müssen, verteilen sich die Aufwendungen. Jedoch können Organisationen, die keinen Zuschuss zahlen, bereits ab dem ersten Tag alle Mitarbeiter zu dem Programm einladen.

Jede BYOD-Richtlinie, mit oder ohne Kostenteilung, sollte zudem eindeutig festlegen, wer für Netzwerkzugriffe außerhalb der Unternehmens-Firewall zahlt, unabhängig davon, ob es sich um ein Mobilfunk-, ein öffentliches Wi-Fi- oder ein privates Breitbandnetz handelt.

6. Sicherheit und Compliance-Überwachung

Es ist sowohl für private als auch unternehmenseigene Endgeräte wichtig, dass Daten geschützt werden und der Benutzerkomfort dabei nicht beeinträchtigt wird. Programme, die private Anwendungen und Daten auf Endgeräten erlauben, die für die Arbeit genutzt werden, können mithilfe des Managements mobiler Anwendungen (Mobile Application Management, MAM) private und Unternehmens-Apps sowie zugehörige Daten von Unternehmensinhalten getrennt halten.

Die Installation von Unternehmens-Apps auf privaten Endgeräten erhöht das Risiko. Wenn Sie jedoch eine Strategie haben, die UEM, Anwendungs- und Desktopvirtualisierung sowie sicheren Dateiaustausch kombiniert, ist dies nicht notwendig. Unternehmensdaten verlassen niemals das Rechenzentrum bzw. die Cloud und bleiben daher geschützt. Müssen Unternehmensdaten auf dem mobilen Endgerät gespeichert werden, können Unternehmensdaten durch Container, Verschlüsselung und die Option zur Remote-Löschung geschützt werden. Außerdem können Sie die Druckfunktion oder den Zugriff auf clientseitige Laufwerke und USB-Speicher deaktivieren.

Sie können den Zugriff auf Apps und Daten mithilfe von Richtlinien, die den Eigentumsstatus, den Mitarbeiterstatus oder den aktuellen Standort überprüfen, kontrollieren, absichern und managen. Sie können jedes Endgerät zulassen und managen, Passwortrichtlinien festsetzen und Endgeräte mit Jailbreak erkennen. Zudem können Sie eine vollständige oder teilweise Löschung auf Endgeräten durchführen, die die Compliance nicht erfüllen, verloren oder gestohlen wurden oder einem Mitarbeiter oder externen Auftragnehmer gehören, der nicht mehr für das Unternehmen tätig ist. Die Anwendungssicherheit wird durch den geschützten Anwendungszugriff über App-Tunnel, Blacklists, Whitelists und dynamische, kontextabhängige Richtlinien gewährleistet.

Zum Schutz des Unternehmensnetzwerks können Sie die NAC-Technologie (Netzwerkzugriffskontrolle) zur Authentifizierung von Anwendern einsetzen, die sich mit dem Netzwerk verbinden. Dadurch prüfen Sie, ob sie aktuelle Antivirussoftware und Sicherheits-Patches installiert haben.

Außerhalb der Firewall können durch Virtualisierung und Verschlüsselung ein Großteil der Sicherheitsschwachstellen von Wi-Fi, WEP-Verschlüsselung, Open Wireless, 3G/4G und anderen Zugriffsmethoden beseitigt werden. Netzwerksicherheitsfunktionen bieten Transparenz und Schutz vor internen und externen mobilen Bedrohungen, erlauben das Sperren von nicht legitimen Geräten, nicht autorisierten Benutzern und nicht kompatiblen Apps sowie Integration in SIEM (Security Information and Event Management) Systeme.

Für den Fall, dass ein Teilnehmer am BYOD-Programm die Organisation verlässt, gegen die jeweilige Richtlinie verstoßen wird oder sein persönliches Endgerät abhanden kommt, sollte die IT über Mechanismen für die sofortige Sperrung des Zugriffs auf Daten und Apps verfügen. Dazu gehört auch die automatische Sperrung von beruflich genutzten SaaS-Konten und die selektive Löschung verloren gegangener Endgeräte. Diese Funktionen sind zudem für Endgeräte in einem COPE- oder CYOD-Programm notwendig. Durch sie können unternehmenseigene Endgeräte an neue Nutzer weitergegeben werden, ohne dass darauf gespeicherte Daten in die Hände einer nicht autorisierten Person fallen.

Anstelle eines offenen BYOD-Programms, mit dem jedes Endgerät für den Zugriff auf Unternehmens-Apps und Daten verwendet werden kann, entscheiden sich einige Organisationen für einen gemanagten Ansatz. In diesem Szenario managt die IT private Endgeräte direkt, einschließlich Registrierung, Validierung, Autorisierung und Zugriff auf Geräteressourcen.

7. Monitoring und Management

Ein durchgehendes Monitoring und Management sind erforderlich, um Richtlinien zuverlässig einzuhalten und den ROI festzustellen.

Einige UEM-Lösungen steigern die IT-Produktivität und -Effektivität, indem mehrere Aspekte des Monitorings und Managements automatisiert werden, darunter die Spezifizierung von Maßnahmen, die im Falle von verschiedenen Verstößen durchgeführt werden sollten. Zu diesen können folgende gehören: vollständige oder selektive Remote-Löschung des Endgerätespeichers, der Compliance-Entzug des Endgeräts, Entzug des Endgeräts oder die Benachrichtigung des Anwenders, ein Problem innerhalb einer Frist zu beheben – z. B. das Entfernen einer nicht genehmigten App –, bevor ernstere Konsequenzen gezogen werden.

