Digital Services

Alles, was Sie über den Arbeitsplatz der Zukunft wissen sollten.

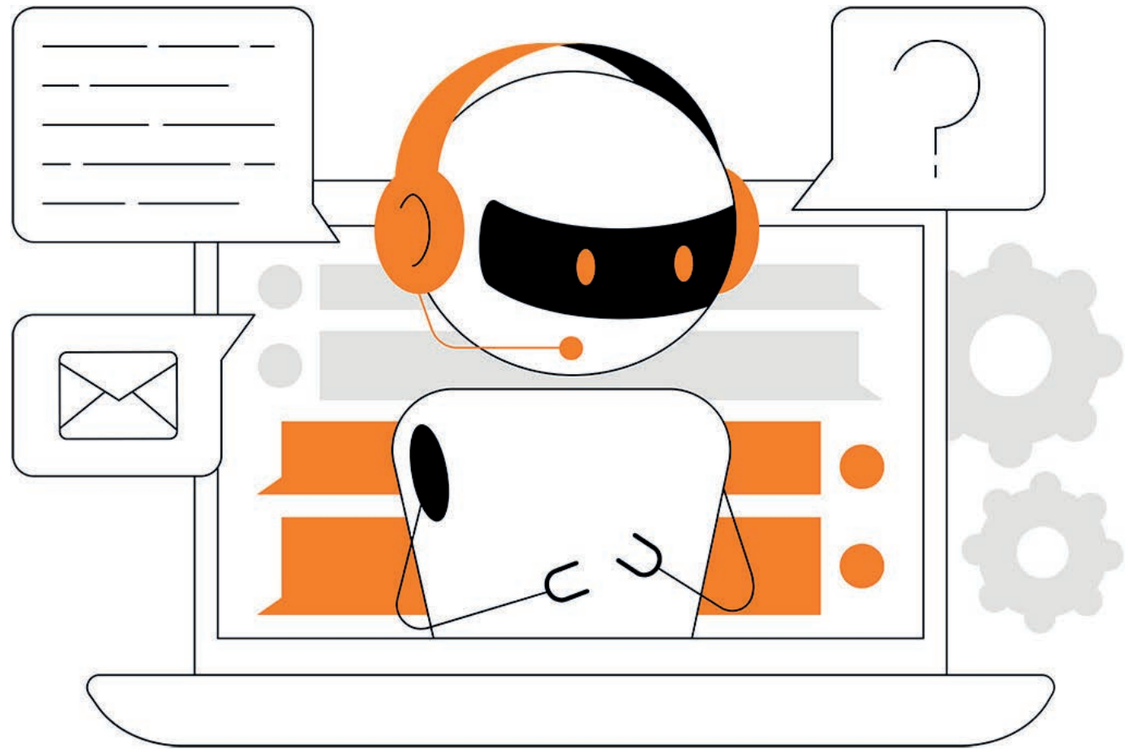
orange™ Business

Von A
wie Autopatch
bis Z
wie Zero Trust

Modern Workplace eBook

Inhalt

Wir gestalten den Arbeitsplatz der Zukunft



Zurück zur Inhaltsangabe

1. Einleitung

Der flexible Arbeitsplatz mit freier Arbeitszeiteinteilung bringt große Mehrwerte:

Mitarbeitende können Privates und Berufliches besser verbinden. Das **steigert** nicht nur die **Attraktivität der Arbeitgeber**, sondern auch die **Zufriedenheit der Mitarbeitenden** – und somit letztlich die Produktivität im Unternehmen. Junge Talente suchen außerdem gezielt Unternehmen, die flexible Arbeitsgestaltung ermöglichen. Ein wichtiger Punkt im Zeitalter des Fachkräftemangels.

Führungskräfte müssen den Teams Rahmenbedingungen vorgeben, in denen sich die Mitarbeitenden selbst organisieren. Darüber hinaus brauchen Teams eine klare Strategie, die sie am besten zusammen in Workshops erarbeiten. Diese muss stetig überprüft und bei Bedarf nachgebessert werden. Wichtig ist hier, dass sich Unternehmen mit dem Thema **„agile Teams“** auseinandersetzen und entsprechende Arbeitsmodelle dort zum Tragen kommen, wo Mehrwerte entstehen.

Mit diesem eBook geben wir einen Einblick in den **„Modern Workplace“** und welche Themenfelder es in Betracht zu ziehen gilt. Weitestgehend herstellerneutral, möchten wir unsere Ansätze sowie Ideen an die Leserschaft weitergeben. Da das Thema sehr komplex ist, können wir hier nicht alles beschreiben. Sie haben Fragen? Natürlich ist ein individuelles persönliches Gespräch möglich.

Viel Spaß mit unserem „Modern Workplace eBook“

Zurück zur Inhaltsangabe

Das Who-is-Who der Mitarbeiter-Devices

Zurück zur Inhaltsangabe

2. Endgeräte

Das Who-is-Who der Mitarbeiter-Devices

Ein essenzieller Teil eines flexiblen Arbeitsplatzes, ist die Hardware oder das Medium oder einfach auch nur das s.g. Benutzerendgerät.

Ein essenzieller Teil eines flexiblen Arbeitsplatzes, ist die Hardware oder das Medium oder einfach auch nur das s.g. Benutzerendgerät. Dabei unterscheiden wir zwischen verschiedenen Modellen und deren Verwendung. So ist es in der heutigen Zeit nicht unüblich, dass ein Arbeitnehmer, zum Beispiel ein Smartphone und ein Computer besitzt, um seine alltäglichen Aufgaben zu erledigen. Andere haben zusätzlich zum Smartphone und PC auch noch ein Tablet, welches z.B. die vorher genannten Geräte in einem kombinieren kann. Gerade die jetzige Entwicklung dieser Medien und auch das, was noch zukünftig kommen wird zielt darauf, den Unternehmen und den Mitarbeitern die Arbeit mehr und mehr zu erleichtern.

Und das genau ist auch das Ziel des Modern Workplace. Die Arbeit mit den bereitgestellten Unternehmensressourcen und auch das Miteinander, Stichwort Collaboration, zu vereinfachen. Dabei ist der Gedanke, die Bereitstellung der Ressourcen hardware- oder medienunabhängig zur Verfügung zu stellen.

Das bedeutet, dass Unternehmen größtenteils freie Hand haben bei der Beschaffung entsprechender Hardware. Dabei ist es egal, ob das Unternehmen das Benutzerendgerät vorgibt oder es dem Mitarbeiter die Möglichkeit gibt, sich eigene Hardware selbst zu beschaffen (BYOD).

2.1
Unterschiede - Computer

Auch wenn es egal ist, welche Hardware verwendet wird, gibt es trotzdem große Unterschiede zwischen den jeweiligen Produkten.

Wie bereits schon beschrieben, gibt es den Computer, das Tablet oder das Smartphone, welche als Medium für die Arbeit mit dem Modern Workplace genutzt werden können. Aber gerade im Bereich Computer gibt es große Unterschiede und ein Unternehmen steht immer irgendwann vor der Frage: Welche Hardware ist die sinnvollste, damit der Mitarbeiter produktiv ist, aber auch flexibel sein kann?

Hier gibt es 3 Formen, die genutzt werden können, der Zero Client, der Thin Client oder der Fat Client.
Während sich die beiden Formen Zero Client und Thin Client grundsätzlich die gleiche Basis teilen, mit der Unterscheidung in der Ausprägung der Hardware und des Betriebssystems, ist der Unterschied zu einem Fat Client immens.

2.2
Der Fat Client (Thick Client)

Der Fat Client (oder Thick Client genannt) ist ein kompletter PC mit CPU, Arbeitsspeicher, Grafikkarte und Festplatte, auf welcher auch lokal Anwendungen installiert und genutzt werden können.

Der Fat Client benötigt grundsätzlich keine Verbindung zu einem Netzwerk, um genutzt werden zu können.
Er kann somit auch eigenständig genutzt werden.

2.1.2

Der Zero
oder
Thin Client

Ein Zero Client ist eine besonders verschlankteForm eines Thin Clients und wird, wie der Thin Client auch, hauptsächlich in VDI- oder Terminalserver Umgebungen verwendet. Ein Zero oder Thin Client dient nur als Verbindungsmedium, um Ressourcen im Unternehmensnetzwerk zu nutzen. Der Zero Client unterscheidet sich zu einem Thin Client hauptsächlich bei der Ausprägung der Hardware und des Betriebssystems.

Ein Zero Client verwendet beim Starten eine sogenannte Firmware (welche nicht als ein Betriebssystem angesehen werden kann), die über das angeschlossene Netzwerk eine Verbindung zur notwendigen Ressource herstellt. Die abgerufenen Informationen werden dann in einen Speicher geladen und verwendet. Dies bedeutet, dass der Zero Client keine Festplatte besitzt und auch keine spezielle Konfiguration.

Ein Zero Client ist vollkommen abhängig von der Ressource, zu der sich verbunden werden soll. Dies setzt immer eine Netzwerkverbindung voraus.

