novaCapta

Whitepaper

Endpoint Management & Protection

Wie der Microsoft Endpoint Manager Sie in unserer mobilen Arbeitswelt unterstützt

DE

novaCapta GmbH
Im Mediapark 5c
50670 Köln

T +49 (0)221 58919 343
M info@novacapta.com
W www.novacapta.com

CH

novaCapta Schweiz AG
Industriestrasse 5a
6210 Sursee

T +41 (0)41 392 20 00
M info.schweiz@novacapta.com
W www.novacapta.ch

Behalten Sie Ihre Endpunkte im Griff

Menschen arbeiten immer mobiler, Anwendungen wandern in die Cloud. New Work, der Siegeszug des Home Office und zahlreiche Remote-Anwender*innen erschaffen in einer zunehmend fragmentierten Arbeitwelt IT-Szenarien, in denen es ein „innerhalb der Sicherheitsgrenzen“ nicht mehr gibt. In dieser hybriden Welt ist der **Endpoint der neue Arbeitsplatz**, der verwaltet und mehr denn je geschützt werden muss.

Der Microsoft Endpoint Manager unterstützt Sie in Ihrem Arbeitsalltag

Aber wie können Sie die ständig steigende Zahl der mobilen Endpunkte bereitstellen, verwalten und gleichzeitig bis ins Home Office absichern? Wie können Sie die gestiegenen Herausforderungen im Clientmanagement meistern?

Und wie lässt sich der schwierige Balanceakt zwischen der Usability der Nutzer, einer komfortablen Einrichtung und der Kontrolle der Geräte all Ihrer Mitarbeitenden lösen?

Unterstützung für Ihren Alltag

Eine umfassende Antwort liefert der Microsoft Endpoint Manager, der sämtliche Aufgaben des Clientmanagements unter einem Dach vereint und Ihre IT-Abteilung im Arbeitsalltag unterstützt.

Dabei sind die grundlegenden Funktionen bereits in der Microsoft 365 E3 oder Enterprise Mobility + Security E3 Lizenz enthalten. Und falls Sie weitere Vorteile nutzen möchten, bietet sich immer noch die Möglichkeit eines Lizenz-Upgrades an.

In diesem Whitepaper lesen Sie, welche Hürden Sie mit den Funktionen des Microsoft Endpoint Manager meistern, um für die Herausforderungen der „neuen Art des Arbeitens“ gerüstet zu sein.

6

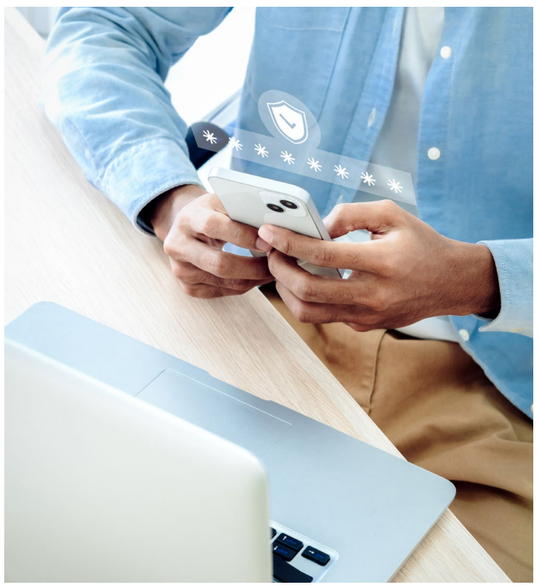
Herausforderungen, die Sie mit dem Microsoft Endpoint Manager meistern

