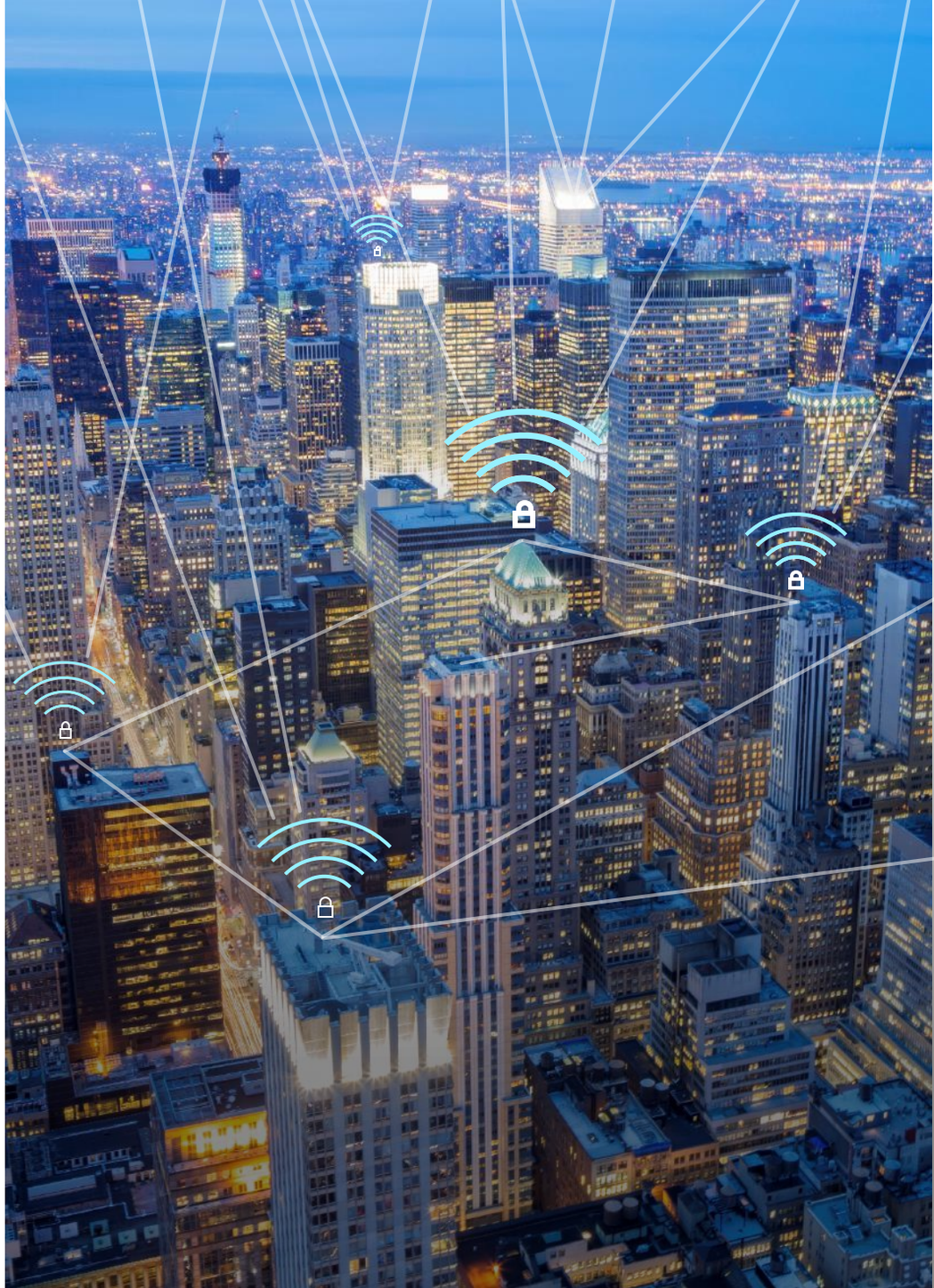
Microsoft

Microsoft Security

Vereinfachung und Verstärkung der Sicherheit mit Sicherheitslösungen von Microsoft



