



Cyber security - why and how

Frankfurt, 14 June 2018

ACHEMA

Identitäts- und Datenschutz in der Azure-Cloud

Azure Security– ein Überblick



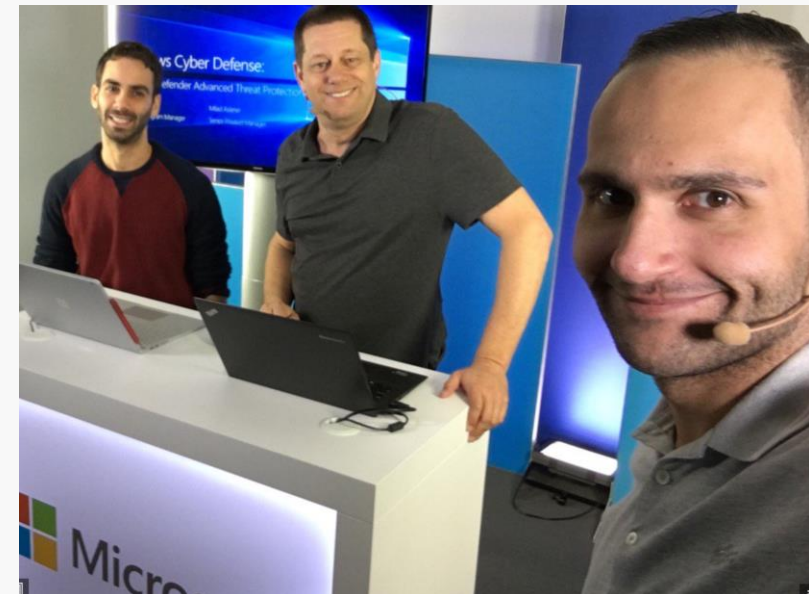
Matthias Partl
Cloud Solution Architect
Identity & Security

Microsoft is the biggest security software
company you've never heard of!

„Microsoft investiert Jahr für Jahr rund eine Milliarde US-Dollar in Cyber-Security.
Datensicherheit, Datenschutz, Transparenz und Compliance haben für uns oberste Priorität. Als globaler Cloud-Anbieter investieren wir gemeinsam mit unseren Partnern konsequent in die neuesten Sicherheitstechnologien, um unsere Kunden ganzheitlich bei ihrer Sicherheitsstrategie zu unterstützen – von der Vorbeugung bis hin zur Bekämpfung erfolgter Angriffe“

Milad Aslaner, Senior Product Manager für Cyber Security, Microsoft Deutschland

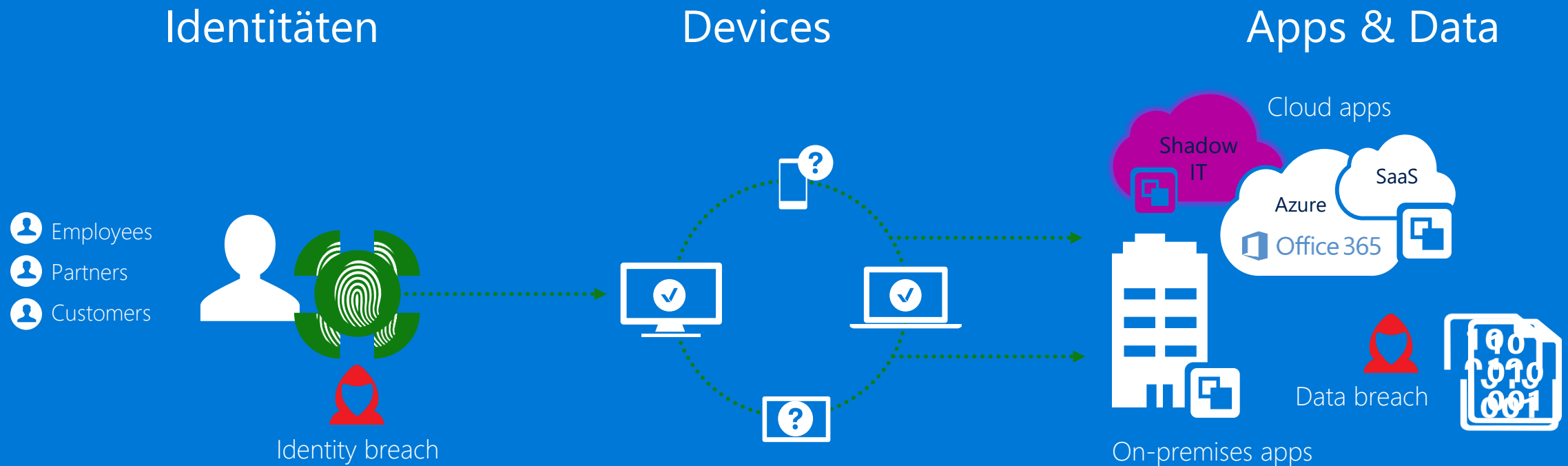
IT-SA Nürnberg, Oktober 2017



Agenda

- ✓ Risiken in Cloud Umgebung
- ✓ Bedrohungslage - 1.Halbjahr 2017
- ✓ Microsoft Security im Überblick
- ✓ Azure – Identity & Access Management (IAM)
- ✓ Azure – Data Protection
- ✓ Azure – Security Management

Ausgangslage: Risiken in Cloud Umgebungen



Übergang zu
Cloud & Mobility

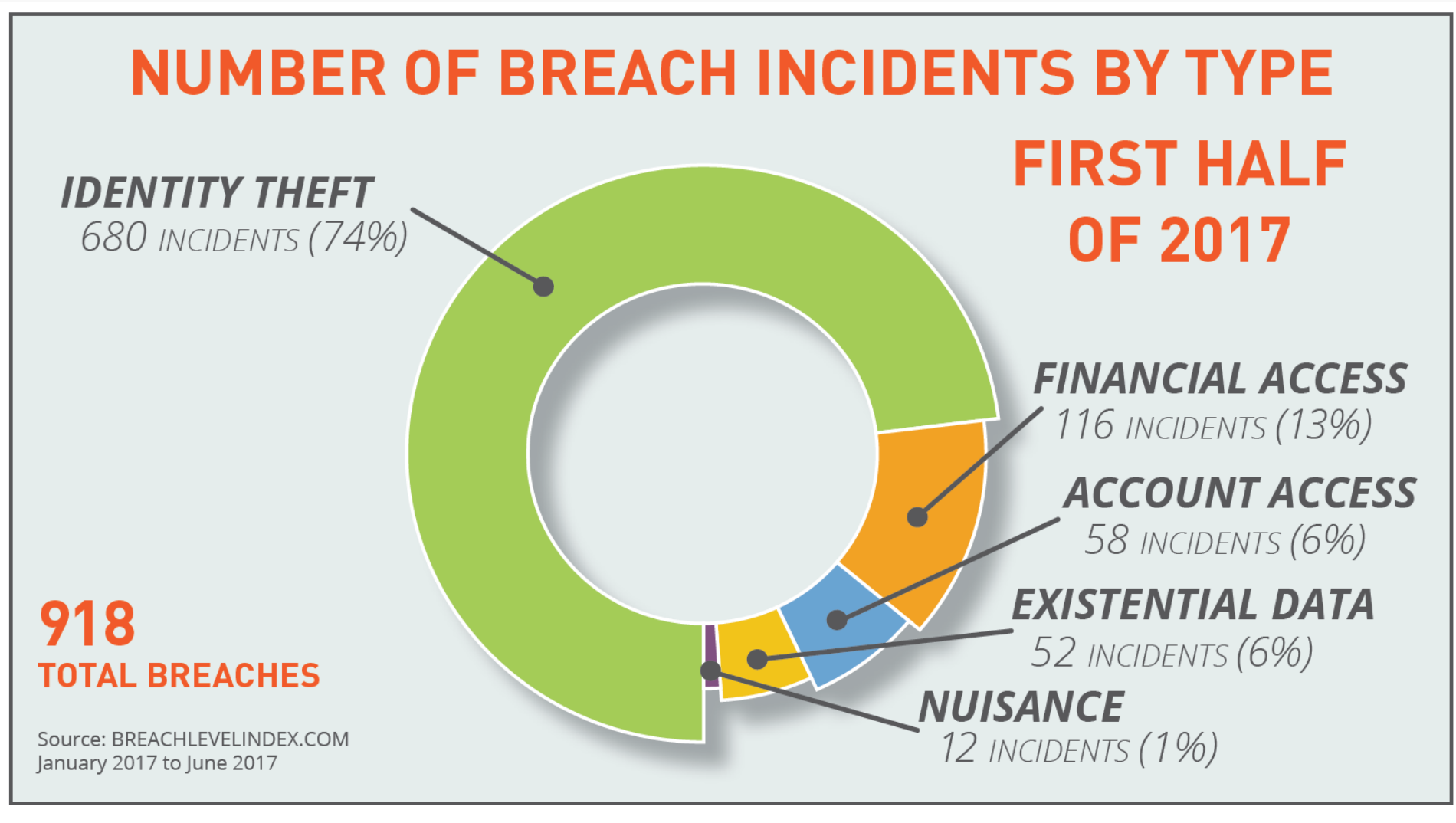


Neue
Angriffsformen



"Identitäten sind der
neue Perimeter"

Bedrohungslage (nach Type) – 1.Halbjahr 2017



Bekannte Angriffsmethoden

- (Spear-) Phishing
- Bruteforce Attacks/Password Cracking
- SQL Injection
- Cross Site Scripting
- DNS Poisoning
- DDoS
- Pass The Hash (PTH)
- Drive-By Attacks

Identitätsdiebstahl durch Spear Phishing Angriff

Von: "Amazon" <metro@krug-entertainment.com>
Betreff: Amazon | Aktuelle Kundenmitteilung! - Ihre Mithilfe ist erforderlich
Datum: 28. April 2018 um 22:26:05 MESZ
An: "partl" <partl@t-online.de>



Aktuelle Kundenmitteilung! - Ihre Mithilfe ist erforderlich.
Samstag, 28.04.2018

Guten Tag,

Durch die Erneuerung des "BDSG" (Bundesdatenschutzgesetzes) ist Amazon EU S.à r.l. als Versandhandelsunternehmen nach §63-67 verpflichtet, Ihre hinterlegten Daten auf Richtigkeit zu überprüfen und zu validieren.

