CCS365

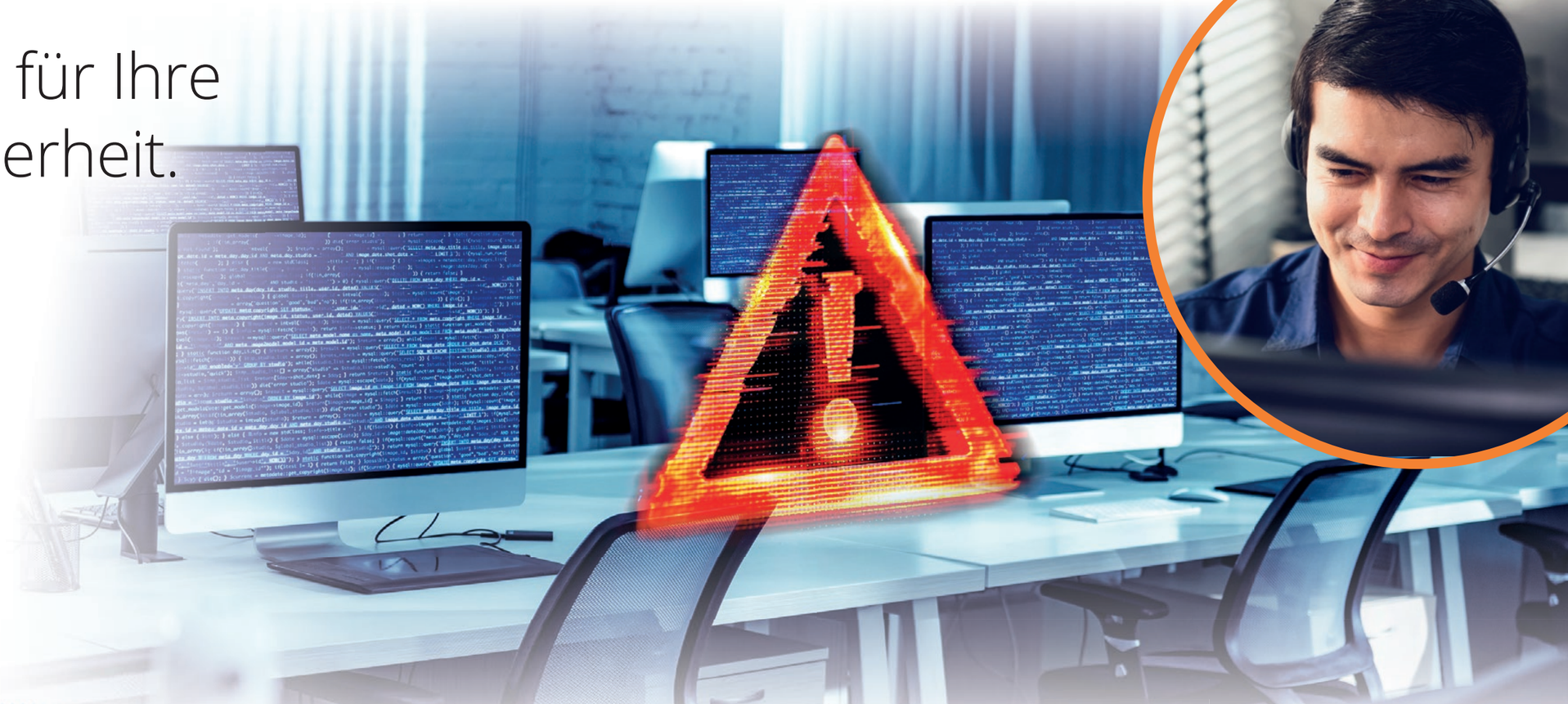
Cloud | Consulting | Services

Gold Microsoft Partner

Microsoft

CCS 365 Security Services

Microsoft Tools für Ihre optimierte IT-Sicherheit.



Endpoint Protection Services

Ein entscheidendes EXTRA für Ihre IT-Sicherheit.

Warum Endpoint Protection Services?

Sie wollen Angriffe auf die Endpunkte Ihrer IT besser verhindern und erweiterte Bedrohungen rechtzeitig erkennen, untersuchen und optimal reagieren? Sie wollen eine „Verteidigungslinie“ aufbauen, die sich nativ in alle Endgeräte, Identitäten, E-Mails und Anwendungen Ihres Unternehmens integriert? Dann sind Microsoft Tools wie Microsoft 365 Defender oder Defender for Endpoint die richtige Wahl für Sie. Denn diese hybrid und cloudbasierten Endpunkt-Sicherheitsplattformen sind ideal für Unternehmen, die ihre Netzwerke mit einer einheitlichen und alle Devices einschließenden Verteidigungssuite vor und auch nach einem Einbruch schützen wollen.