Das Gleiche gilt grundsätzlich auch für einen Thin Client. Nur gibt es hier noch ein paar nennenswerte Unterschiede. Ein Thin Client hat in der Regel bei der Hardwareausstattung einige Vorteile. So wird z.B. in einen Thin Client noch eine zusätzliche Festplatte genutzt, welche meist ein Flashspeicher ist, der in erster Linie der Bereitstellung des Betriebssystems dient.

Dieser Flashspeicher bietet in manchen Fällen auch die Möglichkeit das Betriebssystem mit zusätzlicher Clientsoftware zu erweitern oder eine spezielle Konfiguration bereitzustellen. Aber auch der Thin Client benötigt, um adäquate genutzt werden zu können, eine Verbindung zu einer notwendigen Ressource, welche ein Terminalserver oder eine VDI-Umgebung sein kann. Und er benötigt dafür auch immer eine Verbindung zu einem Netzwerk.

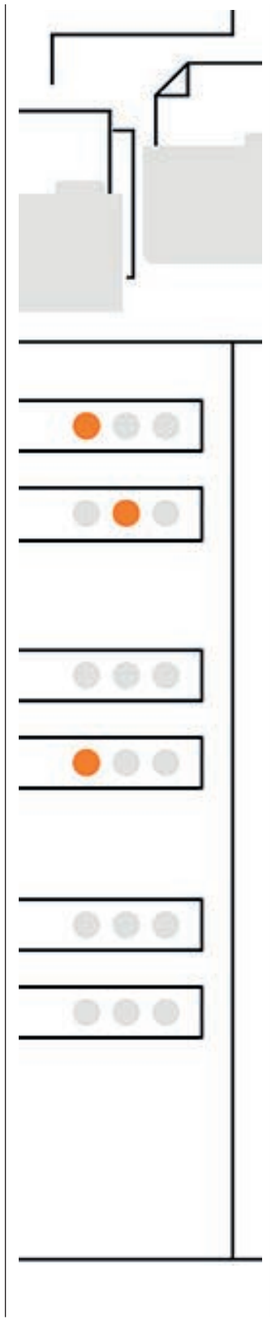
In beiden Formen der Computerbereitstellung, ob Zero oder Thin Client, ist eine Installation von zusätzlichen Anwendungen, als die, die schon im Image des Systems enthalten sind, nur nicht oder nur bedingt möglich.

2.2

Management -
Computer

Ein nächster wichtiger Punkt ist die Verwaltung solcher Geräte. Während der Fat Client in nahezu jede Management Lösung integriert werden kann, ist das Administrieren von Zero oder Thin Clients meistens proprietär und erfolgt über herstellereigene Lösungen. Eine Beschreibung, wie ein Benutzerendgerät Management für Fat Clients aussieht, kann im Kapitel „Unified Endpoint Management“ nachgelesen werden.

Das Verwalten von Zero oder Thin Clients erfolgt meistens über eine Verwaltungssoftware, die über einen separaten Server im Unternehmensnetzwerk zur Verfügung gestellt wird. Die Zero/Thin Clients sind in der Regel dann in dieser Software registriert und können so zentral, über die bereitgestellten Kontroll- und Sicherheitsfunktionen, gesteuert werden.



2.2.1

Unterschiede -
Tablet/ Smartphone

Tablets unterscheiden sich hauptsächlich durch ihre Größe gegenüber gängigen Smartphones und werden nicht zum Telefonieren verwendet.

Das sind aber auch schon die wesentlichsten Unterschiede zwischen diesen Produkten auf der Hardwareseite. Abgesehen noch vom Preis, Tablets sind meistens noch günstiger als Smartphones.

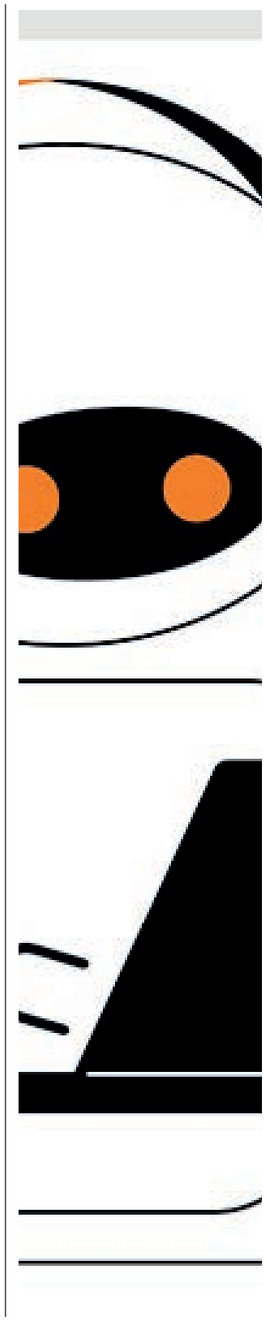
Tablets und Smartphones unterscheiden sich heute kaum noch in der Ausstattung bis auf zum Beispiel die verwendete Kamera oder die Verfügbarkeit eines SIM-Karten-Moduls.

2.2.2

Das Tablet - Klassisch oder 2-in-1

Abgesehen von den klassischen Tablets gibt es aber auch noch Tablets, die sich gegenüber den regulären Tablets, durch eine größere Ausstattung oder Funktionalität unterscheiden. Die Rede ist hier von so genannten Convertibles oder Detachables. Die auch 2-in-1 Tablets genannt werden.

Während ein Convertible physisch mit einer Tastatur verbunden ist und sich nur durch eine 360° Drehung des Displays in ein Tablet verwandeln lässt, kommt ein Detachable mit einer Tastatur, die nur angesteckt ist. Die Verbindung findet dann über eine eigene Schnittstelle statt. Beide 2-in-1 Tablets lassen sich im laufenden Betrieb in ein klassisches Tablet umwandeln und auch wieder zurück.



2.3

Verwendung / Nutzung

Größere Unterschiede zwischen Tablets und Smartphones gibt es bei der Verwendung dieser Geräte. Während Smartphones überwiegend zum Telefonieren oder Nachrichtenschreiben und -senden verwendet werden, wie SMS, Messenger oder E-Mails, wird das Tablet auch in anderen Bereichen genutzt. Dies ist zum Beispiel während Schulungen möglich oder als Kontrollpunkt in Konferenzräumen oder zur Kontrolle von Betriebsabläufen in der Industrie.

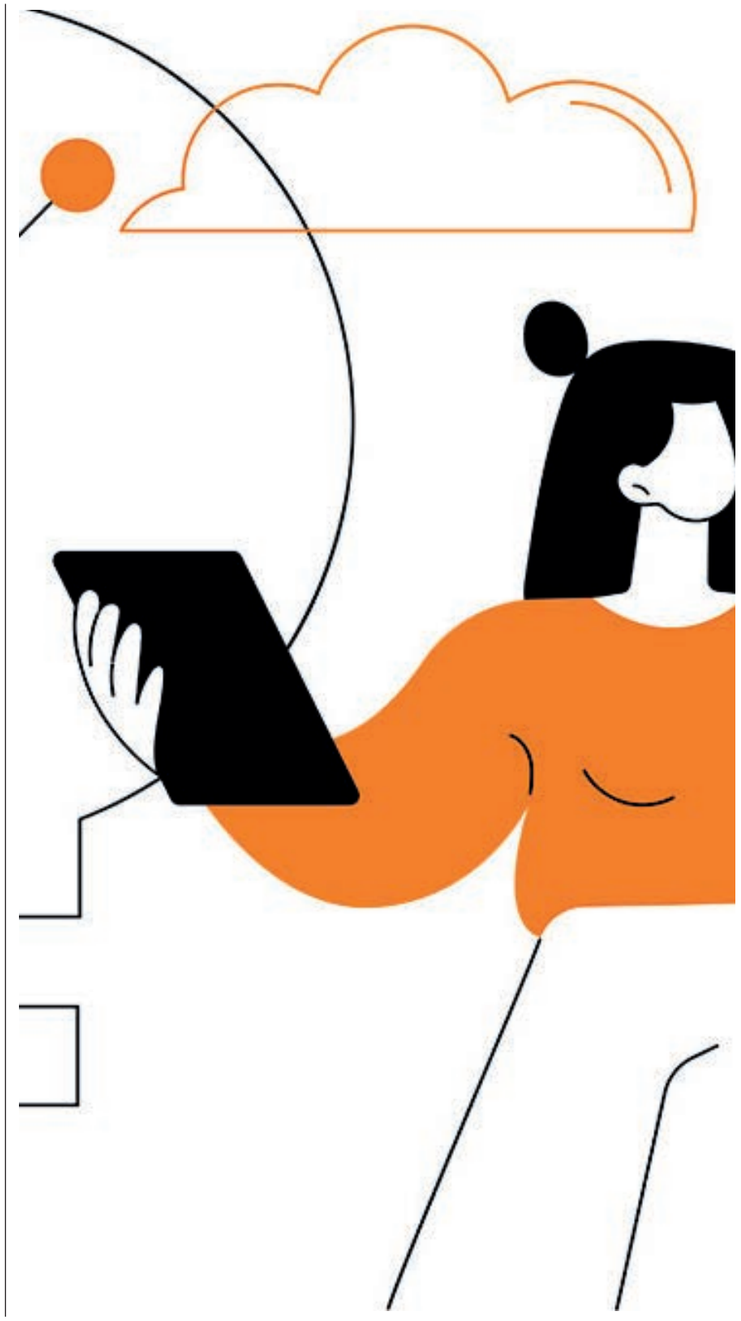
Das Smartphone kann außerdem noch als zusätzliche Authentifizierungsmethode integriert werden, wenn z.B. eine 2-Faktor-Authentifizierung aktiviert wurde. Hierfür gibt es verschiedene Apps und Mechanismen, die dafür genutzt werden können.