8. Support und Wartung für Endgeräte

Mit einem BYOD-Programm wird häufig der anfallende Wartungsaufwand für die einzelnen Endgeräte verringert, da der Anwender gleichzeitig auch der Eigentümer ist. Vor diesem Hintergrund sollte mit einer Richtlinie eindeutig festgelegt werden, wie verschiedene Support- und Wartungsaufgaben behandelt werden und wer dafür zahlt. Dadurch soll eine gesteigerte Komplexität und eine erhöhte Belastung der IT verhindert werden. In den meisten CYOD- oder COPE-Programmen ist die IT vollständig für den Support und die Wartung der Endgeräte verantwortlich.

So ermöglicht Citrix Workspace ein sicheres Endgerätemanagement

Jedes Endgerätemanagement-Programm muss Technologien bieten, die einen sicheren Zugriff auf Unternehmensanwendungen und -dateien über private Endgeräte ermöglichen. Citrix Workspace enthält alle wichtigen Funktionen, die notwendig sind, um BYOD, CYOD und COPE für jede Organisation einfach, sicher und effektiv zu gestalten. Die Lösung kombiniert Endpoint Management, Virtualisierung von Windows-Desktops und -Anwendungen, sicheren Dateiaustausch und Anwendungsbereitstellung. Dadurch können Sie Unternehmensanwendungen und -daten auf jedem Endgerät bereitstellen, das Anwender für die Arbeit nutzen, und gleichzeitig die Sicherheit und Kontrolle wahren.

Einheitliches Endgerätemanagement

Profitieren Sie von der benutzerabhängigen Bereitstellung und Kontrolle von Apps, Daten und Endgeräten, automatischer Konto-Deaktivierung bei ausgeschiedenen Mitarbeitern und selektivem Löschen von Daten auf verloren gegangenen Geräten. Mit Citrix Workspace können

Sie Endgeräte managen, einschließlich IoT-Geräte. Gleichzeitig können Sie auf Programmebene Sicherheits- und Kontrollfunktionen einrichten, um Unternehmensdaten zu schützen, ohne die Nutzung privater Inhalte auf BYOD-, CYOD- oder COPE-Endgeräten zu beeinträchtigen. Mit dem Endpoint Management von Citrix Workspace können Sie auswählen, welche MAM-Strategie sich am besten für Sie eignet. Dabei kann es sich um eine MAM-Plattform wie Samsung KNOX oder Appconfig, Citrix MDX (das eine zusätzliche Ebene der Anwendungsverschlüsselung ohne die Registrierung von Endgeräten bereitstellt) oder um Intune MAM handeln.

Windows-Desktop- und App-Virtualisierung

Statt auf jedem einzelnen Endgerät Windows-Anwendungen und -Desktops zu installieren, können Sie diese als On-Demand-Services bereitstellen. Da die Apps und Daten zentral in einem Rechenzentrum oder einer Cloud betrieben werden, bietet die IT für persönliche wie auch unternehmenseigene Endgeräte den Zugriff auf die gleiche integrierte Umgebung mit zentralisiertem Datenschutz, Anwendermanagement, Compliance- und Zugriffskontrolle.

App-Store

Bieten Sie Anwendern Zugriff auf Web-, Saas-, Unternehmens- und Windows-Anwendungen sowie mobile Apps über einen zentralen App-Store. Es spielt keine Rolle, für welches Endgerät sich Anwender entscheiden – Windows- oder Mac-Computer; iOS-, Android- oder Windows-basierte mobile Geräte oder Google Chromebooks –, der Benutzerkomfort ist stets erstklassig, unabhängig von Endgerät, Standort und Netzwerk.

Sicherer Zugriff

Dank eines einheitlichen Management-Frameworks kann die IT den Zugriff auf Anwendungen, Desktops und Services über jedes Endgerät absichern, kontrollieren und optimieren. Auditing- und Berichtfunktionen unterstützen Compliance und Datenschutz. Nur Citrix bietet einzigartige Micro-VPN-Funktionen, um Anwendungen und Daten zwischen dem mobilen Endgerät und den Ressourcen des Unternehmens hinter der Firewall weiter zu schützen.

Sicheres Filesharing

Mitarbeiter können mit anderen Personen inner- oder außerhalb ihrer Organisation sicher Dateien austauschen und diese mit all ihren Endgeräten synchronisieren. Richtlinienbasierte Zugriffskontrolle, Auditing, Reporting-Funktionen und Remote-Löschung von Endgeräten helfen beim Schutz der Unternehmensdaten.

Mit den richtigen Richtlinien und Technologien können Sie Mitarbeitern eine freie Auswahl und der IT umfassende Sicherheit und Kontrolle bieten. Erfahren Sie auf www.citrix.de/workspace

Enterprise Sales
Nordamerika | 800-424-8749
Weltweit | +1 408 790 8000

Standorte
Unternehmenszentrale | 851 Cypress Creek Road Fort Lauderdale, FL 33309, USA
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, USA