Hierzu bitten wir Sie, Ihre Informationen in einem kurzen Datenabgleich zu bestätigen. Bitte validieren Sie Ihre Identität als primärer Accountinhaber, damit eine erneute Herstellung der Handlungsfähigkeit erfolgen kann.

Bitte seien Sie aufmerksam bei der Eingabe Ihrer Informationen. Sollten die von Ihnen angegeben "Adress"- und "Zahlungsdaten" sich zu den bereits hinterlegten Informationen unterscheiden, ist eine Legitimierung nur noch auf postalischen Weg möglich.

Sollten wir Unregelmäßigkeiten finden, wird sich der Kundenservice innerhalb von 24 Stunden mit Ihnen in Verbindung setzen. Falls Sie innerhalb der 24 Stunden nicht vom Support kontaktiert werden betrachten Sie diese E-Mail als hinfällig.

Jetzt Identität bestätigen

Vielen Dank für Ihr Verständnis! Als kleine Belohnung für die Unannehmlichkeiten erhalten Sie eine 10EUR Amazon - Gutschrift* auf Ihr Gutschein-Konto zugeschrieben, sobald Ihre Daten erfolgreich aktualisiert wurden.

Mit freundlichen Grüßen

Ihr Amazon Service Team

Dies ist eine automatisch versendete Nachricht. Bitte antworten Sie nicht auf dieses Schreiben.

© 1999-2018 Amazon. Alle Rechte vorbehalten.

Handelsregisternummer: R.C.S. Luxembourg B 118 349 - Conseil de gérance der Amazon (Europe) S.à r.l.

Bedrohungslage 2017



Öffnen von gefährlichen E-Mails



Klicken auf Attachments/Links

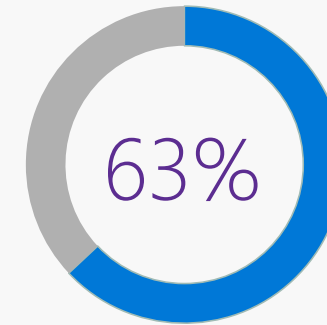
alle 4 Minuten

286 Tage

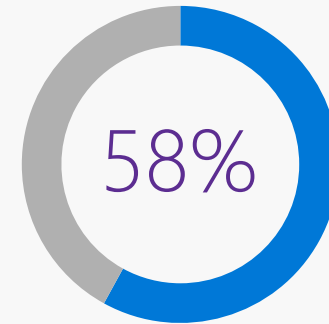
Angriffserkennung

80 Tage

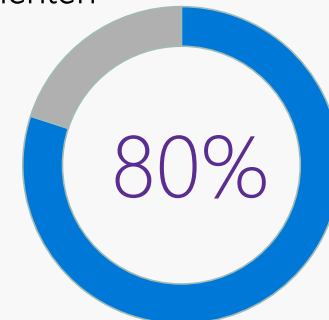
Feststellen des Schadens



Schwache/Standard oder gestohlene Passwörter



Irrtümliches Teilen von vertraulichen Dokumenten



Verbotene SaaS Anwendungen: Schatten IT

Microsoft Security im Überblick



Identity & Access Management

Protect users' identities & control access to valuable resources based on user risk level

Azure Active Directory (Premium)
Azure AD Identity Protection
Microsoft Intune
Windows Hello
Windows Credential Guard



Threat Protection

Protect against advanced threats and recover quickly when attacked

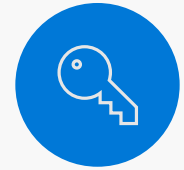
Advanced Threat Analytics
Windows Defender
Advanced Threat Protection
Office 365 Advanced Threat Protection
Office 365 Threat Intelligence



Data Protection

Ensure documents and emails are seen only by authorized people

Azure Information Protection
Windows Information Protection
Office 365 Data Loss Prevention
Office 365 Advanced Security Mgmt.
Transparent Data Encryption (TDE)
Azure Disk Encryption / Bitlocker
Storage Blobs Encryption
Azure KeyVault



Security Management

Gain visibility and control over security tools

Azure Security Center
Windows Defender Security Center
Office 365 Security Center
Microsoft Cloud App Security

Azure Compliance Zertifizierungsnachweise

Global	✓ ISO 27001:2013 ✓ ISO 27017:2015 ✓ ISO 27018:2014	✓ ISO 22301:2012 ✓ ISO 9001:2015 ✓ ISO 20000-1:2011	✓ SOC 1 Type 2 ✓ SOC 2 Type 2 ✓ SOC 3	✓ CSA STAR Certification ✓ CSA STAR Attestation ✓ CSA STAR Self-Assessment ✓ WCAG 2.0
US Gov	✓ FedRAMP High ✓ FedRAMP Moderate ✓ EAR	✓ DoD DISA SRG Level 5 ✓ DoD DISA SRG Level 4 ✓ DoD DISA SRG Level 2 ✓ DFARS	✓ DoE 10 CFR Part 810 ✓ NIST SP 800-171 ✓ NIST CSF ✓ Section 508 VPATs	✓ FIPS 140-2 ✓ ITAR ✓ CJIS ✓ IRS 1075
Industry	✓ PCI DSS Level 1 ✓ GLBA ✓ FFIEC ✓ Shared Assessments ✓ FISC (Japan)	✓ FCA (UK) ✓ MAS + ABS (Singapore) ✓ 23 NYCRR 500 ✓ HIPAA BAA ✓ HITRUST	✓ 21 CFR Part 11 (GxP) ✓ MARS-E ✓ NHS IG Toolkit (UK) ✓ NEN 7510:2011 (Netherlands) ✓ FERPA	✓ CDSA ✓ MPAA ✓ FACT (UK) ✓ DPP (UK)
Regional	✓ Argentina PDPA ✓ Australia CCSL / IRAP ✓ Canada Privacy Laws ✓ China GB 18030:2005 ✓ China DJCP (MLPS) Level 3	✓ China TRUCS / CCCPPF ✓ EN 301 549 ✓ EU ENISA IAF ✓ EU Model Clauses ✓ EU – US Privacy Shield ✓ Germany IT-Grundschutz workbook	✓ Germany C5 ✓ India MeitY ✓ Japan CS Mark Gold ✓ Japan My Number Act ✓ Netherlands BIR 2012 ✓ New Zealand Gov CIO Fwk	✓ Singapore MTCS Level 3 ✓ Spain ENS ✓ Spain DPA ✓ UK Cyber Essentials Plus ✓ UK G-Cloud ✓ UK PASF