Alternde Technologie birgt Risiken

- Ausgefeilte Bedrohungen
- Alternde Technologie schafft Barrieren
- Wartung erschwert Innovation

TECH INSIDER

BUSINESS INSIDER AUSTRALIA

Die 21 schwersten Datenschutzverletzungen 2018

PAIGE LESKIN
12. DEZ. 2018, 12:00 Uhr

MARRIOTT

500 Millionen Kunden waren vom Marriott-Hack betroffen

CATHAY PACIFIC

9,4 Mio. Kunden, 860K Passnummern, 245K Personalausweise

TICKETFLY

Die personenbezogenen Daten von 27 Mio. Kunden wurden gestohlen

SingHealth

Auf die personenbezogenen Daten von 1,5 Mio. Patienten wurde zugegriffen

Quelle: https://www.businessinsider.com.au/data-hacks-breaches-biggest-of-2018-2018-12

Ein hohes Sicherheitsniveau ist unerlässlich

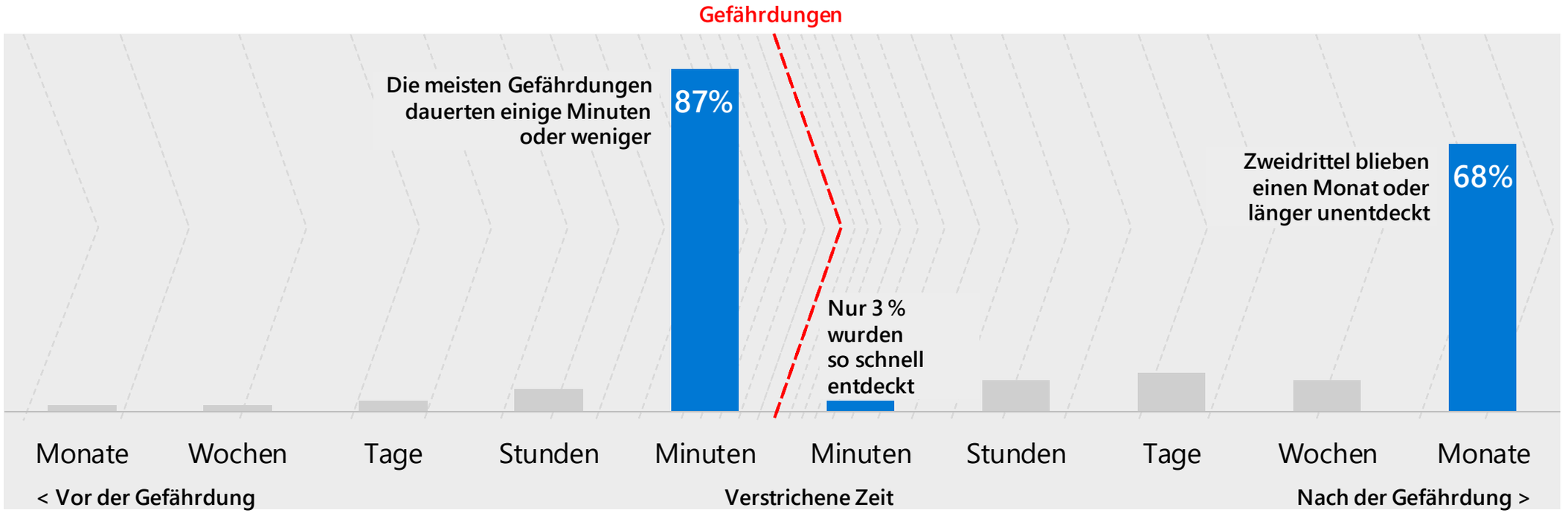
Ein Sicherheitsbruch kann innerhalb kürzester Zeit das Vertrauen der Kunden für immer erschüttern