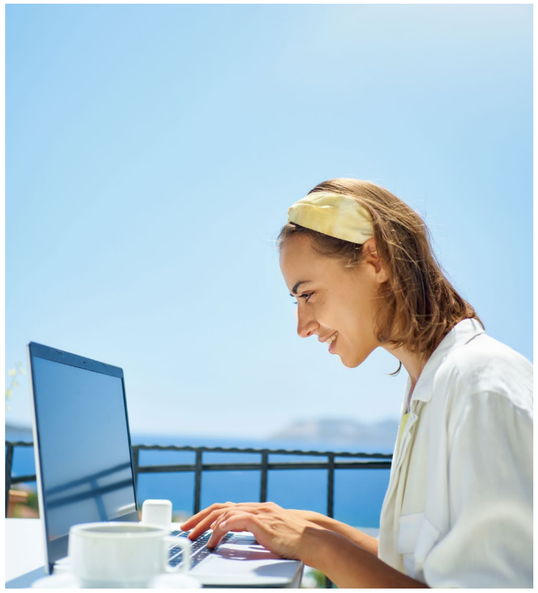
1

Endpoints außerhalb des Perimeters absichern

Immer mehr Benutzer*innen, Anwendungen, Geräte und Verbindungen im Netzwerk und der Cloud machen es schwieriger, jedem und jeder einzelnen Ressource den richtigen Zugriff zu gewähren. Traditionelle Sicherheitskonzepte stoßen hier an ihre Grenzen, weshalb Endgeräte leicht zum schwächsten Glied in Ihrer Zero Trust-Sicherheitsstrategie werden können.

Um Daten und wichtige Assets auch außerhalb des Unternehmensnetzwerks zu schützen, müssen Sie sicherstellen, dass die verwendeten Endpoints über vertrauenswürdige Identitäten verfügen. Und zwar völlig unabhängig davon, ob es sich um ein privates Bring Your Own Device (BYOD), ein Corporate Owned, Personally Enabled (COPE) oder um ein unternehmenseigenes Gerät handelt.





Dafür registrieren Sie diese Geräte in der Azure Active Directory (Azure AD), um sie anschließend mit dem Microsoft Endpoint Manager bzw. Microsoft Intune zu verwalten. Für einen Compliance-Check erstellen Sie via Conditional Access individuelle Richtlinien, die in bestimmten Situationen bestimmte Aktionen vorgeben:

- **Sind alle Standards erfüllt?**
- **Ist die Festplatte verschlüsselt?**
- **Sind alle Windows-Updates installiert?**
- **Wann war der letzte Virenscan?**
- **Arbeitet der MS Defender ordungsgemäß?**
- **Und noch vieles mehr!**

Mit den Antworten teilen Sie die Endpoints in verschiedene Bedrohungsstufen ein und legen darauf basierend fest, ob das jeweilige Gerät Zugriff auf Unternehmensressourcen erhält oder nicht.

2

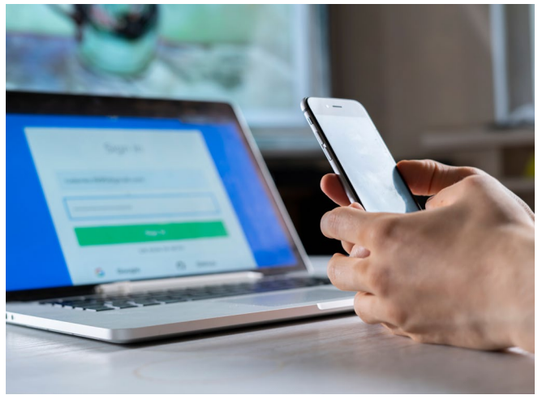
Multi-Faktor-Authentifizierung einführen

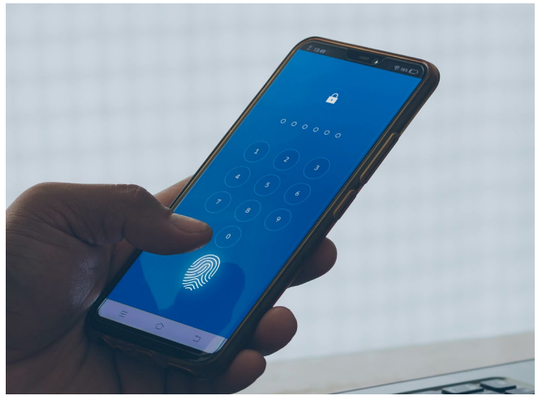
Die Authentifizierung von Zugriffen ist einer der wichtigsten Bausteine von Zero Trust. Und da schwache Zugangsdaten ein Hauptgrund für Datenpannen sind, kann die Multi-Faktor-Authentifizierung (MFA) mit einem zusätzlichen Identifizierungsmerkmal das Schutzniveau deutlich erhöhen.