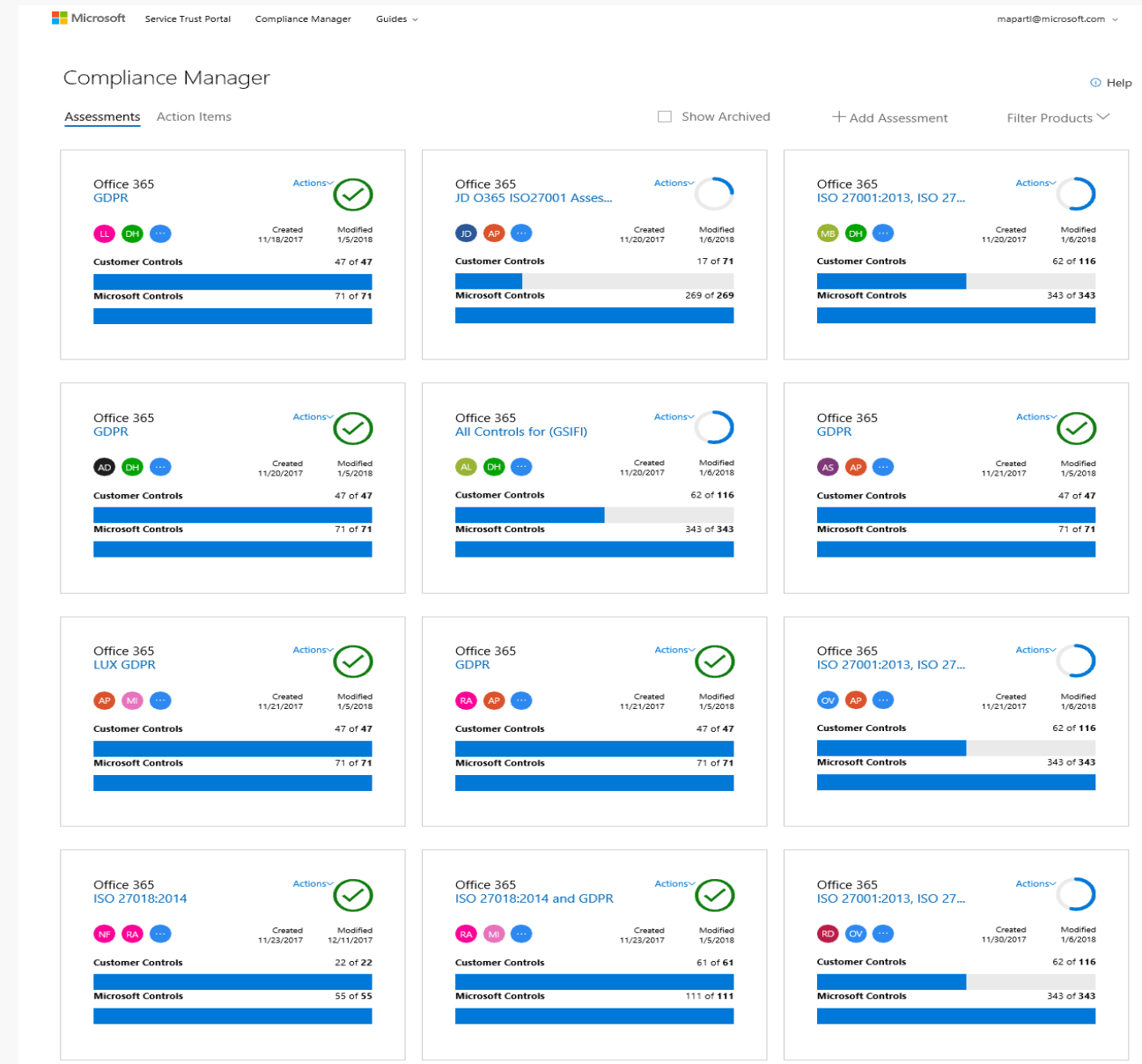


Unsere **INTELLIGENZ** – Digital Crime Unit (DCU)



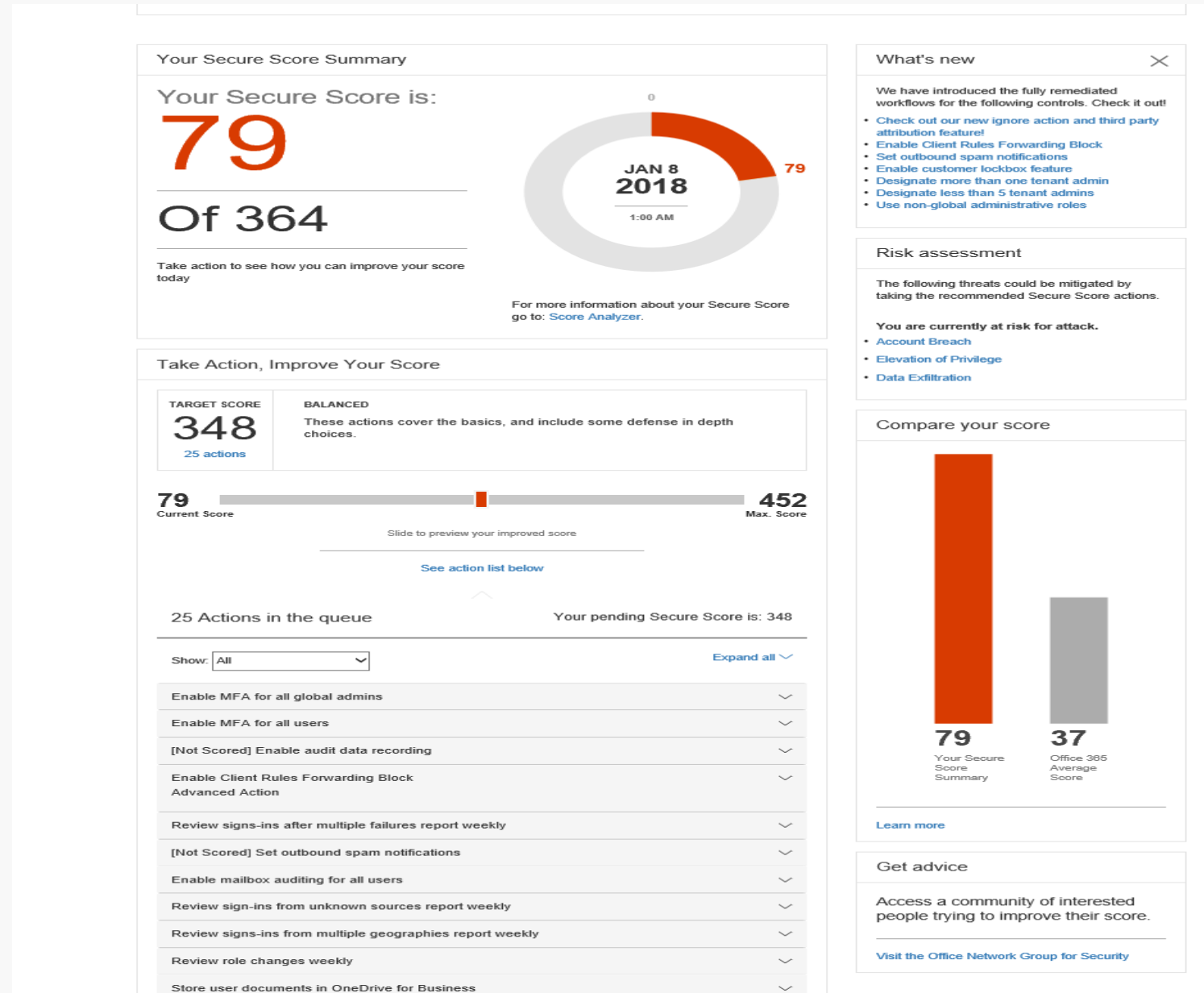
Compliance Manager (zu ISO 27001/27018 und GDPR)

<https://servicetrust.microsoft.com/>



Microsoft Office 365 Secure Score

<https://seurescore.office.com/>



Microsoft bietet einen ganzheitlichen Sicherheitsansatz

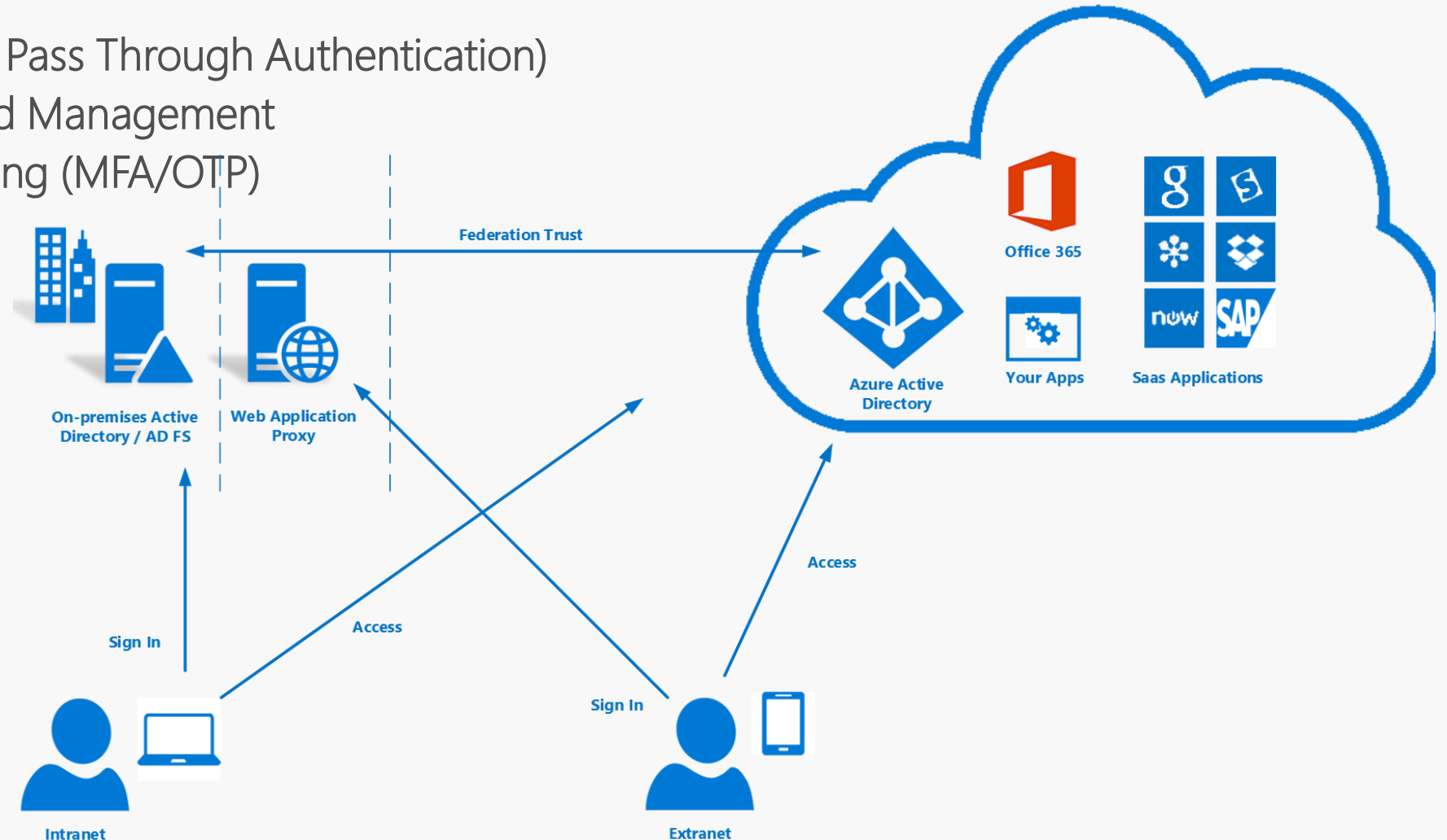
- Enterprise Mobility & Security (EMS) für Modernen Arbeitsplatz/Azure Infrastrukturen
- Azure Security Center für komplexe hybride Azure Data/AI Infrastrukturen