4,2 Mrd.
Datensätze wurden 2016 von Hackern gestohlen

20 %
aller Unternehmen **verlieren Kunden** durch einen Hackerangriff

30 %
aller Unternehmen **verlieren Umsätze** durch einen Hackerangriff

28 %
aller Hackerangriffe **erfolgen intern** – und sind schwerer aufzudecken



Verizon Data Breach Investigations Report 2018

Quellen: Risk Based Security Report, 2017; Cisco 2017 Annual Cybersecurity Report; Juniper Research Cybercrime & The Internet of Threats, 2017; Verizon Data Breach Investigations Report 2018

Microsoft Integrated Security

Vereinfachte und verstärkte Sicherheit mit Sicherheitslösungen von Microsoft

Identitäts- und Zugriffs-management

Schützen Sie die Identität Ihrer Anwender und kontrollieren Sie den Zugriff auf wertvolle Ressourcen anhand der Risikostufe des Anwenders

Bedrohungs-schutz

Schutz vor ausgefeilten Bedrohungen und schnelle Wiederherstellung nach einem Angriff

Informations-schutz

Stellen Sie sicher, dass Ihre Dokumente und E-Mails nur von befugten Personen gelesen werden können

Sicherheits-management

Gewinnen Sie Transparenz und die Kontrolle über Ihre Sicherheitswerkzeuge

Microsoft Integrated Security

Vereinfachte und verstärkte Sicherheit mit Sicherheitslösungen von Microsoft

Identitäts- und Zugriffs-management

Schützen Sie die Identität Ihrer Anwender und kontrollieren Sie den Zugriff auf wertvolle Ressourcen anhand der Risikostufe des Anwenders

Bedrohungs-schutz

Schutz vor ausgefeilten Bedrohungen und schnelle Wiederherstellung nach einem Angriff

Informations-schutz

Stellen Sie sicher, dass Ihre Dokumente und E-Mails nur von befugten Personen gelesen werden können

Sicherheits-management

Gewinnen Sie Transparenz und die Kontrolle über Ihre Sicherheitswerkzeuge

Kostenreduzierung mit einer integrierten Lösung

Effektive Sicherung hybrider Umgebungen

Einsatz der größten und vertrauenswürdigsten Sicherheitspräsenz der Welt

Identitäts- und Zugriffsmanagement

Prüfen Sie, ob ein Anwender befugt und sicher ist, bevor der Zugriff auf Apps und Daten freigegeben wird

Schutz direkt an der Haustür

Vereinfachen Sie den Zugriff auf Geräte und Apps

Sichern Sie Ihre Zugangsdaten

Bedrohungsschutz

Schutz vor ausgefeilten Angriffen, erkennen und reagieren Sie schnell auf einen Verstoß

Schützen Sie
Ihr Unternehmen vor ausgefeilten Cyber-Angriffen

Erkennen Sie
illegale Aktivitäten

Reagieren Sie
schnell auf Bedrohungen

Informationsschutz

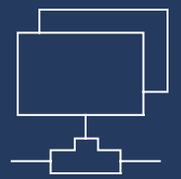
Schutz sensibler Daten im gesamten Lebenszyklus – intern und extern

Ermittlung

Klassifizierung

Schutz

Überwachung



GERÄTE

CLOUD

ON-PREMISES

Intelligentes Sicherheitsmanagement

Umfassende Sicherheitsintegration mit Microsoft Intelligent Security Graph

Microsoft Integrated Security

Einsatz branchenführender Technologien für 360°-Schutz

Identitäts- und Zugriffs-management

Azure Active Directory

Conditional Access

Windows Hello

Windows Credential Guard

Bedrohungs-schutz

Advanced Threat Analytics

Windows Defender Advanced Threat Protection

Office 365 Advanced Threat Protection

Office 365 Threat Intelligence

Informations schutz

Azure Information Protection

Office 365 Data Loss Prevention

Windows Information Protection

Microsoft Cloud App Security

Office 365 Advanced Security Mgmt.