Der Vorteil mit MFA

Dabei liegt ein großer Vorteil der MFA mit Hilfe von Azure AD und Conditional Access darin, dass Sie diese während bestimmter Anmeldeereignisse aktivieren und deaktivieren können:

- Zum Beispiel brauchen Sie die MFA nicht vollständig scharf schalten, wenn einer Ihrer Mitarbeitenden auf einen Dienst von einer bekannten IP-Adresse aus dem Firmenbüro zugreifen möchte
- Oder auch dann nicht, wenn er ein vollständig verwaltetes Unternehmensgerät nutzt
- Andererseits sollte die MFA immer dann erfolgen, wenn es sich um private und nicht zum Unternehmensbestand gehörende Geräte handelt



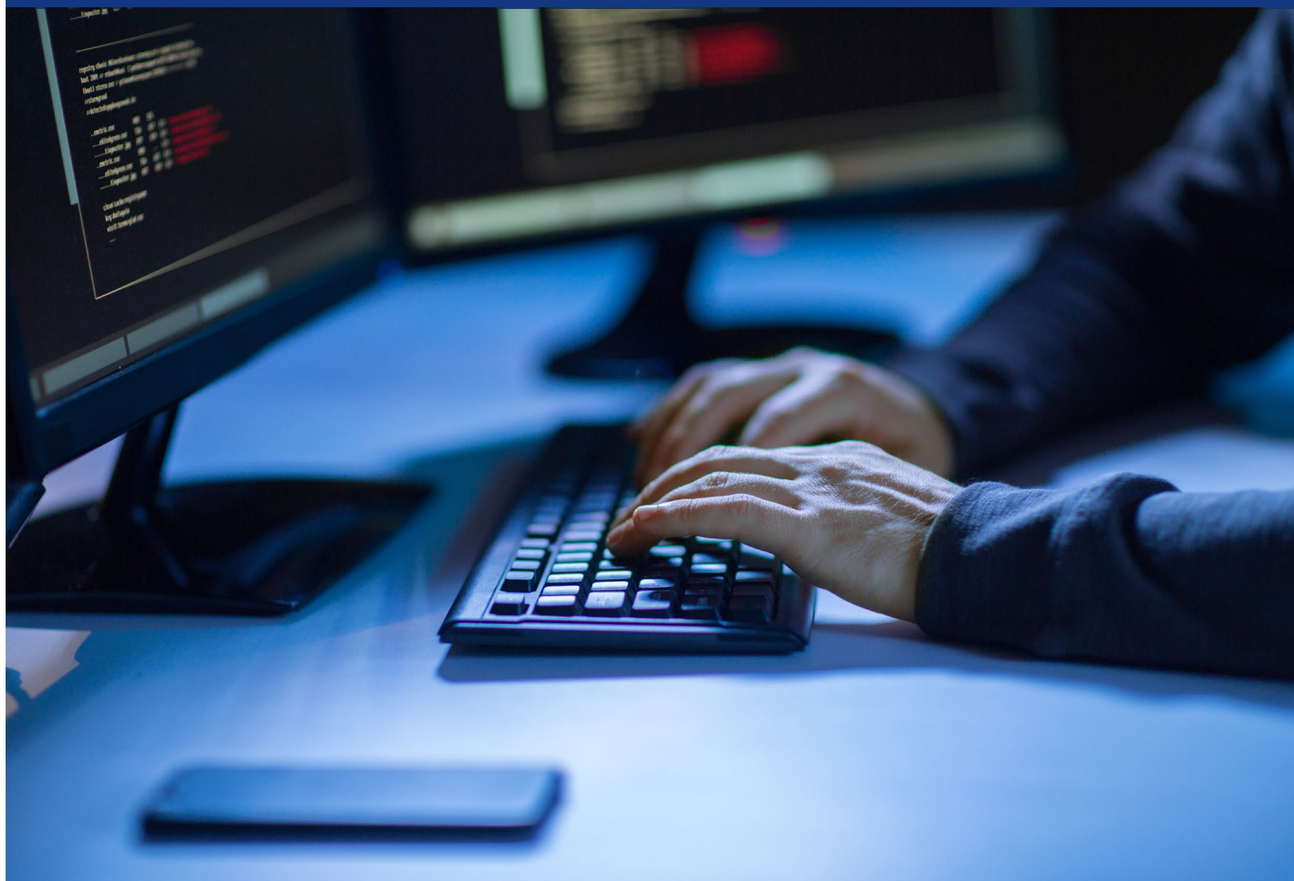


Letztendlich können Sie durch bestimmte Regelungen selbst und individuell festlegen, welche Authentifizierungsprozesse nötig sind und den Nutzer*innen damit bei größter Sicherheit noch den gewünschten Anmeldungskomfort bieten.

Zero Trust: Wie das Prinzip Misstrauen die Sicherheit erhöht

Bei Zero Trust handelt sich um ein modernes Cyber-Security-Konzept, das auf einem strengen Prozess der Identitätsprüfung basiert. So geht man immer und grundsätzlich davon aus, dass kein*e Nutzer*in, keine Anfrage, kein Dienst, keine Anwendung und kein Gerät vertrauenswürdig ist – es sei denn, das Gegenteil wird bewiesen. Dieses Vertrauen wird bei jedem internen oder externen Zugriff immer wieder dynamisch auf die Probe gestellt.