2.4

Management - Tablet / Smartphone

Die Administration dieser Geräte kann als relativ einfach bezeichnet werden. Tablets und Smartphones lassen sich in jede derzeit verfügbare Endpoint Management Lösung problemlos integrieren und verwalten.

Welche Möglichkeiten es gibt wird im Kapitel „Unified Endpoint Management“ näher beschrieben.



2.5

Fazit

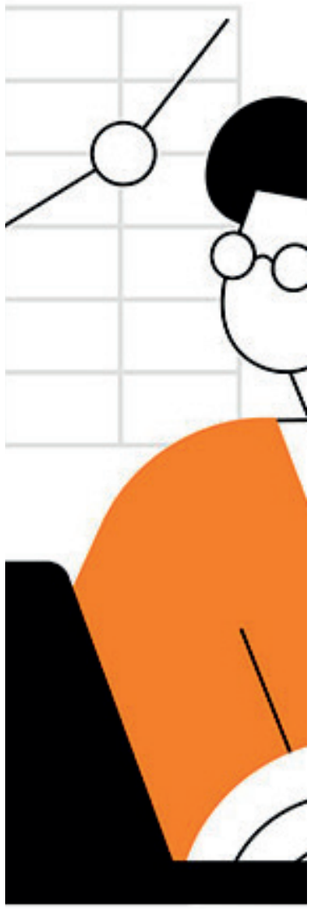
Den Unternehmen stellt sich immer wieder die Frage: Wie soll mein Mitarbeiter arbeiten können? Wie schon in der Einleitung erwähnt, nutzen viele Unternehmen die Möglichkeit der Flexibilität und statten den Mitarbeiter mit einem unternehmenseigenenPC und Smartphone aus, oder gewähren, im Rahmen einer BYOD-Regelung, dem Arbeitnehmer die Beschaffung eines eigenen Benutzerendgerätes innerhalb

Anders sieht es hingegen aus, wenn der Mitarbeiter in den unternehmenseigenen Büroräumen tätig werden soll. Hier stellt sich die Frage, arbeitet der Arbeitnehmer an einem festen Arbeitsplatz mit einem fest zugewiesenen Computer oder ist es ein Großraumbüro mit flexibler Arbeitsplatzeinteilung. Aber wenn ein flexibler Arbeitsplatz besteht, sind die PCs fest zugewiesen oder frei nutzbar.

Während in einem eigenen Büro der Fat Client durchaus seine Daseinsberechtigung hat, ist er in einem Großraumbüro weniger praktikabel, da starr und immer irgendwie präsent. Ein Zero oder Thin Client wiederum ist sind in beiden Welten durchaus praktikabel. Zero/Thin Clients können z.B. an der Rückseite eines Monitors befestigt werden und verschwinden so aus dem Sichtfeld des Mitarbeiters.

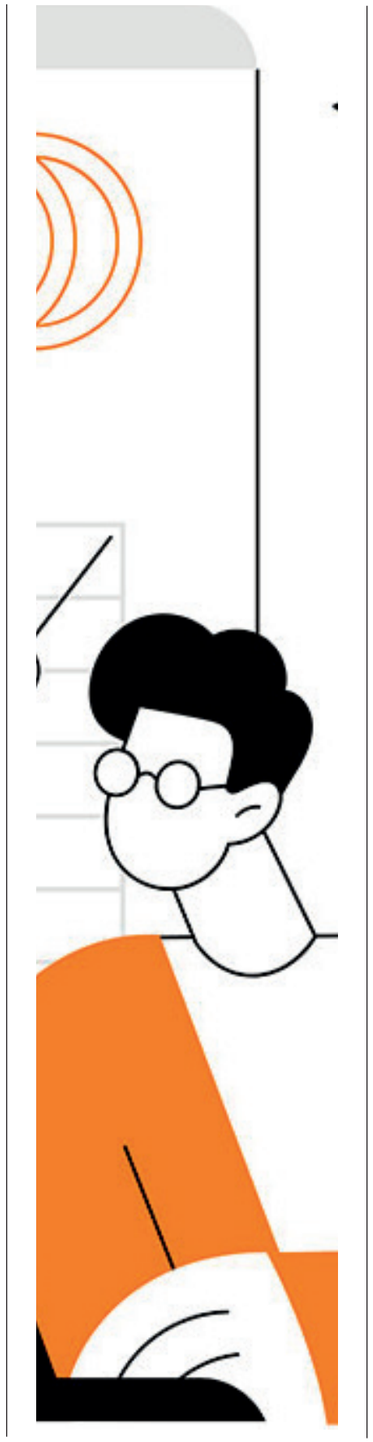
Sie benötigen allerdings eine bestehende Netzwerkstruktur, über welche die Unternehmensressourcen erreicht und genutzt werden können.

Zurück zur Inhaltsangabe

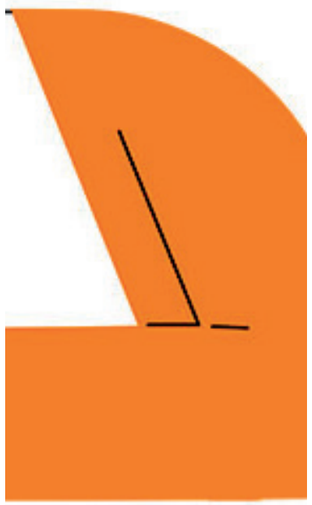


In der folgenden Matrix sind noch einmal **die Unterschiede**
zu den bestimmten Kriterien zum Fat Client und den Zero-/Thin Clients gelistet:

	Zero Client	Thin Client	Fat Client (Thick Client)
Hardware	- Kein eigenes Laufwerk - Bootet aus dem Netzwerk - Notwendige Informationen werden in den Arbeitsspeicher geladen - Grafik rendern nur eingeschränkt sinnvoll	- Eigenes Laufwerk vorhanden *(Flash Speicherkarte)* - Grafik oder Media rendern möglich *(abhängig von der Hardwareausprägung)*	- Eigenes Laufwerk vorhanden. *(z.B. SSD)* - Grafik oder Media rendern gegeben
Betriebssystem	- Kein OS vorhanden *(boot von Firmware)* - Verbindung zu einer entsprechenden Ressource *(Netzwerk)* notwendig	- OS vorhanden *(kompakt und eingeschränkt anpassbar)* - Verbindung zu einer entsprechenden Ressource (Netzwerk) notwendig	- OS vorhanden *(anpassbar und erweiterbar)* - Nutzbar auch ohne Verbindung zu einer entsprechenden Ressource *(Netzwerk)*
Verwaltung	- Proprietäre oder extra auf das Produkt abgestimmtes 3rd-Party Tool - Steuerung/ Kontrolle zentral über dieses Tool	- Proprietäre oder extra auf das Produkt abgestimmtes 3rd-Party Tool - Steuerung/ Kontrolle zentral über dieses Tool	- Integration in nahezu alle Management Tools möglich - Steuerung/ Kontrolle in manchen Fällen eingeschränkt



	Zero Client	Thin Client	Fat Client (Thick Client)
Programmausführung	- Keine Programmausführung direkt auf dem Zero Client - Keine lokale Installation von Programmen oder Tools möglich	- Keine Programmausführung direkt auf dem Thin Client. - Keine lokale Installation von Programmen oder Tools möglich - Nachinstallation bestimmter Tools in manchen Fällen möglich	- Programmausführung direkt auf dem Fat Client möglich - Installationen von Programmen auf dem Fat Client möglich
Herstellerabhängigkeit	Unterstützung meist nur ein oder zwei Remote-Protokolle	Keine unmittelbare Hersteller-abhängigkeit, da meist mehrere Server-Lösungen und Remote-Protokolle unterstützt werden	Keine Herstellerabhängigkeit
Ressourcenabhängig-keit	Klare Abhängigkeit zum Server, ohne den ein Zero Client nicht arbeiten kann.	Klare Abhängigkeit zum Server, ohne den ein Thin Client nicht arbeiten kann verhält sich wie ein Terminal zum Server	Keine Ressourcenabhängigkeit Fat Client nutzt eigenes OS und Programme