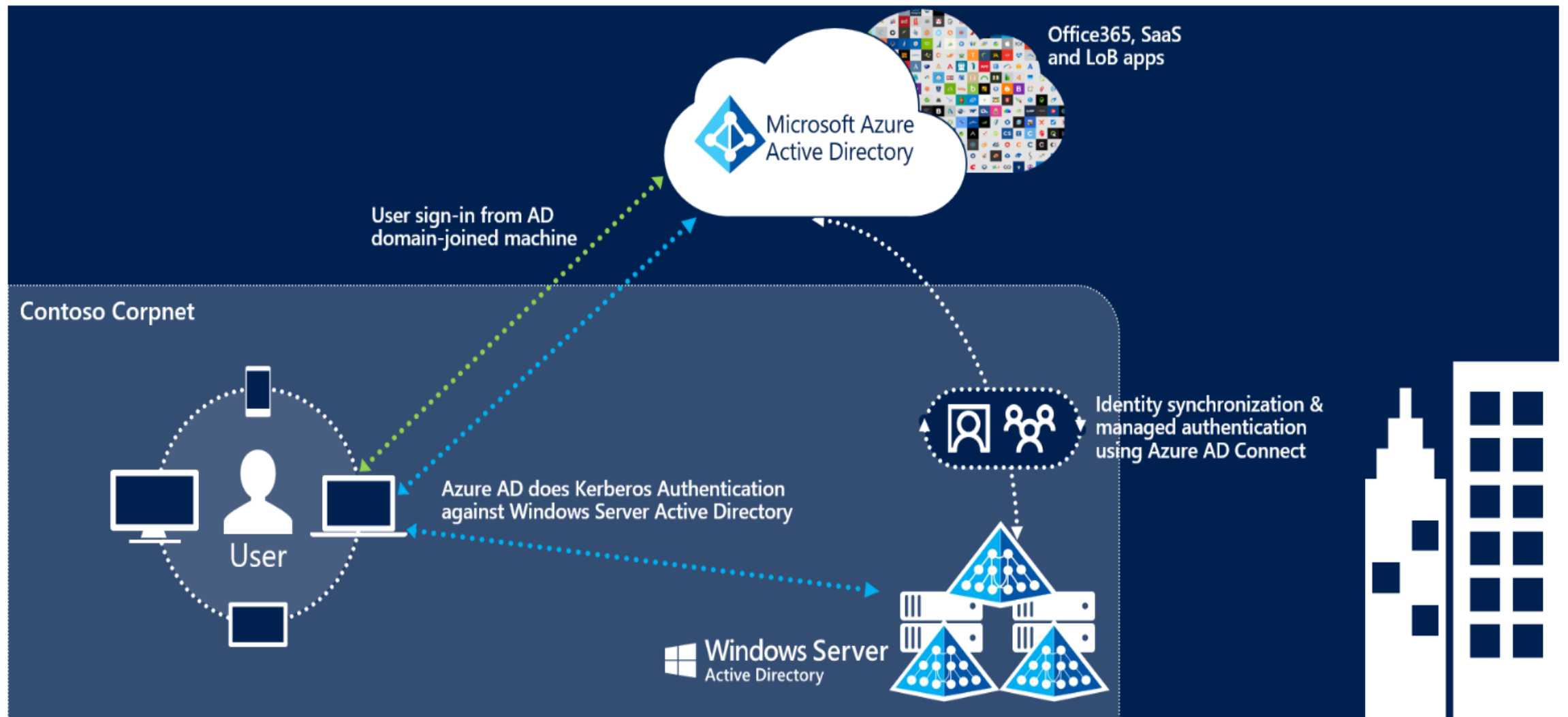
Azure
Identity & Access
Management

Azure Active Directory Premium (AADP)

- ✓ Single Sign On (SSO) für SaaS- und "On-Prem" Applikationen
- ✓ Conditional Access
- ✓ Application Proxy (z.B. für Pass Through Authentication)
- ✓ User Self-Service Password Management
- ✓ Multifaktor Authentifizierung (MFA/OTP)



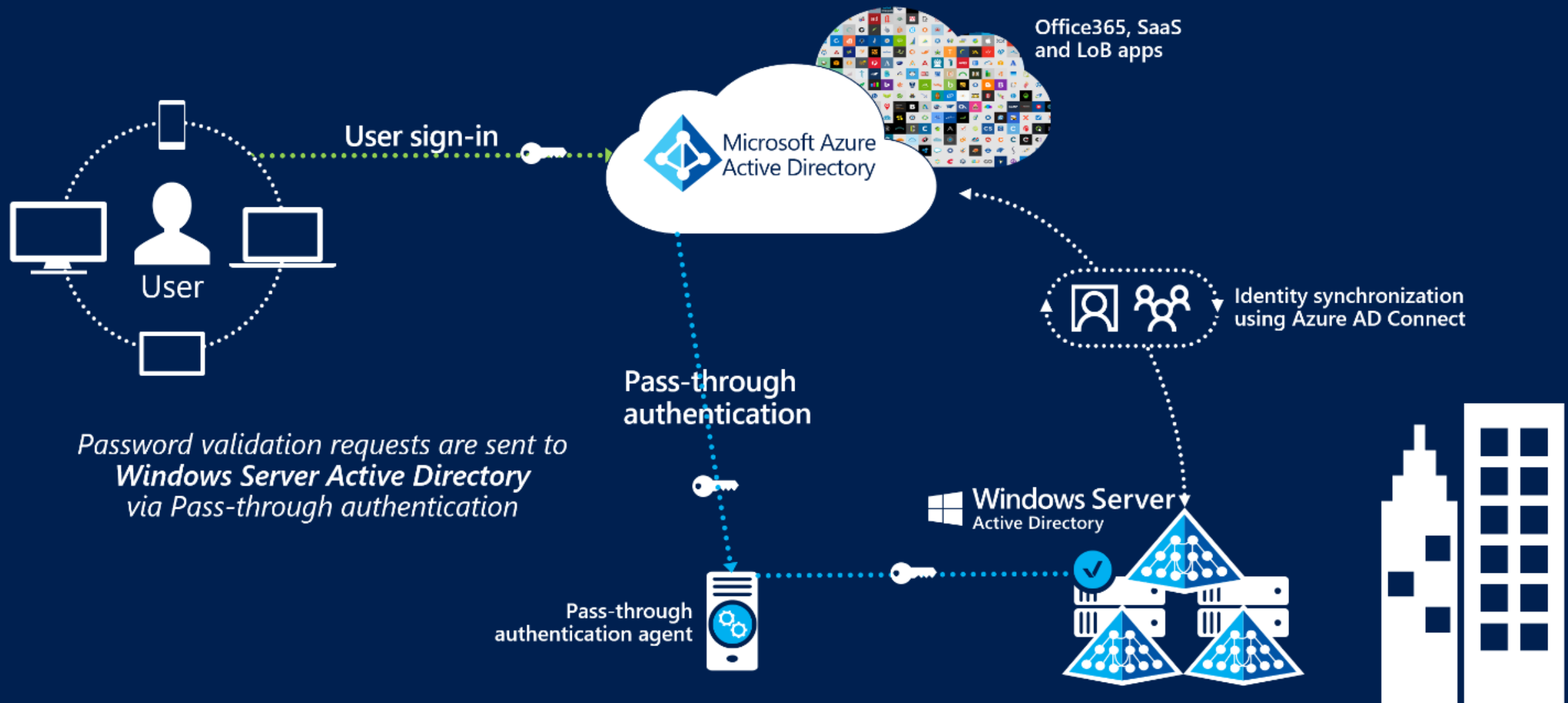
Azure AD Seamless SSO (Azure AD Password Hash Synchronization)