Mit der Entwicklung und Migration einer Zero Trust-Lösung entsteht also ein umfangreiches Informations-Framework, in dem wirklich nur absolut authentifizierte und autorisierte Akteure maximal restriktiven Zugriff auf Daten und Anwendungen im Netzwerk erhalten. Die Möglichkeiten für potenzielle Angreifer sind damit stark eingeschränkt.



3

Neue Geräte im Home Office bereitstellen und einrichten

Eine weitere Herausforderung, die sich durch die hybride Arbeitswelt ergibt, ist die Bereitstellung neuer Geräte im Home Office. Hier bietet der Microsoft Endpoint Manager den Vorteil, dass das komplette Deployment über den Windows Autopilot via Zero Touch Provisioning erfolgen kann. Sprich: Neue Geräte lassen sich mitsamt Betriebssystem-Setup, VPN- und WLAN-Profilen, Software sowie Richtlinien, Einstellungen und Sicherheitsstandards passend zum Mitarbeiterkonto über die Cloud vorkonfigurieren.

Dass der Hersteller das neue Gerät direkt auch über die OEM-Schnittstelle registrieren und direkt an den Mitarbeiter oder die Mitarbeiterin schicken kann, macht es umso einfacher. **Dann heißt es im Home Office nur noch auspacken, auf Knopfdruck einrichten und sicher losarbeiten** – die Benutzer*innen müssen das neue Gerät weder im Büro abholen noch sich in ein VPN einwählen oder den Prozess manuell anstoßen.