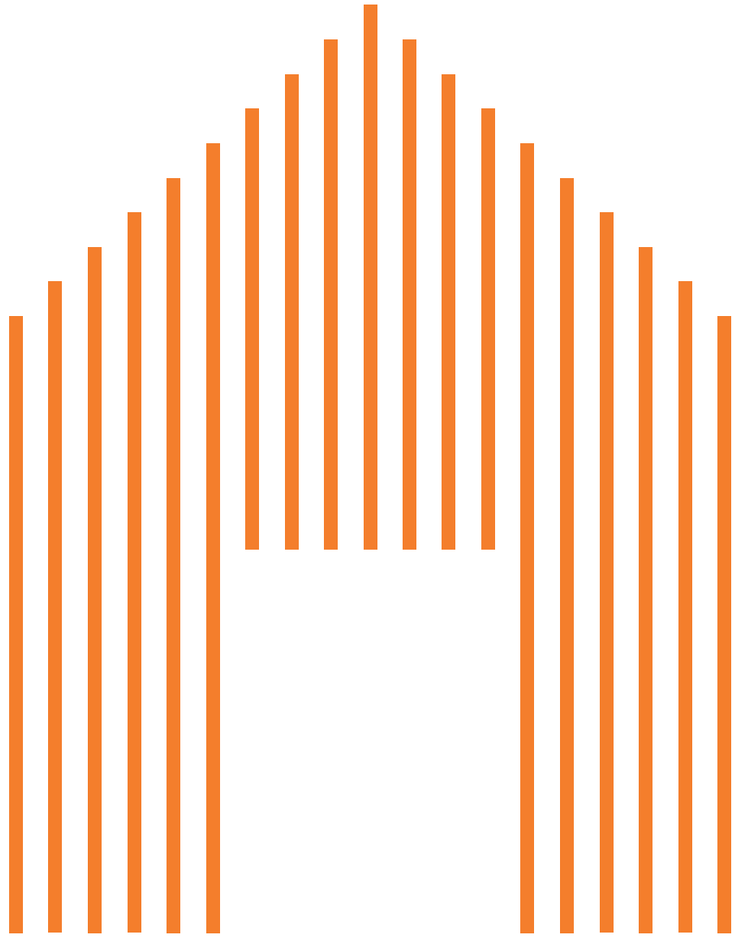


	Zero Client	Thin Client	Fat Client (Thick Client)
Sonstiges (Strom, Anschaffung)	- Geringer Stromverbrauch - Geringere Kosten gegenüber Thin und Fat Client	- Geringer bis mäßiger Stromverbrauch - Höhere Kosten gegenüber dem Zero Client aber niedrigere zum Fat Client	- Höherer Stromverbrauch gegen über dem Zero und Thin Client - Mäßige bis höhere Kosten gegenüber dem Zero und Thin Client
Komfort	- Einfache Bereitstellung - Einfache Verwaltung - Kaum sichtbar	- Einfache Bereitstellung - Einfache Verwaltung - Kaum sichtbar *(abhängig vom ausgewählten Platz)*	- Einfache bis mäßige Bereitstellung - Komplexere Verwaltung - Immer sichtbar und präsent

Zurück zur Inhaltsangabe

3. Unified Endpoint Management

Viele Endpunkte, eine Plattform. *Hier läuft alles zusammen.*



Zurück zur Inhaltsangabe

3. Unified Endpoint Management

In diesem Kapitel werden wir das Konzept des Unified Endpoint Managements (UEM) und seine grundlegenden Komponenten näher betrachten. UEM ist ein Ansatz für das Endpoint Management, der mehrere Aspekte der Geräte-, Anwendungs- und Datenverwaltung in einer einzigen, vereinheitlichten Plattform integriert.

Durch die Kombination der Funktionalitäten von Mobile Device Management (MDM), Mobile Application Management (MAM) und Enterprise Mobility Management (EMM) vereinfacht und optimiert UEM das Management von Endpunkten unabhängig von deren Typ oder Betriebssystem.

3.1 Definition von UEM und seiner Hauptkomponenten

Unified Endpoint Management bezeichnet die Praxis, alle Endgeräte innerhalb einer Organisation von einer zentralen Konsole aus zu verwalten. Endgeräte, im Sinne von UEM, können traditionelle Geräte wie Desktops, Laptops, Mobiltelefone oder Tablets sowie IoT-Geräte und andere intelligente Endpunkte umfassen.

Die Hauptkomponenten von UEM sind:

Geräteverwaltung:
UEM ermöglicht grundsätzlich die Registrierung, Konfiguration und Verwaltung von Endgeräten. Zum Beispiel können verwaltete Endgeräte aus der Ferne gesperrt, zurückgesetzt oder gelöscht werden. Dies gewährleistet einerseits mehr Sicherheit z.B. bei Verlust oder Diebstahl der verwalteten Endgeräte und reduziert andererseits den Aufwand bei der Einrichtung oder Fehlerbehebung von verwalteten Endgeräten.

Anwendungsverwaltung:
Weiterhin können Anwendungen auf allen verwalteten Endgeräten implementiert, aktualisiert und konfiguriert werden. Dies umfasst in der Regel die Verwaltung von sowohl nativen Apps als auch von Drittanbieter Anwendungen und beinhaltet auch die Zugriffssteuerung und z.B. das Einhalten von Lizenzbestimmungen für Anwendungen im Besitz des Unternehmens.

3.1 Definition von UEM und seiner Hauptkomponenten

Inhaltsverwaltung:
UEM ermöglicht eine sichere Verteilung von und den Zugriff auf Inhalte, sodass Mitarbeiter auf Unternehmensressourcen zugreifen können, während der Datenschutz gewährleistet wird. Administratoren können gleichzeitig Verschlüsselung und Zugriffskontrollen durchsetzen, um Datenlecks zu verhindern. So kann zum Beispiel definiert werden, dass vom Unternehmen verwaltete Inhalte nur unter bestimmten Bedingungen zugegriffen oder weitergegeben werden können.

Sicherheits- und Compliance-Richtlinien:
UEM ermöglicht die Durchsetzung von Sicherheitsrichtlinien auf allen Endgeräten, um sich effektiv vor potenziellen Bedrohungen zu schützen. Hierzu gehören Funktionen wie Passwortrichtlinien, Verschlüsselung, Firewall-Einstellungen und Compliance-Überprüfungen.

Berichterstellung und Analyse:
UEM bietet Administratoren Einblicke in die Nutzung der Endgeräte, den Sicherheitsstatus und deren Compliance-Einhaltung durch umfassende Berichterstattungs- und Analysetools.

3.2 Entwicklung des Endpoint Managements: MDM, MAM und EMM

Bevor das Konzept des UEM entstand, verließen sich Organisationen auf separate Lösungen zur Verwaltung verschiedener Arten von Endgeräten.

Diese Lösungen umfassten:

Mobile Device Management (MDM):
Konzentrierte sich hauptsächlich auf Smartphones und Tablets und ermöglichte Administratoren die Kontrolle über Geräteeinstellungen, die Durchsetzung von Sicherheitsrichtlinien und die Remote-Verwaltung von Geräten.

Mobile Application Management (MAM):
Konzentrierte sich auf die Verwaltung und Sicherheit von Anwendungen auf mobilen Geräten. Es konzentrierte sich auf die Verteilung, Aktualisierung und Überwachung von Apps, ohne eine umfassende Gerätekontrolle.

Enterprise Mobility Management (EMM):
War eine integrierte Lösung, die die Funktionen von MDM und MAM kombinierte. Sie bot einen umfassenderen Ansatz zur Verwaltung von Geräten und Anwendungen.

3.3 Herausforderungen durch traditionelle Endpoint Management-Lösungen

Obwohl MDM, MAM und EMM wertvolle Funktionen boten, traten auch mehrere Herausforderungen für Organisationen auf:

Komplexität:
Die Verwaltung mehrerer Lösungen führte zu betrieblichen Komplexitäten, da separate Konsolen, Lizenzen und Fachkenntnisse erforderlich waren.

Fragmentierter Ansatz:
Der fragmentierte Ansatz führte zu isolierten Verwaltungsprozessen, was es schwierig machte, konsistente Richtlinien für alle Endpunkte durchzusetzen.

Benutzererfahrung:
Getrennte Managementlösungen beeinträchtigten manchmal die Benutzererfahrung und Produktivität.

Sicherheitsrisiken:
Lücken zwischen verschiedenen Verwaltungstools könnten potenzielle Sicherheitslücken und Datenschutzverletzungen verursachen.

3.4 Vorteile der Einführung eines UEM-Ansatzes

Durch die Umstellung auf Unified Endpoint Management können Organisationen mehrere Vorteile realisieren:

Vereinfachte Verwaltung:
UEM konsolidiert das Endpoint Management in einer einzigen Plattform und vereinfacht so den Betrieb und reduziert die Betriebskosten.

Erhöhte Sicherheit:
Einheitliche Sicherheitsrichtlinien für alle Endgeräte gewährleisten ein höheres Maß an Schutz vor Sicherheitsbedrohungen.

Verbesserte Produktivität:
UEM bietet eine nahtlose Benutzererfahrung, wodurch Mitarbeiter produktiver und effizienter arbeiten können.