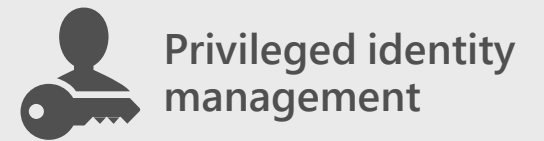
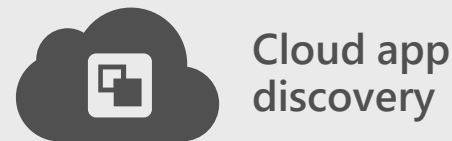
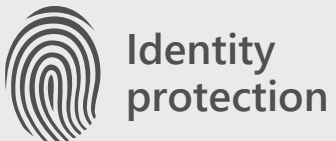
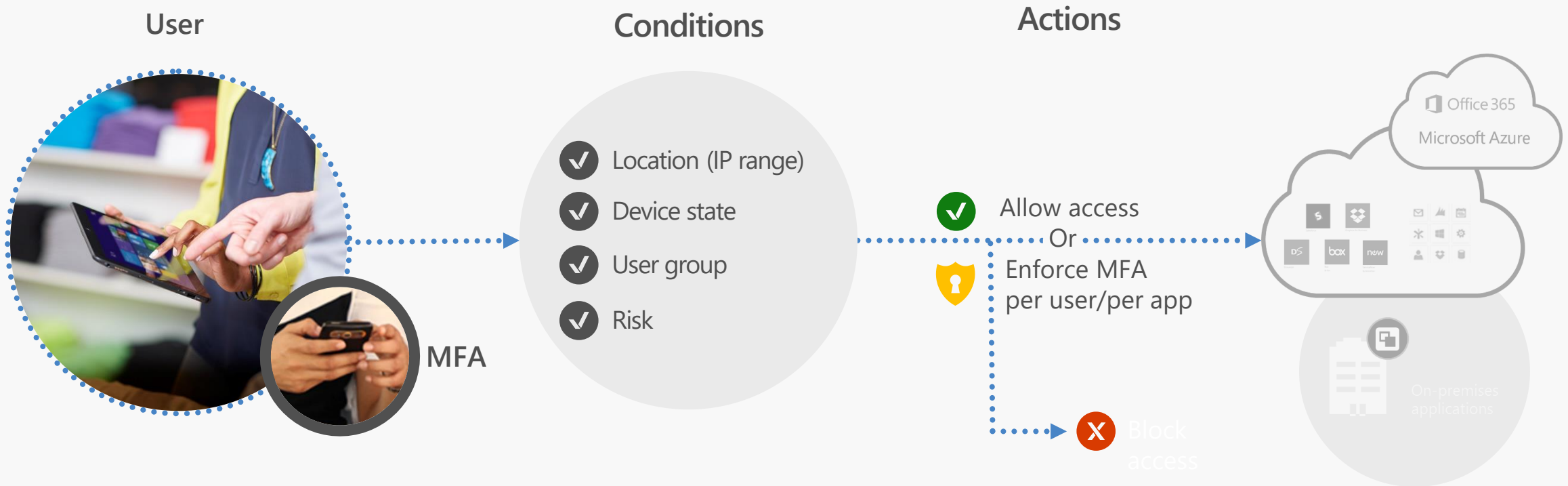
Security & Compliance Richtlinien erlauben die Synchronisation von Benutzer Passwörtern zwischen Microsoft AD (on-prem) und Azure AD nicht immer

Lösungsansatz: Pass-through Authentication (PTA)

Azure Pass Through Authentication (PTA)



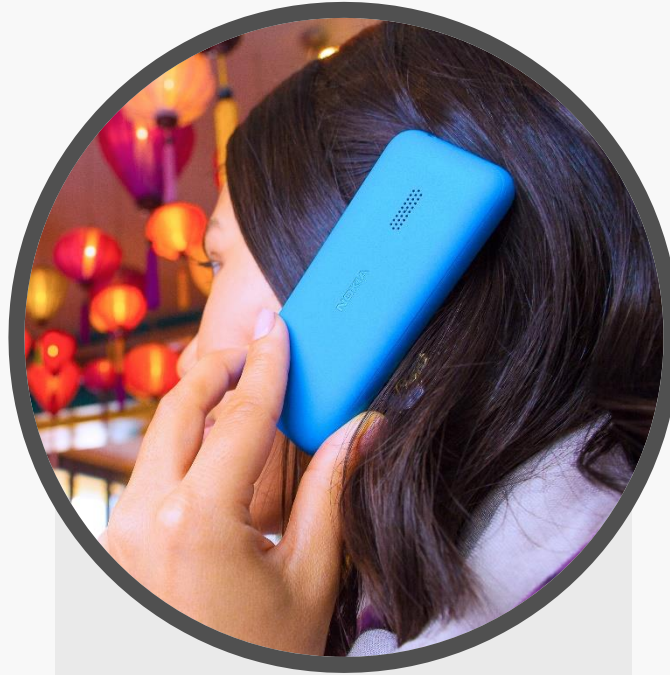
Azure AD Premium - Conditional Access



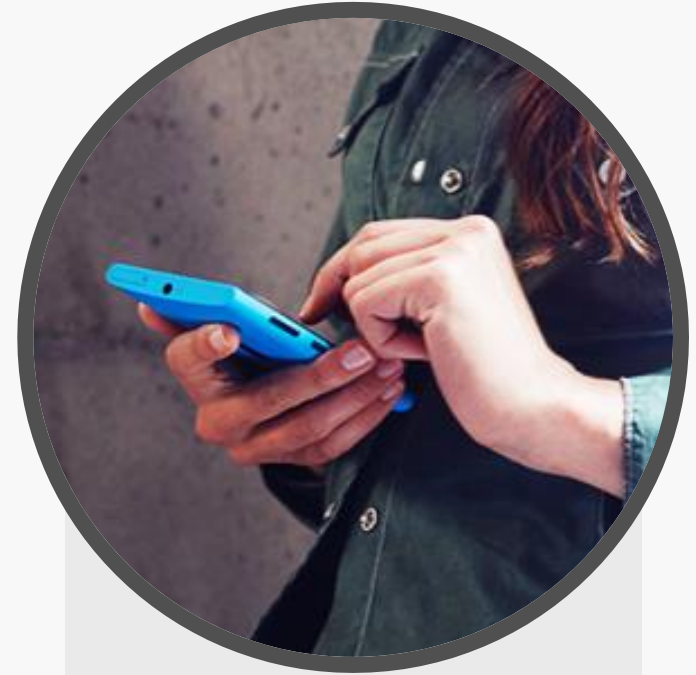
Multifaktor Authentifizierung (MFA)