Diese Vorteile haben Sie mit uns

Microsoft 365 Defender for Endpoint aktiviert Endpunktverhaltenssensoren, die in Windows 10 eingebettet sind. Diese Sensoren sammeln und verarbeiten Verhaltenssignale des Betriebssystems und senden diese an die private, isolierte Cloud-Instanz von Microsoft 365 Defender for Endpoint. Daraufhin erfolgt eine Cloud-Sicherheitsanalyse, die bestimmte Verhaltenssignale in Erkenntnisse, Entdeckungen und empfohlene Reaktionen auf erweiterte Bedrohungen übersetzt. Abschließend greift die Threat Intelligence, die von Microsoft-Jägern und Sicherheitsteams generiert wird und durch Partner wie CCS 365 passgenau ergänzt wird. Sie ermöglicht Microsoft 365 Defender for Endpoint die Tools, Techniken und Verfahren von Angreifern zu identifizieren und Benachrichtigungen zu generieren, wenn sie in den erfassten Sensordaten beobachtet werden.

Sie wollen diesen optimalen Schutz für Ihr Unternehmen? In nur einem Tag konfigurieren wir Microsoft 365 Defender for Endpoint und schulen Ihr Team so, dass die Sicherheits-Plattform garantiert fachgerecht und passgenau genutzt wird.

Exchange Online Protection (EOP)

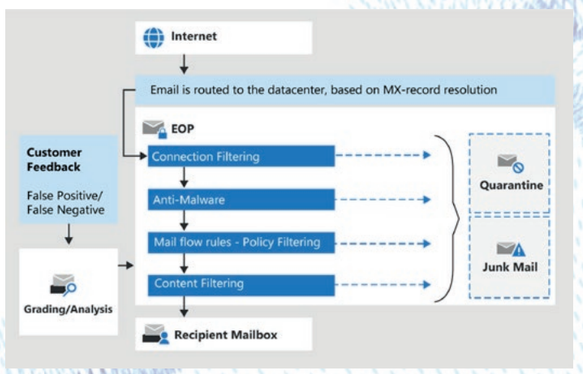
Der ideale Schutz vor Spam und Schadsoftware für sorgenfreies Mailen

Warum empfehlen wir EOP?

Sie wollen besser geschützt sein vor Spam, Schadsoftware und anderen E-Mail-Bedrohungen? Sie wollen Ihre Schutzrichtlinien passgenau konfigurieren und jederzeit aktualisieren können? Mit der richtigen Nutzung des cloudbasierten Filterdienstes Exchange Online Protection (EOP), der in allen Microsoft 365-Anwendungen mit Exchange Online-Postfächern enthalten ist, ist das kein Problem. EOP schützt dank mehrerer Anti-Malware-Engines Ihr Unternehmen vor Spam, Schadsoftware und anderen E-Mail-Bedrohungen. Das Tool überprüft die aktive Nutzlast im Nachrichtentext und alle Nachrichtenanlagen auf Schadsoftware. Außerdem können als weiterer Filter unternehmensspezifische Schutzrichtlinien festgelegt werden.

Was machen wir?

Unser EOP-Paket schließt die korrekte Konfiguration und eine Schulung ein, damit Sie alle Vorteile von EOP auch passgenau und korrekt nutzen und jederzeit anpassen können. Wir helfen Ihnen dabei, die Werte für Ihre maßgeschneiderten Schutzrichtlinien zu definieren und zu konfigurieren. Mit EOP verfügen Sie automatisch über eine umfangreiche Liste von Domänen, von denen bekannt ist, dass sie Spam senden, sowie über mehrere URL-Sperrlisten, die Unterstützung beim Erkennen bekannter schädlicher Links in Nachrichten bieten. Diese Listen werden regelmäßig aktualisiert, so dass Ihr EOP stets auf einem aktuellen Stand ist. Sie haben Fragen zu unserer EOP-Konfiguration und Schulung? Wir helfen Ihnen gern.



Bildnachweis: https://learn.microsoft.com/de-de/microsoft-365/security/office-365-security/eop-about?view=o365-worldwide

Conditional Access Services

Mehrstufige Zugriffs-kontrolle für Ihre optimierte IT-Sicherheit.

Warum brauchen Sie Conditional Access?

Sie wollen die Anmelde- und Zugangsprozesse auf Ihren Devices kontrolliert steuern können und Missbrauch minimieren? Sie suchen nach einer Lösung, riskantes Anmeldeverhalten mittels einer Signalintegration zu erkennen und sofort Gegenmaßnahmen einleiten zu können? Dann empfehlen wir unsere Conditional Access Services. Mit dieser Hybrid- oder Cloud-Azure-AD-basierten Service-Leistung bringen wir die Sicherheitsperimeter Ihrer Benutzer- und Geräteidentitäten auf den bestmöglichen Stand. Nach einer maßgeschneiderten Beratung in der wir mit Ihnen gemeinsam Ihre Sicherheitsrichtlinien festlegen, konfigurieren wir Ihre Devices passgenau.