Bessere Compliance:
UEM ermöglicht die Einhaltung von gesetzlichen Anforderungen durch die Implementierung konsistenter Sicherheitsmaßnahmen und Überwachungsfunktionen.

Skalierbarkeit:
Mit der Einführung neuer Endgeräte und der Erweiterung des Geräte-Ökosystems wächst UEM problemlos mit der Organisation mit.

4. Softwareverteilung

Bereit,

weil perfekt bereitgestellt

Zurück zur Inhaltsangabe

4. Softwareverteilung

Die schnelle und zuverlässige Bereitstellung von Software zählt zu den Kernaufgaben des UEM. In der Vergangenheit wurden oftmals verschiedene Management Lösungen in Abhängigkeit von der Art des Endgeräts und seines primären Einsatzortes genutzt. Diese Aufteilung auf verschiedene Systeme und oft auch verschiedene Zuständigkeiten führt zu Mehraufwänden im Bereich Infrastruktur, Lizenzkosten, Softwarepaketierung, Applikationsmanagement, Reporting und Personal. Softwareverteilung ist in diesem Umfeld eine Verteilung verschiedener, unabhängig voneinander erstellter Pakete für verschiedene Zielsysteme. Koordination und Reporting im Zusammenhang mit Releasewechseln sind nur eingeschränkt und mit hohem Aufwand möglich. Je nach aktuellem Aufenthaltsort der jeweiligen Endgeräte kann auf die Bereitstellungsorte der Pakete nicht zugegriffen werden.

Für eine agile und sowohl Orts-, als auch geräteunabhängige Arbeitsweise muss eine einheitliche Management Umgebung geschaffen werden, die Schnittstellen in allen notwendigen Umgebungen bereitstellt. Softwareverteilung im Sinn von der unabhängigen Bereitstellung und Verteilung verschiedener und unabhängiger Pakete auf unterschiedliche Endgeräte in unterschiedlichen Umgebungen wird ersetzt durch die Bereitstellung von einheitlichen Applikationen.

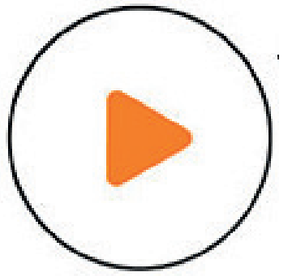
Dieser Ansatz ermöglicht es, Applikationen unabhängig von der Art ihrer Umsetzung für verschiedene Endgeräte zeitgleich bereitzustellen und deren Bereitstellung zentral zu überwachen.

Eine Applikation kann sowohl Softwarepakete, auch mehrere für verschiedene Anforderungen oder Umgebungen, aber auch Links zu Webseiten, App Stores, RDS und SaaS Lösungen beinhalten. Welches konkrete Paket verwendet wird, wird dynamisch in Abhängigkeit von Gerät und Umgebung entschieden. Die Bereitstellung von Softwarepaketen kann sowohl über klassische Depotserver, als auch Content Delivery Networks oder Cloud Storage Lösungen erfolgen. Welche Quelle genutzt wird, wird abhängig von der jeweiligen Umgebung entschieden.

4.1 Enrollment

Idealerweise erfolgt das Enrollment, also die Registrierung, von Endgeräten ganz ohne administrativen Aufwand direkt bei der Beschaffung des jeweiligen Geräts. Hierfür haben mittlerweile eigentlich alle gängigen Hersteller Mechanismen und Schnittstellen etabliert, welche genau diese Anforderung adressieren.

Diese Möglichkeit steht hauptsächlich nur unternehmenseigenen Geräten offen. Eigene Geräte von Mitarbeitern (Stichwort: Bring your own device) können natürlich ebenfalls registriert und anschließend entsprechend verwaltet werden.

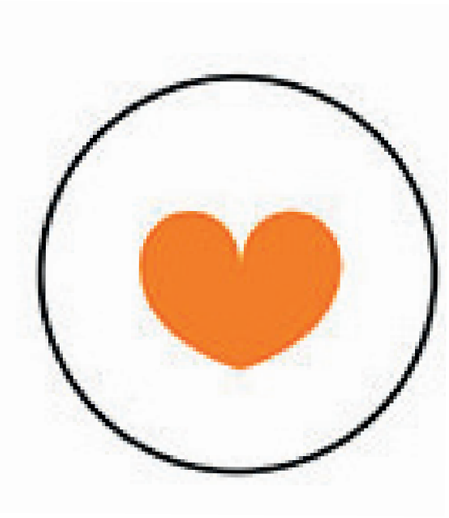


4.2 Autopilot

Microsoft hat für das Enrollment und die initiale Konfiguration von ausschließlich Windows Geräten Windows Autopilot in Intune integriert. Windows Autopilot ermöglicht ein tatsächliches Zerotouch Deployment von Windows Geräten und sorgt dabei für deren Enrollment, die OS-Konfiguration und die Installation von Anwendungen.

Die einzige Voraussetzung hierfür ist das Vorhandensein einer Internetverbindung. Idealerweise können die Endgeräte also direkt dem Mitarbeiter übergeben werden, welcher Dieses ortsunabhängig (Im Office, Homeoffice oder gar unterwegs) ohne administratives Zutun konfigurieren lassen kann. Ein Reset von Autopilot Geräten kann im Fehlerfall ebenfalls durchgeführt werden und wird entweder vom Mitarbeiter selbst oder einem Supportmitarbeiter initiiert.

4.3 Funktionen und Vorteile



Automatisiertes Enrollment von Windows Geräten durch zertifizierte OEM Hersteller Ortsunabhängiges Deployment von Endgeräten:

Windows Endgeräte können sowohl innerhalb des Unternehmensnetzwerks als auch überall dort deployed werden, wo sie über eine stabile Internetverbindung verfügen (LAN und WLAN).

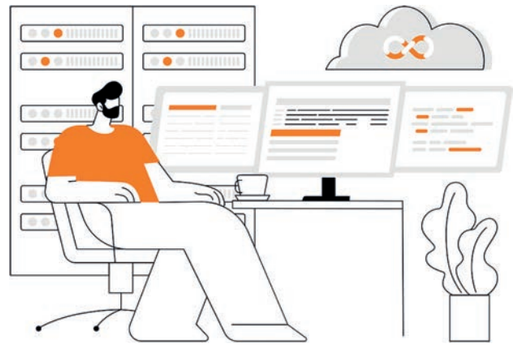
Editionswechsel von Windows Instanzen:
Abhängig von vorhandenen Lizenzmodellen kann die Windows Edition (ab Pro) geändert werden.

Umfassende Konfigurationsmöglichkeiten:
Beim Deployment ziehen Windows Autopilot Geräte zugewiesene Intune Richtlinien und Regelsätze an. Dies bedeutet, dass alle in Intune bereitgestellten Konfigurationen und Applikationen im Rahmen dieses Deployments ebenfalls angewandt werden.

Zerotouch IT:
Neue Endgeräte oder Endgeräte mit Software-problemen können ohne Zutun der IT-Abteilung bereitgestellt und zurückgesetzt werden. Dies ermöglicht z.B. das Verschlanken von Lieferketten und sorgt auf Seiten der Supportorganisation für erhebliche Zeitersparnisse.

4.4

Fazit



Windows Autopilot ist ein moderner Deploymentansatz für Windows Devices, welcher nahtlos in Microsoft Intune integriert ist.

Windows Geräte können mittels Windows Autopilot ortsunabhängig und automatisiert bereitgestellt und zurückgesetzt werden.

Dies erhöht die Flexibilität und senkt gleichzeitig den Konfigurations- und Verwaltungsaufwand.

Zurück zur Inhaltsangabe

5. AutoPatch

Automatisch aktuell, mit bester “Patch-Work-Performance”

Zurück zur Inhaltsangabe

5. AutoPatch

In der heutigen schnelllebigen ITLandschaft ist die Verwaltung von Software-Patches und Aktualisierungen für Unternehmen von entscheidender Bedeutung. Ein effektives Patch-Management kann Sicherheitsrisiken minimieren, Systemstabilität gewährleisten und die Gesamtleistung der ITInfrastruktur verbessern.
Microsoft, als Vorreiter im Bereich der Unternehmenslösungen,hat sich dieser Herausforderung angenommen und bietet mit „Microsoft AutoPatch“ eine fortschrittliche Lösung zur Automatisierung von Aktualisierungsprozessen.

5.1 Die Essenz von Microsoft AutoPatch

Microsoft AutoPatch ist ein intelligenter Ansatz zur Aktualisierung und Verwaltung von Software in Microsoft-basierten Umgebungen. Es zielt darauf ab, den Prozess der Bereitstellung von Patches und Aktualisierungen effizienter zu gestalten, indem es manuelle Schritte minimiert und die Automatisierung in den Vordergrund stellt.