Mobile
apps



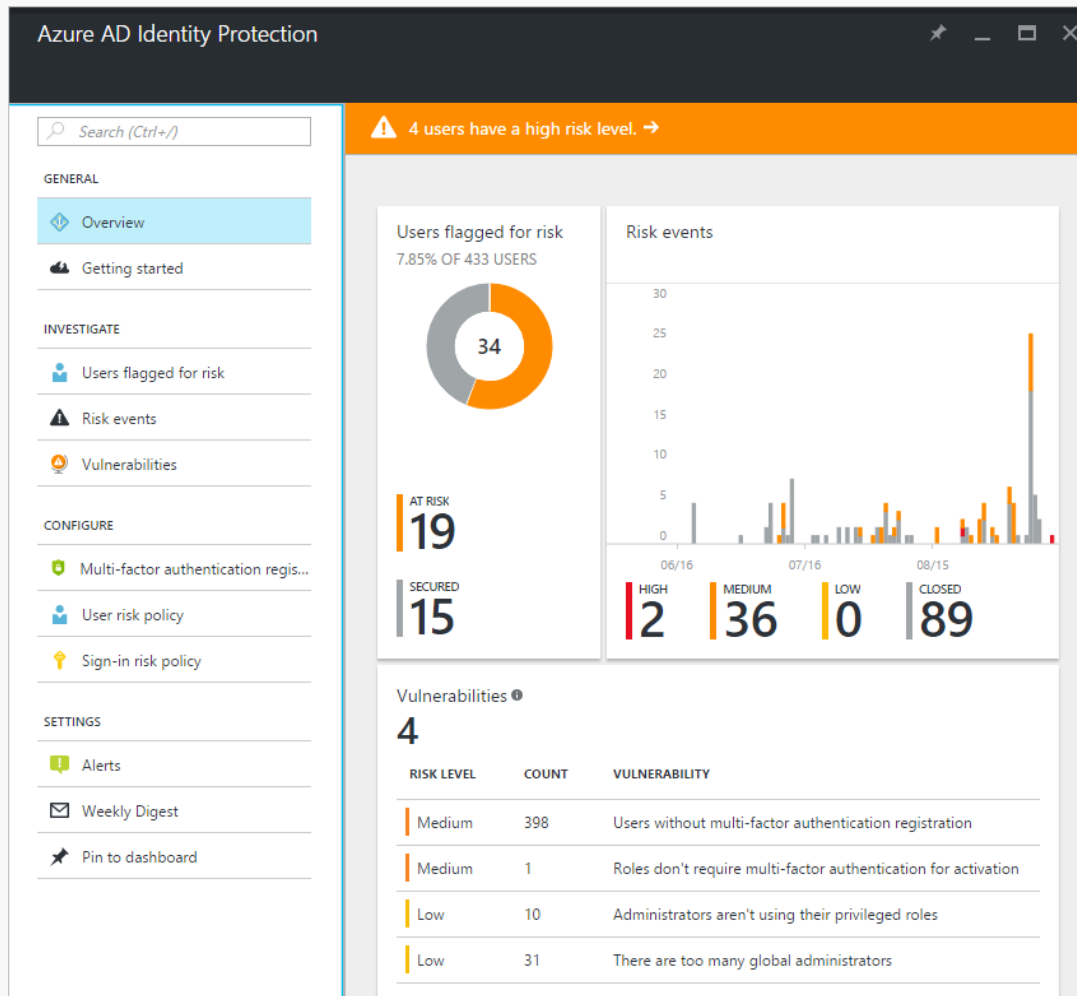
Phone
calls



Text
messages

Azure AD Identity Protection

Azure Active Directory Identity Protection analyses your configuration and detects vulnerabilities that can have an impact on your user's identities.

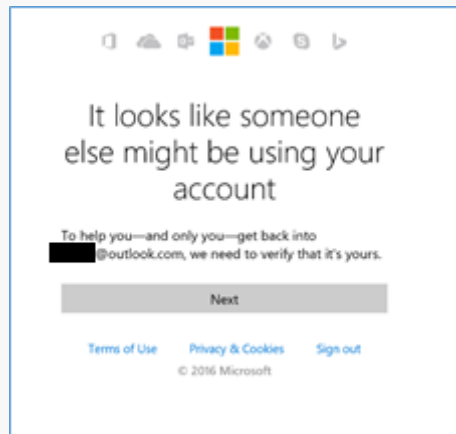


- ✓ Benutzer mit kompromittierten Anmeldeinformationen
- ✓ Anmeldungen von anonymen IP-Adressen
- ✓ Unmöglicher Ortswechsel zu atypischen Orten
- ✓ Anmeldungen von infizierten Geräten
- ✓ Anmeldungen von IP-Adressen mit verdächtigen Aktivitäten
- ✓ Anmeldungen von unbekannten Standorten

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials ⓘ	44 of 45	12/7/2016 1:04 AM
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ	76 of 78	1/17/2017 2:44 PM
Medium	Offline	Impossible travels to atypical locations ⓘ	11 of 14	1/17/2017 2:44 PM
Medium	Real-time	Sign-in from unfamiliar location ⓘ	0 of 1	11/15/2016 7:18 PM
Low	Offline	Sign-ins from infected devices ⓘ	76 of 78	1/17/2017 2:44 PM

Azure AD Identity Protection - Beispiel

“when we detect a user’s password is compromised, Azure AD admins can have the account automatically locked down and protected before the bad guy can ever use the credentials”



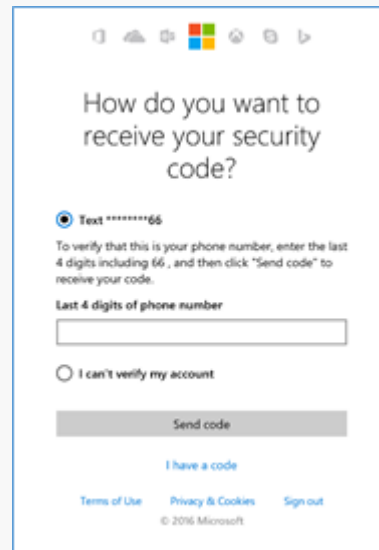
It looks like someone else might be using your account

To help you—and only you—get back into [redacted]@outlook.com, we need to verify that it's yours.

Next

[Terms of Use](#) [Privacy & Cookies](#) [Sign out](#)

© 2016 Microsoft



How do you want to receive your security code?

☒ Text *****66

To verify that this is your phone number, enter the last 4 digits including 66, and then click "Send code" to receive your code.

Last 4 digits of phone number

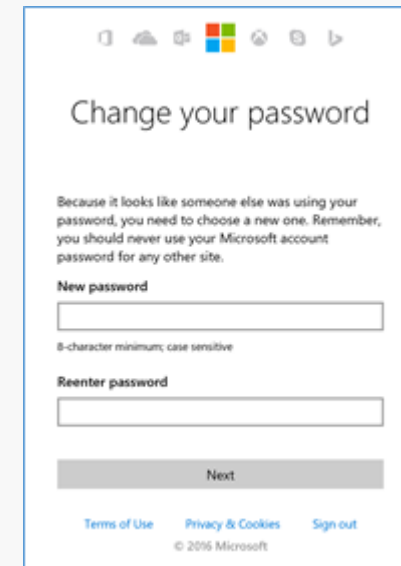
☐ I can't verify my account

Send code

[I have a code](#)

[Terms of Use](#) [Privacy & Cookies](#) [Sign out](#)

© 2016 Microsoft



Change your password

Because it looks like someone else was using your password, you need to choose a new one. Remember, you should never use your Microsoft account password for any other site.

New password

8-character minimum; case sensitive

Reenter password

Next

[Terms of Use](#) [Privacy & Cookies](#) [Sign out](#)

© 2016 Microsoft



Azure Data Protection

Die Evolution von Azure Information Protection



Classification
& labeling

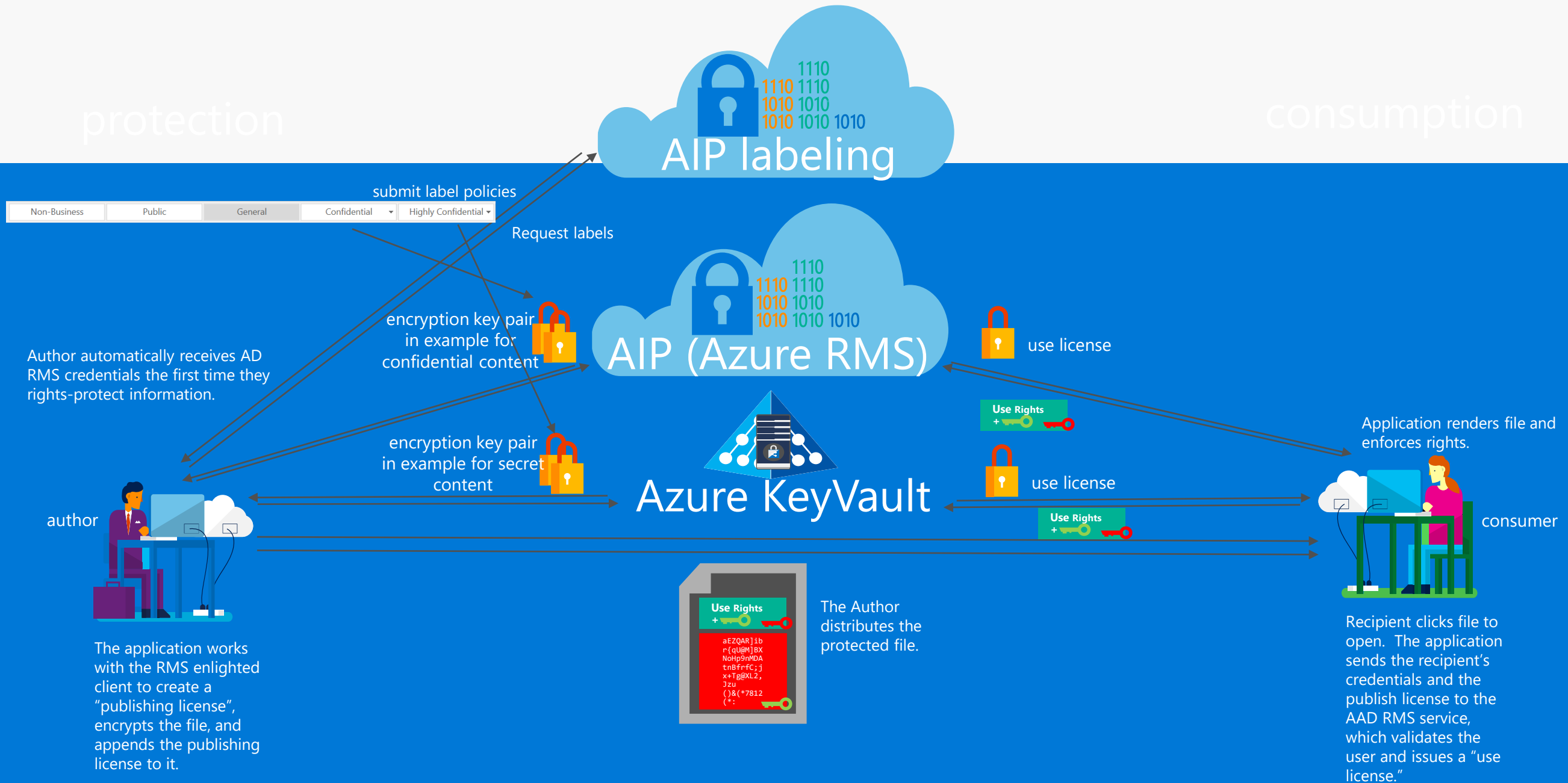
Protect

Monitor &
respond

Wie funktioniert Azure Information Protection?