4

Private und berufliche Daten trennen

Ob das eigene Gerät beruflich genutzt wird (BYOD) oder ob es sich um ein Company Owned, Personally Enabled Device (COPE) handelt – als Unternehmen will man verhindern, dass sich private und geschäftliche Daten vermischen. Hier nur ein Beispiel aus der Praxis:

- Der Mitarbeiter speichert seine Outlook-Kontakte auf seinem Smartphone
- Öffnet er dann WhatsApp, um einen privaten Chat zu starten, möchte der Messenger von Facebook auf das lokale Adressbuch zugreifen
- Bestätigt der Nutzer dies unbedacht, sind alle Unternehmenskontakte plötzlich da, wo sie eigentlich nicht hingehören

Mit dem Endpoint Manager können Sie mittels Azure AD-Anbindung Privates vom Geschäftlichen trennen. Und zwar mit Möglichkeiten, die sich zwischen der vollen Kontrolle, unterschiedlichen Arbeitsprofilen oder einer regulären Multi-Faktor-Authentifizierung für diverse Anwendungen bewegen.

Privates und Berufliches trennen mit dem Microsoft Endpoint Manager

Von Forrester und Gartner zum Leader ernannt

Unternehmen verlassen sich gerne auf die unabhängigen Bewertungen renommierter Analystenhäuser. Einen der meistbeachteten Anbietervergleiche liefert **Forrester Research** mit der Forrester Wave, bei dem Microsoft im Bereich Unified Endpoint Management (UEM, Q4 2021) als Leader anerkannt wurde.

Der Forrester-Bericht stellt fest, dass Microsoft **„Kunden bei der Migration zu einer modernen Endpunktverwaltung hervorragend unterstützt"** und dass seine Desktop Analytics-Funktionen zu den fortschrittlichsten in der Bewertung gehören.

Das **Beratungsunternehmen Gartner** sieht das ähnlich und hat Microsoft im Magic Quadrant für Endpunktschutzplattformen (EPP) 2021 zum Leader mit der höchsten Position für die Fähigkeit zur Umsetzung ernannt. Laut Gartner verfügen Leaders „über **umfassende Fähigkeiten im Bereich des fortschrittlichen Malware-Schutzes und über bewährte Management-Fähigkeiten für große Unternehmenskunden.**

Zusätzlich bieten Sie ganzheitliche Plattformen an, die es Kunden ermöglichen, ihre anderen Tools zu konsolidieren und eine Lösung von einem einzigen Anbieter zu übernehmen."

5

Probleme und Bedrohungen proaktiv antizipieren

Ein Notebook, das zum Starten häufig länger als fünf Minuten braucht? Eine App, die ständig abstürzt? Einblicke in die Probleme und Zustände von Geräten und Apps, die sich von Help-desk- oder IT-Teams aus der Ferne bearbeiten lassen, können die Produktivität steigern und Frustrationen der Nutzer*innen verringern.

Endpoint Analytics in Endpoint Manager bietet diese Funktionen, die das digitale Erlebnis der Mitarbeitenden unterstützen. Das gleiche gilt für den Schutz vor digitalen Bedrohungen, denn unzureichend gesicherte Endgeräte sind ein willkommenes Einfallsto für Viren, Verschlüsselungstrojaner, Spyware und Datendiebstähle.

Mit dem Endpoint Manager schützen Sie nicht nur Ihre Daten, sondern wissen auch, wo Gefahren auftreten, um diesen proaktiv zu begegnen. So bietet der optionale Defender für Endpunkt eine KI-basierte Prozessanalyse und verhaltensbasierte Überwachung.

Zudem lassen sich mittels Microsoft Defender Advanced Threat Protection (ATP) Informationsquellen für Richtlinien zur Gerätekonformität und Regeln für den bedingten Zugriff auf Geräte integrieren.

6

Alle Tools auf einer Plattform konsolidieren

Ein wichtiger Aspekt in puncto Endpoint Management sind die Kosten. Im Idealfall sollten Sie von einer Lösung profitieren, die andere Drittanbieter-Produkte überflüssig macht, weil die Lizenzen bereits vorliegen und die nötigen Tools bereits in die vorhandene Plattform integriert sind.