5.2 Funktionen und Vorteile

Automatisierte Patch-Bereitstellung: Eine der zentralen Funktionen von Microsoft AutoPatch ist die Fähigkeit, Patches und Aktualisierungen automatisch über das Internet zu verteilen. Dies reduziert die Notwendigkeit manueller Eingriffe und gewährleistet eine konsistente Anwendung von Sicherheitspatches auf allen relevanten Systemen.
Zeitgesteuerte Aktualisierungen: Mit AutoPatch können IT-Teams Zeitpläne für die Installation von Patches festlegen. Dadurch können Aktualisierungen außerhalb der geschäftigen Betriebszeiten durchgeführt werden, um die Produktivität nicht zu beeinträchtigen.

5.2 Funktionen und Vorteile

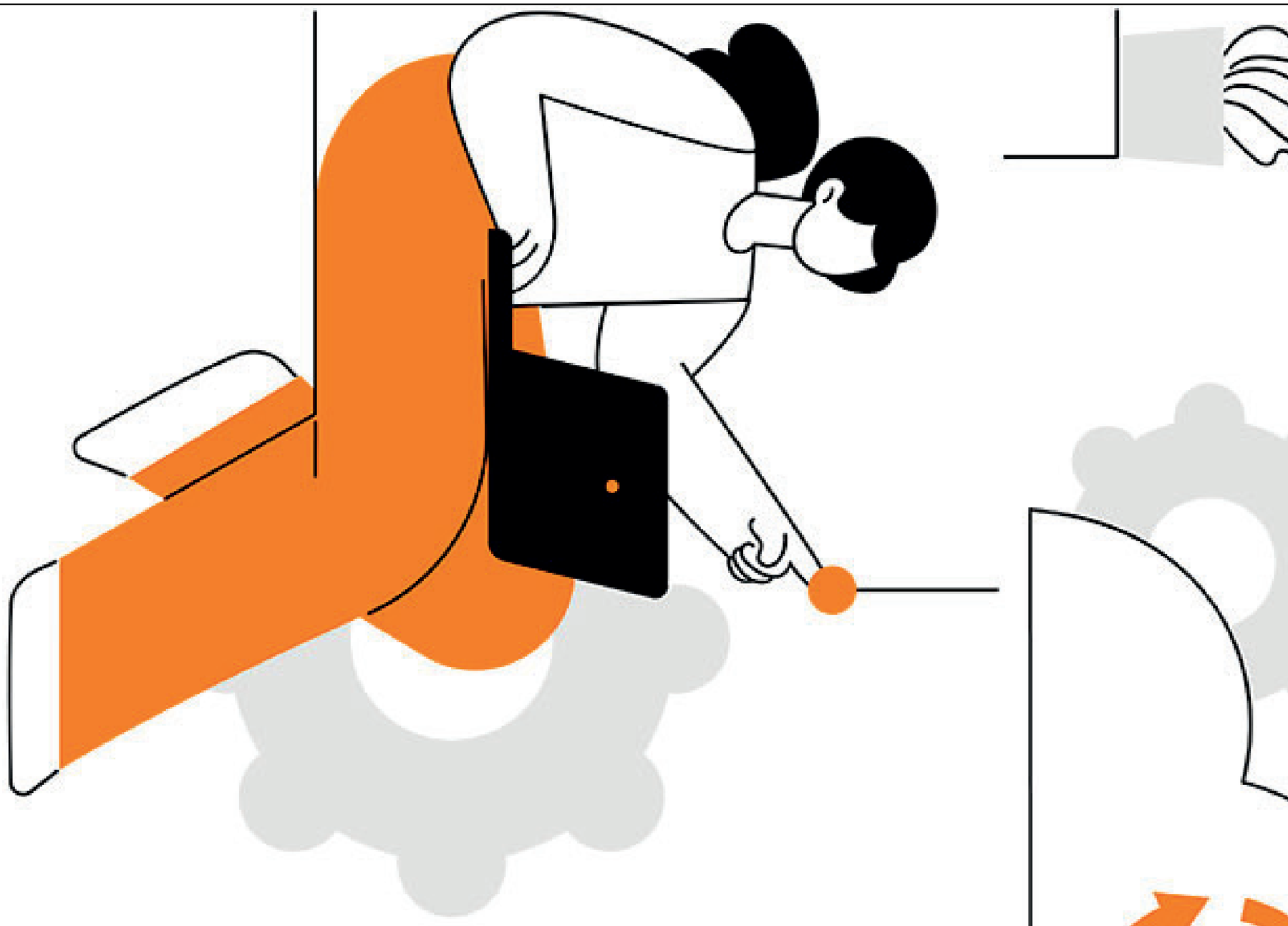
Intelligente Priorisierung: AutoPatch erkennt automatisch kritische Sicherheitspatches und priorisiert deren Bereitstellung. Dies hilft, potenzielle Schwachstellen schnell zu schließen und die Sicherheit der Systeme zu gewährleisten.
Statusüberwachung und Berichterstattung:

Die Lösung bietet umfassende Einblicke in den Patch-Status der Systeme. IT-Administratoren können den Fortschritt überwachen und detaillierte Berichte erstellen, um die Einhaltung von Richtlinien nachzuweisen.

5.3 Voraussetzungen und Implementierung

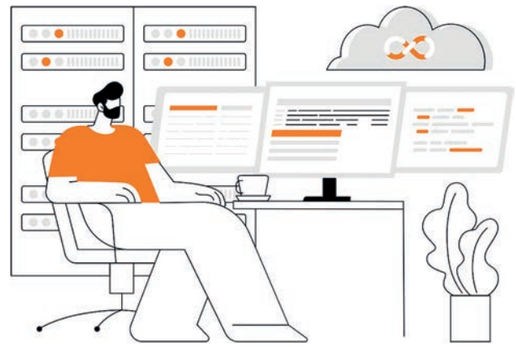
Die Einführung von Microsoft AutoPatch erfordert eine Microsoft-basierte IT-Infrastruktur, sowie ein eingerichteter und gepflegter Microsoft Azure Tenant, vorangig Microsoft Endpoint Manager inklusive der benötigten Lizenzen. Es ist wichtig sicherzustellen, dass alle beteiligten Systeme mit den erforderlichen Konfigurationen und Zugriffsberechtigungen ausgestattet sind.

Die Implementierung von AutoPatch erfordert eine sorgfältige Planung. Dies beinhaltet die Konfiguration von Patch-Regeln, die Festlegung von Aktualisierungszeitplänen und die Testphase, um sicherzustellen, dass die Patches die Systemstabilität nicht beeinträchtigen.



5.4

Fazit



Microsoft AutoPatch ist eine wegweisende Lösung für Unternehmen, die die Effizienz ihrer Patch-Verwaltungsprozesse steigern möchten. Durch die Automatisierung der Aktualisierungen können Sicherheitsrisiken minimiert, die Systemintegrität gewahrt und die Betriebszeit optimiert werden.

Die intelligente Priorisierung und Berichterstattungsfunktionen bieten eine umfassende Kontrolle über den Patch-Status der Systeme.

Zurück zur Inhaltsangabe

6. Desktop Virtualisierung

Einfache Lösungen für komplexe Anforderungen

Zurück zur Inhaltsangabe

6. Desktop Virtualisierung

Insbesondere durch die Initiativen unserer Kunden im Bereich des „Modern Workplace‘ erleben virtuelle Desktops eine Renaissance, da sie oft die einzige Möglichkeit sind, komplexe Anwendungen, die nicht für einen modernen Arbeitsplatz konzipiert wurden, bereit zu stellen. Kunden, die sich mit Modern Workplace beschäftigen, betrachten auch ganz intensiv die zur Verfügung stehenden VDI-Lösungen.

An dieser Stelle verweisen wir gerne auf unser VDI & Cloud-Computing Whitepaper, welches gesondert angefordert werden kann.

Heben Sie Ihre Zusammenarbeit auf eine neue Ebene

Zurück zur Inhaltsangabe

7. Collaboration & Productivity

Es ist faszinierend zu beobachten, wie sich die Art und Weise der Zusammenarbeit und Produktivität in der Geschäftswelt kontinuierlich weiterentwickelt. In einer Zeit, in der der Wettbewerb intensiver wird und die Technologie unaufhaltsam voranschreitet, gewinnen Aspekte wie nahtlose Zusammenarbeit, erhöhte Produktivität und effiziente Kommunikation.eine unvergleichliche Bedeutung.

7.1 Zusammenarbeit als Schlüssel zum Erfolg

In der heutigen globalisierten Welt sind Unternehmen auf Zusammenarbeit angewiesen, um ihre Innovationskraft zu steigern und schneller auf sich ändernde Marktbedingungen zu reagieren. Ein moderner Ansatz für Zusammenarbeit geht über geografische Grenzen hinaus und ermöglicht es Teams, unabhängig von ihrem Standort nahtlos zusammenzuarbeiten. Dies bedeutet, dass Teammitglieder in Echtzeit Informationen teilen, Ideen diskutieren und gemeinsam an Projekten arbeiten können.