protection

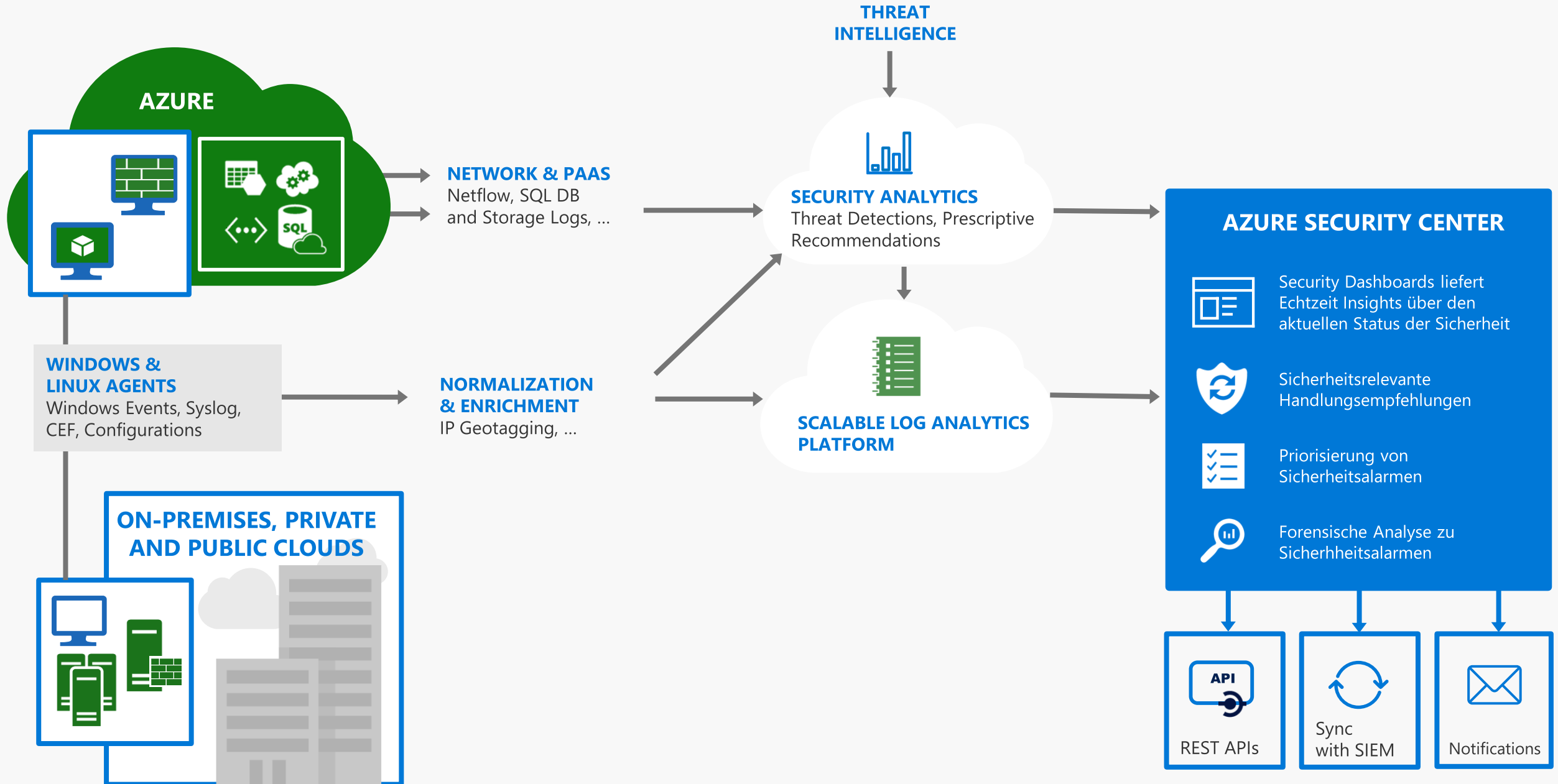
consumption





Azure
Security
Management

Azure Security Center Architektur



Azure Security Center – Security Management



DETECT

- ✓ Nicht gepatchte VM's
- ✓ Schwachstellen (CVE)
- ✓ Fehlende FW Regeln (NSG)
- ✓ Bruteforce Angriffe
- ✓ Kompromittierte VM's



PROTECT

- ✓ Zugriffsregeln
- ✓ Datenschutz durch Verschlüsselung von SQL Datenbanken und Storage Umgebungen
- ✓ NSG FW Regeln
- ✓ Endpoint Schutz



RESPOND

- ✓ Fehlende Sicherheitsrichtlinien
- ✓ Gegenmaßnahmen bei Sicherheitsvorfall

1. Schritt

Defintion ein Sicherheitsrichtlinie

Security policy
ASC DEMO

Save Discard

Data collection
Collect data from virtual

On Off

Data Collection is

Choose a storage acco
All configured

Policy components

 Prevention

 Email no

 Pricing t

Prevention policy
ASC DEMO

Show recommendations for

System updates ⓘ	On Off
OS vulnerabilities ⓘ	On Off
Endpoint protection ⓘ	On Off
Disk encryption	On Off
Network security groups	On Off
Web application firewall	On Off
Next generation firewall	On Off
Vulnerability Assessment	On Off
Storage Encryption	On Off
JIT Network Access	On Off
SQL auditing & Threat detection	On Off
SQL Encryption	On Off

Erkennung von Risiken

Anpassung der Unternehmensrichtlinie durch Sicherheitsempfehlung

Recommendations

Filter

DESCRIPTION	RESOURCE	STATE	SEVERITY
Enable VM Agent	VM-L3	Open	High
Install Endpoint Protection	VM-W5	Open	High
Add a web application firewall	VM-W5	Open	High
Add a Next Generation Firewall	3 endpoints	Open	High
Finalize web application firewall setup	VM-W6	Open	High
Enable Network Security Groups on sub...	2 subnets	Open	High
Enable Network Security Groups on virt...	VM-CL-W1	Open	High
Enable Auditing on SQL servers	sqlserver1a	Open	High
Enable Auditing on SQL databases	SQL-Db1	Open	High
Enable Transparent Data Encryption	SQL-Db1	Open	High
Apply system updates	VM-CL-W1	Open	High
Apply disk encryption	5 virtual mac...	Open	High
Update OS version	WorkerRole1	Open	High
Restrict access through Internet facing...	2 virtual mac...	Open	Medium
Provide security contact details	2 subscriptio...	Open	Medium
Resolve mismatch baseline rules	3 virtual mac...	Open	Low

Transparent data encryption

Save Discard Feedback



Transparent Data Encryption protects your data and helps meet compliance requirements by encrypting your database, associated backups, and transaction log files at rest without requiring changes to your application.

[Learn more about transparent data encryption.](#)