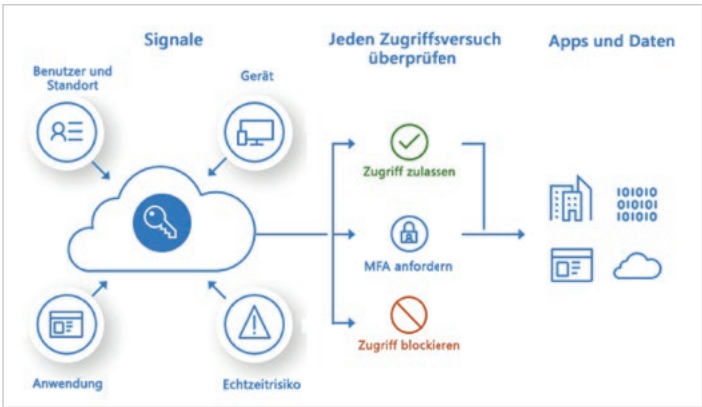
Step One

Im ersten Schritt legen wir die Managed Multi-Faktor-Authentifizierung (MFA) fest, gemäß der mit Ihnen festgelegten Richtlinien für einen bedingten Zugriff . Hierbei handelt es sich meist um "if-Anweisungen", um auf eine Ressource zugreifen zu können; zum Beispiel: Wenn der Leiter der Lohnbuchhaltung auf die Gehaltsabrechnung zugreifen möchte, muss er für den Zugriff zuerst die Multi-Faktor-Authentifizierung durchführen.

Fortsetzung nächste Seite >

Step Two

Der Kern dieser neuen identitätsbasierten Steuerungsebene ist der Azure AD bedingte Zugriff, der auch die Azure AD Identiy Protection einschließt. Diese Funktion erkennt durch eine Signalintegration, einen fehlerhaften Anmeldeversuch und erzwingt die Änderung des Benutzerkennworts, eine Multi-Faktor-Authentifizierung oder eine Zugriffsperrung, bis der Administrator manuelle Maßnahmen ergreift. Je nachdem welche Sicherheitsrichtlinien von Ihnen gemeinsam mit uns hinterlegt werden.



Bildnachweis: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Step Three

Zu unseren Conditional Access Services gehört auch das Einrichten des Location based Access, der Ihnen dabei hilft IP-Adressen besser zu organisieren. Wir legen mit Ihnen vertrauenswürdige IP-Adressbereiche fest. Man kann diese Funktion auch nutzen, um IP-Bereiche ganzer Länder und Regionen zu blockieren, um Ihr Spam und Angriffsrisiko zu minimieren. Und schließlich kümmern wir uns noch um Ihr Device Management. Welche Richtlinien können auf bestimmte User-Gruppen, zum Beispiel externe Mitarbeiter*innen, angewendet werden, sodass sie auf bestimmte Plattformen nur bedingten Zugriff haben oder wo sollen privilegierte Zugriffsrechte eingerichtet werden? Wir entwickeln die Antworten auf alle Ihre Fragen mit Ihnen gemeinsam.

Unser Ziel ist es, Ihnen so zu helfen, dass Sie als Administrator*innen nach Abschluss unserer Conditional Access Services die uneingeschränkte, aber differenzierte Kontrolle über alle Devices-Zugriffe in Ihrem Unternehmen haben.

Schnellübersicht der CCS 365 Security Services Leistungen

	Endpoint Protection	Exchange Online Protection	Conditional Access
Produktleistungen	Aktivierung der Endpointsensoren, Cloud-Sicherheitsanalyse, Threat Intelligence	Connection Filtering, Anti-Malware, Policy Filtering, Content Filtering	Managed MFA, Identity Protection, Location based access, Managed Devices
Umgebung	Hybrid / Cloud (AAD-Joined)	Hybrid / Cloud (AAD-Joined)	Hybrid / Cloud (AAD-Joined)
Konfiguration	✔	✔	✔
Schulung	✔	✔	✔
Bearbeitung	Geschäftszeiten Mo - Fr; 9 - 17 Uhr	Geschäftszeiten Mo - Fr; 9 - 17 Uhr	Geschäftszeiten Mo - Fr; 9 - 17 Uhr
Sprache	deutsch	deutsch	deutsch
Projektdauer	1 Tag	1 Tag	3 Tage
Kosten	1.290,-*)	1.290,-*)	3.490,-*)

*) zzgl. MwSt.

CCS 365 GmbH
Ramersdorfer Straße 1
D-81669 München
ccs365.de
ccs365-shop.de

Sie möchten mehr erfahren?

Wir helfen gerne.
089 666 17 66 0 | info@ccs365.de

Microsoft Solutions Partner
Modern Work