7.2 Produktivität im Fokus

Produktivität ist der Schlüssel zur Maximierung der Effizienz eines Unternehmens. Moderne Arbeitsplätze setzen auf Technologien, die es Mitarbeitern ermöglichen, ihre Aufgaben effizient zu erledigen, ohne von überflüssigen Hindernissen ausgebremst zu werden. Cloud-Technologien und mobile Lösungen ermöglichen es den Mitarbeitern, von überall aus auf relevante Informationen zuzugreifen und Aufgaben zu erledigen. Dies führt nicht nur zu einer Steigerung der Produktivität, sondern auch zu einer besseren Work-Life-Balance der Mitarbeiter.

7.3 Moderne Kollaborationsmöglichkeiten nutzen

Moderne Kollaborationsplattformen bieten eine breite Palette von Tools, die die Art und Weise, wie Teams zusammenarbeiten, revolutionieren. E-Mail war gestern, heute setzen Unternehmen auf Plattformen wie Microsoft Teams, Slack und andere, um die Kommunikation zu vereinfachen und den Austausch von Informationen zu beschleunigen. Diese Plattformen integrieren Chat, Videokonferenzen, Dokumentenfreigabe und vieles mehr in einer einzigen Umgebung, wodurch die Notwendigkeit reduziert wird, zwischen verschiedenen Anwendungen hin und her zu wechseln.

7.4 Dynamische und zielgerichtete Kommunikation und Zusammenarbeit

Die heutige Geschäftswelt erfordert eine agile und zielgerichtete Kommunikation. Moderne Teams müssen in der Lage sein, schnell auf Nachrichten zu reagieren, sich in Diskussionen einzubringen und Entscheidungen in Echtzeit zu treffen. Kollaborationstools bieten nicht nur Möglichkeiten zur schnellen Kommunikation, sondern ermöglichen es auch, Diskussionen und Informationen in thematischen Threads zu organisieren, um die Übersichtlichkeit und Nachvollziehbarkeit zu verbessern.

7.5 Effizienzsteigerung als Ziel

Letztendlich geht es bei all diesen Bemühungen um die Steigerung der Effizienz. Durch den Einsatz moderner Kollaborations- und Produktivitätstools können Unternehmen ihre Prozesse optimieren, Ressourcen besser nutzen und die Zeit, die für die Erledigung von Aufgaben benötigt wird, verkürzen. Die Automatisierung wiederkehrender Aufgaben und die Integration von intelligenten Technologien wie KI tragen dazu bei, Engpässe zu beseitigen und menschliche Ressourcen für kreativere und strategischere Aufgaben freizusetzen.

7.6

Fazit

Die heutige Geschäftswelt erfordert eine proaktive Herangehensweise an Zusammenarbeit und Produktivität. Moderne Technologien, einschließlich innovativer Kollaborationsplattformen, bieten Unternehmen die Werkzeuge, die sie benötigen, um effizienter zu arbeiten, die Kommunikation zu verbessern und letztendlich ihre Wettbewerbsfähigkeit zu steigern.

Gleichzeitig sollte man jedoch nicht vergessen, dass Technologie nur ein Mittel zum Zweck ist. Eine starke Unternehmenskultur, klare Kommunikation und eine offene Einstellung zur Veränderung sind entscheidende Elemente, um die Vorteile der modernen Zusammenarbeit und Produktivität voll auszuschöpfen.

Zurück zur Inhaltsangabe

Ihr betrieblicher Schutzschild

Da bin ich mir sicher

Zurück zur Inhaltsangabe

8. Sicherheit

Modernes Arbeiten definiert sich branchenübergreifend durch die Möglichkeiten des orts-, zeit- und geräteunabhängigen Arbeitens. Damit einher geht die Notwendigkeit von erhöhter IT-Sicherheit, um den Zugriff auf sensible Firmendaten auch weiterhin ausreichend schützen zu können. In diesem Zusammenhang gilt es daher nicht nur die Endgeräte und Identitäten selbst abzusichern, sondern auch genau festzulegen wann, von wo und wie auf bestimmte Inhalte, Informationen und Anwendungen zugegriffen werden darf.

8.1 Zero Trust

Das Kernprodukt der modernen Anforderungen an die IT-Sicherheit ist Zero-Trust. Dabei handelt es sich um ein Konzept, bei dem strikt davon ausgegangen wird, dass keiner Komponente mehr vertraut werden kann. Entsprechend müssen sich Benutzer, Geräte und Dienste unabhängig von ihrer aktuellen Lokation stets explizit authentifizieren, bevor Zugriffe auf die Infrastruktur oder Firmendaten autorisiert werden dürfen. Netzwerktechnisch wird beispielsweise nicht länger zwischen Zugriffen aus dem Firmennetzwerk oder dem Internet unterschieden, da jede Anforderung automatisch so behandelt wird, als würde sie aus einem öffentlichen Netzwerk stammen. Dies hat kontinuierliche Authentifizierung und lückenlose Verschlüsselung zur Folge. Gleichzeitig werden sowohl an Mitarbeiter als auch an Administratoren lediglich minimale Berechtigungen (Least-Privilege Principle) vergeben und fortwährend überwacht. Mithilfe von künstlicher Intelligenz können so Auffälligkeiten und Anomalien frühzeitig erkannt und etwaige Gefahren direkt unterbunden werden.

Generell gilt es jedoch zu beachten, dass ein Zero-Trust-Modell stets ein ganzheitliches Sicherheitskonzept darstellt.
In den kommenden Abschnitten werden einige mögliche Bestandteile eines solchen Konzepts dargestellt.

8.2 Identity Protection

Identity Protection liefert zuverlässigen Schutz gegen Identitätsdiebstahl und -missbrauch. Diese Schutzmaßnahme überwacht das Anmeldeverhalten und den Anmeldekontext von Endnutzern. Bei Auffälligkeiten wird – je nach Kritikalität – beispielsweise eine Warnmeldung erzeugt, ein zusätzlicher Authentifizierungsfaktor angefordert oder eine Kennwortänderung erzwungen.

Maßgeblich hierfür sind Anmeldungen außerhalb fest definierter Parameter (z.B. nicht vertrauenswürdige Lokationen) oder Anmeldungen, die aus etwaigen anderen Gründen nicht in das typische Anmeldeverhalten des jeweiligen Benutzers fallen. Auch die Integrität der Anmeldedaten selbst wird konstant überprüft, was zum Beispiel durch Abgleich mit bekannten Datenbanken im Darknet geschieht.

8.3 Conditional Access

Mithilfe von Conditional Access lässt sich granular steuern, ob und wie ein bestimmter Mitarbeiter, abhängig vom aktuellen Kontext, Zugriff auf Anwendungen und Informationen erhält. Grundlage hierfür liefert zum Beispiel das hierfür verwendete Endgerät und dessen aktueller Sicherheits- bzw. Compliance-Status oder die gegenwärtige Geo-Lokation.

Dies kann etwa zu Folge haben, dass der Zugriff von einem Firmengerät auf eine sensible Unternehmensanwendung nur dann möglich ist, wenn die dort installierte Antivirenlösung aktuell ist. Gleichzeitig wird demselben Benutzer mit demselben Gerät die Verwendung der Applikation bei einer Anmeldung außerhalb von Europa prinzipiell blockiert.

Die zugrundliegenden Bedingungen (z.B. Herkunft der Anforderung, Geräteinformationen, etc.) können granular und pro Dienst gestaltet und mit entsprechenden Aktionen (Zugriff zulassen, weitere Authentifizierungsschritte, Zugriff verweigern, etc.) verknüpft werden.

8.4 Digital Rights Management (DRM)

Mithilfe von DRM lässt der Zugriff auf digitale Inhalte kontrollieren und beschränken. Bei diesen Inhalten kann es sich um Dokumente, Dateien oder eine andere Form von geistigem Firmeneigentum handeln. Mittels DRM kann entsprechend Einfluss darauf genommen werden, ob und wie diese Daten beispielsweise mit Dritten geteilt werden können. So können bestimmte Dokumente u.a. nicht per E-Mail versendet oder ausgedruckt werden. Dies wird mithilfe geeigneter Klassifizierung, Verschlüsselung und dynamischer Zugriffskontrolle gewährleistet.

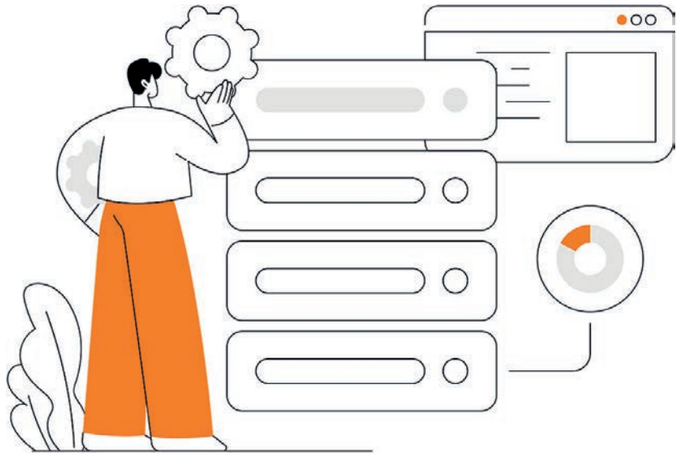
8.5 Data Loss Prevention (DLP)

DLP bezeichnet alle Maßnahmen, die ergriffen werden, um einem Datendiebstahl oder einem „einfachen“ Datenverlust vorzubeugen. DLP unterstützt Anwender beim Einhalten vorhandener Prozesse und Vorgaben und liefert den technischen Werkzeugkasten für den Umgang mit schützenswerten Informationen, indem vertrauliche Daten klassifiziert und überwacht werden. Zugriffe auf Daten und deren Nutzung wird erfasst und protokolliert. Verdächtige Aktivitäten werden automatisch erkannt und blockiert. DLP wird nahtlos in das bestehende Portfolio der Informationssicherheit (siehe auch DRM) und dem Informationslebenszyklus integriert.