Data encryption

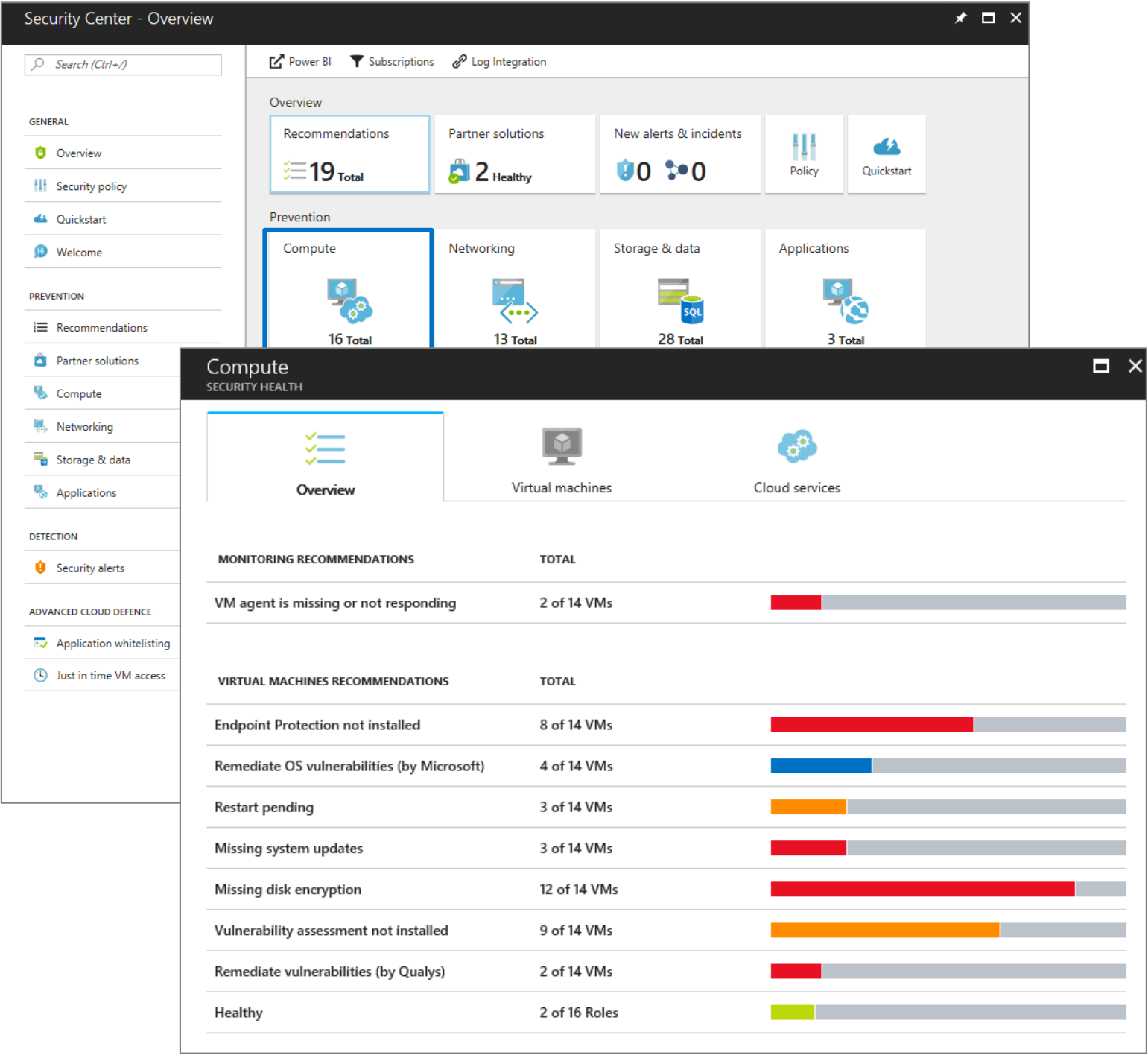
ON OFF

Encryption status

Unencrypted

Prävention

Überwachung der Unternehmensrichtlinie durch Microsoft Intelligence



Prävention – Integration von Partner Lösungen



- Handlungsempfehlungen zur Provisionierung von Partnerlösungen
- Integriertes zentrales Alerting (Security Incident & Event Management)
- Aktiviert Monitoring & Management der Partnerlösung
- Verfügbar über Azure Marketplace



Einfaches Deployment von Partnerlösungen und automatische Integration von Log Informationen

The screenshot illustrates the steps to add a Web Application Firewall (WAF) solution to an Azure environment. It shows the 'Recommendations' pane, the 'Add a Web Application Firewall' dialog, the 'Create a new Web Application Firewall' selection screen, and the 'F5 WAF Solution' configuration page.

Recommendations

DESCRIPTION	RESOURCE	STATE	SEVERITY
Enable VM Agent	VM-L3	Open	High
Install Endpoint Protection	VM-W5	Open	High
Add a web application firewall	VM-W5	Open	High
Add a Next Generation Firewall	3 endpoints	Open	High

Add a Web Application Firewall

Select an existing solution or create a new one -

Create New

- Or -

Use existing solution

Create a new Web Application Firewall

- Barracuda Networks, Inc.
2 Packages
- F5 Networks
F5 WAF Solution**
- Imperva Inc.
SecureSphere WAF Deployment Kit

F5 WAF Solution
F5 Networks

Bring Your Own License enabled.

Enable compliance and better protect your applications with the F5 web application firewall solution, which delivers:

- Protection from common application vulnerabilities
- Defense against OWASP Top 10 threats and layer 7 DDoS attacks
- Compliance with PCI-DSS requirements
- High application performance without compromises

Designed to run as a pre-configured service within the Azure Security Center

The F5 web application firewall solution (in preview) is built using the industry-proven F5 [BIG-IP Application Security Manager \(ASM\)](#) and [BIG-IP Local Traffic Manager \(LTM\)](#) technologies. By activating this solution within the Azure Security Center, you can realize the benefits of BIG-IP products, as well as customize the configuration to satisfy the unique needs of your application or organizational policies.

The **F5 web application firewall** solution leverages industry-proven and ICSA-certified BIG-IP Application Security Manager (ASM) and BIG-IP Local Traffic Manager (LTM) technologies as a pre-configured virtual solution within Azure Security Center.

This preview is currently offered at no charge using a BIG-IP Evaluation license and must be launched through the Azure Security Center.

For more information, visit f5.com.

PUBLISHER F5 Networks

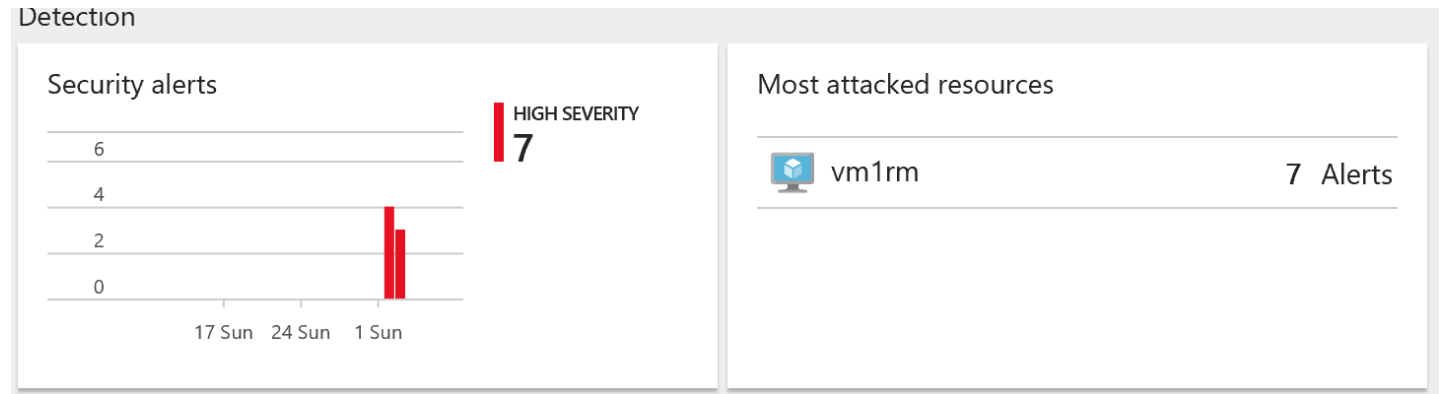
Select a deployment model

Resource Manager

Create

Angriffserkennung & Gegenmaßnahmen

24x7 Databreach Reporting durch Email Notifications



Mo 02.10.2017 17:50

Microsoft Azure Security Center <alerts-noreply@azuresecuritycenter.microsoft.com>

New Suspicious command execution alert on subscription 31f96730-662b-41d1-9b1a-fea6f99aa483

n Matt Partl

Diese Nachricht wurde mit der Priorität "Hoch" gesendet.

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Klicken Sie hier, um die...

Klicken Sie hier, um die...

Dear Azure customer,

[Azure Security Center](#) has discovered a potential security threat on your environment:



Suspicious command execution

Machine logs indicate a suspicious command line execution by user vm1rm\$.

10/02/2017 15:50:01 (UTC)



VM1RM
Attacked Resource



Microsoft
Detected by



High
Severity



Thank you,
Microsoft Azure Security Team

Azure Security Center – Alerting

 Microsoft
Cyber Defense Operations Center
C+E Security - Security Incident Management

Action Required: Security Alert Generated

This message is to notify you that the Cyber Defense Operations Center received a security alert that was generated from a system or server that your property is responsible for. This alert may indicate that this server was compromised.

Please take the appropriate next step to resolve this notice:

- Reply to this email indicating that this was known and/or good activity.
- If there is an indication of unauthorized access and/or a security issue, please email the CDOC (cdoc@microsoft.com) and request that the Security Incident Management on-call engineer be engaged via a two way escalation.

System information

Ticket: 196129
Server Name: VM1RM
Event Text Details:

Attribute Name	Attribute Value
ActionTaken	Detected

Weiterführende Informationen

GDPR – Allgemein:

<http://www.microsoft.com/gdpr>

<http://aka.ms/it-sicherheit>

<http://www.microsoft.com/de-de/trustcenter/privacy/GDPR>

Azure Security

<http://docs.microsoft.com/en-us/azure/security/azure-security>

Q&A

matthias.partl@microsoft.com