Der Microsoft Endpoint Manager ist solch ein Fall: Indem die zentrale Management-Plattform viele Produkte unter einer einzigen Lizenz konsolidiert, sorgt sie dafür, dass die „neue Art des Arbeitens" umfassend abgesichert und effektiv zu verwalten ist. Administratoren erhalten eine Konsole, die eine nahtlose Integration aller Endgeräte ins Windows-Betriebssystem ermöglicht – ganz gleich, ob es sich dabei um Devices mit Windows, iOS, MacOS, Android und bald auch Linux handelt.

So trägt der Microsoft Endpoint Manager dazu bei, die Investitionen von Unternehmen in ihre digitale Infrastruktur zu maximieren, indem die IT-Produktivität verbessert und das Risiko zunehmender Cyber-Security-Bedrohungen in der wachsenden Endpoint-Landschaft vermindert wird.

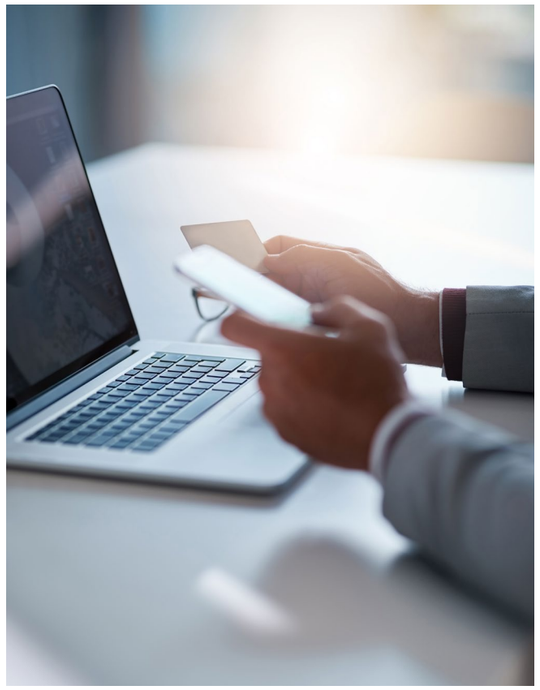
Alle Tools in der zentralen Management Plattform integriert

Nutzen Sie mehr IQ fürs Clientmanagement

Sie merken: Der Microsoft Endpoint Manager ist eine integrierte Lösung für die Verwaltung all Ihrer Geräte, die die Endpunktsicherheit, Geräteverwaltung und Cloudaktionen in einer einheitlichen Verwaltungsplattform umfasst.

Er vereint Azure AD für die Verwaltung von Identitäten mit dem Configuration Manager plus Intune ohne komplexe Migration. Sie profitieren von nur einer Lizenzierung und können Ihre vorhandenen Investitionen und gleichzeitig die Vorteile der Microsoft-Cloud nutzen.

Dazu kommen der Windows Autopilot zur einfachen Bereitstellung von Geräten, Endpoint Analytics für datengesteuerte Empfehlungen und der Microsoft Defender, um Endpoints gegen Cyberbedrohungen abzusichern.



Und falls Sie Fragen zum Thema haben oder noch mehr über die Möglichkeiten erfahren möchten, die der Endpoint Manager Ihnen bietet, ist **novaCapta als Microsoft Premium Partner** gerne für Sie da: Gemeinsam finden wir die beste Auswahl aus den Microsoft Bausteinen, damit Sie für die Herausforderungen der neuen Arbeitswelt gerüstet sind.

novaCapta

Ihr Microsoft Premium Partner

Kontaktieren Sie uns!

Bei Fragen zu unseren Themen sind wir gerne für Sie da und finden gemeinsam mit Ihnen die beste Auswahl aus den Microsoft Bausteinen

DE

novaCapta GmbH
Im Mediapark 5c
50670 Köln

T +49 (0)221 58919 343
M info@novacapta.com
W www.novacapta.com

CH

novaCapta Schweiz AG
Industriestrasse 5a
6210 Sursee

T +41 (0)41 392 20 00
M info.schweiz@novacapta.com
W www.novacapta.ch