Ganz nach oben mit Ihrem neuen digitalen Arbeitsplatz

Zurück zur Inhaltsangabe

9. Workspace Services



Workspace Services sind ein wichtiger Bestandteil moderner Arbeitsumgebungen, die darauf abzielen, die Effizienz zu steigern und die Arbeitsorganisation zu optimieren. In einer Zeit, in der die Arbeitswelt sich ständig verändert und flexibler wird, sind Workspace Services ein unverzichtbares Instrument, um den Anforderungen von Unternehmen und Mitarbeitern gerecht zu werden. Diese Beschreibung wird Ihnen einen umfassenden Überblick über Workspace Services geben, ihre Bedeutung für Unternehmen und Mitarbeiter erläutern und praktische Tipps zur Implementierung und Nutzung bieten.

Workspace Services beziehen sich auf eine Vielzahl von Dienstleistungen und Ressourcen, die es Unternehmen und Mitarbeitern ermöglichen, effizienter zu arbeiten und ihre Arbeitsumgebung flexibler zu gestalten. Dazu gehören flexible Arbeitsplatzlösungen, gemeinsam genutzte Ressourcen und Dienstleistungen sowie digitale Tools, die die Kommunikation und Zusammenarbeit unterstützen.

Die Arbeitswelt hat sich in den letzten Jahrzehnten stark verändert. Früher waren traditionelle Büros mit festen Schreibtischen und starren Arbeitszeiten die Norm. Heute suchen Unternehmen nach flexibleren Lösungen, um den unterschiedlichen Bedürfnissen ihrer Mitarbeiter gerecht zu werden. Workspace Services sind eine Reaktion auf diese Veränderungen und bieten flexible Arbeitsmöglichkeiten, die es den Mitarbeitern ermöglichen, produktiver und zufriedener zu arbeiten.

Workspace Services bieten zahlreiche Vorteile sowohl für Unternehmen als auch für Mitarbeiter. Unternehmen können ihre Betriebskosten reduzieren, die Mitarbeiterbindung erhöhen und flexibler auf Veränderungen reagieren. Mitarbeiter profitieren von einer verbesserten Work-Life-Balance, mehr Flexibilität und einer besseren Arbeitsumgebung, die ihre Produktivität steigert.

Workspace Services umfassen auch die gemeinsame Nutzung von Büroinfrastruktur und -diensten. Unternehmen können Büroflächen, Besprechungsräume, Drucker und andere Ressourcen gemeinsam nutzen, um Kosten zu reduzieren und effizienter zu arbeiten.

Workspace Services bieten auch eine breite Palette von Technologie- und Kommunikationsdiensten, die die Zusammenarbeit und Kommunikation erleichtern. Dazu gehören Tools für Videokonferenzen, Projektmanagement-Software und Cloud-Speicherlösungen, die es den Mitarbeitern ermöglichen, von überall aus effizient zu arbeiten.

Nachhaltigkeit und soziale Verantwortung werden immer wichtiger in der Arbeitswelt. Workspace Services können dazu beitragen, nachhaltigere Arbeitsweisen zu fördern, indem sie die Nutzung von Ressourcen optimieren und umweltfreundliche Lösungen bieten. In diesem Kapitel werden Ansätze zur Förderung von Nachhaltigkeit und sozialer Verantwortung in der Arbeitswelt diskutiert. Workspace Services sind mehr als nur ein aktueller Trend in der Arbeitswelt. Sie bieten Unternehmen die Möglichkeit, ihre Arbeitsumgebung flexibler zu gestalten, Kosten zu reduzieren und die Zufriedenheit der Mitarbeiter zu steigern.

10.

Schlusswort

Modern Workplace und damit neue Arbeitsmodelle stellen mal eben die IT auf den Kopf. Ein breites Thema, das von immer mehr Firmen adressiert wird und in unterschiedlichen Ausprägungen Gefallen findet. Jedoch ein großer Schritt in Richtung hybride IT-Landschaft, doch haben wir diese nicht schon heute?

Modern Workplace und dessen Transformation ist kein Ziel, es ist eine Reise mit vielen Möglichkeiten und Stolperstellen.

Mit diesem eBook haben Sie hoffentlich inspirierende Ideen für die Optimierung Ihres eigenen Arbeitsplatzes bekommen. Wir hoffen, dass Sie die Informationen und Tipps nutzen können, um Ihre Arbeitsumgebung zu verbessern und so die Effizienz und Organisation am Arbeitsplatz zu steigern.

Uns ist bewusst, dass wir mit diesem eBook nie am Zahn der Zeit sein werden. Für eine persönliche Beratung, abgestimmt auf Ihre Bedürfnisse, sprechen Sie uns gerne an.

Zurück zur Inhaltsangabe

Die ∞ Autoren

Zurück zur Inhaltsangabe

Matthias P.
Senior Architect Modern Workplace, mahr als 20 Jahre IT Erfahrung im Microsoft Umfeld, Schwerpunkte Zusammenarbeit und Kommunikation, Identitäts- und Gerätesicherheit und IT Governance

Ghulam
Consultant mit dem Schwerpunkt Microsoft Azure, Modern Workplace und Security. Er hat sich die letzten Jahre als System Engineer und Consultant mit dem Schwerpunkt Microsoft 365 ein großes Wissen mit praktischen Erfahrungen angesammelt.

Florian
Senior Consultant, mehr als 12 Jahre IT Erfahrung mit Schwerpunkt im Enduser Computing mit Microsoft und Citrix Technologien

Peter
Senior Consultant, mehr als 25 Jahre IT Erfahrung mit Schwerpunkt Client Mangement

René
René ist der IT-Dinosaurier. 30 Jahre IT Erfahrung. Gestartet mit 2400 BAUD und UUCP, über FoxPro , VB, Delphi, C++, C#, Objective C, klarer Entwicklerhintergrund. Seit 10 Jahren Beratung in allen Bereichen der IT und Erweiterung des Wissens Richtung Cloud und Cloudstrukturen. Als Senior Consultant aktuell der Schwerpunkt VDI und AVD, Konzeption und Umsetzung. Bei Orange Business aktuell der PO Digital Workplace Services

Dominik
Dominik ist mit den ersten Windows-Betriebssystemen aufgewachsen und hat seine Leidenschaft für Technik vor mehr als 10 Jahren zum Beruf gemacht. Neben dem Berater-Gen kennzeichnet ihn eine ausgeprägte Hands-On-Mentalität. Als Senior IT Architect umfasst sein Aufgabengebiet die ganzheitliche Beratung, das Design und die Implementierung von Lösungen zum Thema Modern Workplace. Sein Schwerpunkt liegt dabei auf dem Microsoft- und Citrix-Portfolio sowie Hybrid- und Cloud-Infrastrukturen. Umfassende Zertifizierungen belegen Dominiks Expertise in diesen Bereichen. Kunden schätzen vor allem seine Motivation und seinen Weitblick sowie die Genauigkeit seiner Arbeit.

Matthias S.
Matthias beschäftigt sich seit über 20 Jahren mit dem Bereich End-User-Computing und dessen Bereitstellung in großen Kundenumgebungen mit bis zu 200.000 Anwendern. Dabei gehören Design und Architektur sowie Kundenworkshops zu seinen Hauptaufgaben. Er zählt zu den Industrie-Experten und wurde dafür 2018 von Citrix als Citrix Technology Professional (CTP) ernannt. Sein Schwerpunkt liegt im Microsoft und VDI Umfeld sowie Automatisierung mit Microsoft PowerShell und API's. Er ist Sprecher auf nationalen und internationalen Veranstaltungen.

Bernd
Bernd ist seit 20 Jahren in der IT tätig, und dort anfänglich speziell im Bereich Terminalserver und Citrix. Er hat sich aber dann in den letzten Jahren mehr und mehr auf Cloud Technologien spezialisiert (verstärkt auf Azure) und sich so auch umfassend zum Cloud Solution Architect zertifiziert. Themen, wie Sicherheit, Management und Architektur in der Cloud gehören ebenso zu seinen Kernkompetenzen, wie auch die Konzeptionierung von Kundenumgebungen mit entsprechendem Design Ausblick und die Beratung in entsprechenden Kundenworkshops.

Bereit für die Zukunft?

orange™ Business