Microsoft Intune

Sicherheits-management

Azure Security Center

Office 365 Security Center

Windows Defender Security Center

Munich RE

„Azure ermöglicht uns, die Risiken der Veränderung infolge des Klimawandels in bisher nie dagewesener Form zu analysieren."

– Robin Johnson: CIO – Munich Re

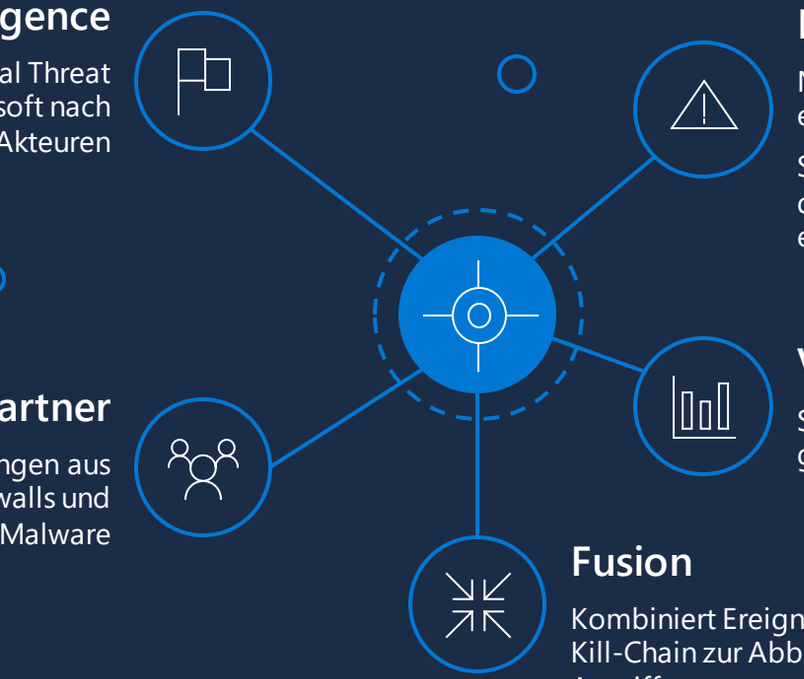
Nächste Schritte

Weitere Informationen über Sicherheitslösungen von Microsoft erhalten Sie von Ihrem Microsoft-Partner.

Sicherheitspraktiken

Bei Microsoft hat Sicherheit in jedem Schritt Priorität, von der Code-Entwicklung bis zur Incident Response

Integrierte Informationen und erweiterte Analysen



Threat Intelligence

Sucht mit der Global Threat Intelligence von Microsoft nach bekannten böswilligen Akteuren

Partner

Integriert Warnungen aus Partnerlösungen wie Firewalls und Anti-Malware

Erkennen von Anomalien

Nutzt statistisches Profiling zum Aufbau einer historischen Ausgangsbasis

Sendet Warnungen bei Abweichungen, die einem potenziellen Angreifer entsprechen

Verhaltensanalyse

Sucht nach bekannten Mustern und gefährlichen Verhaltensweisen

Fusion

Kombiniert Ereignisse und Warnungen aus der Kill-Chain zur Abbildung der Zeitachse des Angriffs

Auf der Basis von Microsoft Intelligent Security Graph

Erkennt Bedrohungen in der Kill-Chain

Ziel und Angriff

Eingehende Brute-Force-, RDP-, SSH-, SQL-Angriffe und mehr

Applikation und DDoS-Angriffe (WAF-Partner)

Eindringungserkennung (NG-Firewall-Partner)

Installation und Nutzung

In-Memory Malware und Ausnutzungsversuche

Verdächtige Prozessausführung

Laterale Verschiebung

Interne Aufklärung

Nach einem Angriff

Kommunikation mit einer bekannten illegalen IP (Datenexfiltration oder Command and Control)

Verwendung kompromittierter Ressourcen zur Durchführung weiterer Angriffe (Scannen der Ausgangsports, Brute-Force-, RDP-/SSH-Angriffe, DDoS und Spam)

Konzentration auf die kritischsten Bedrohungen

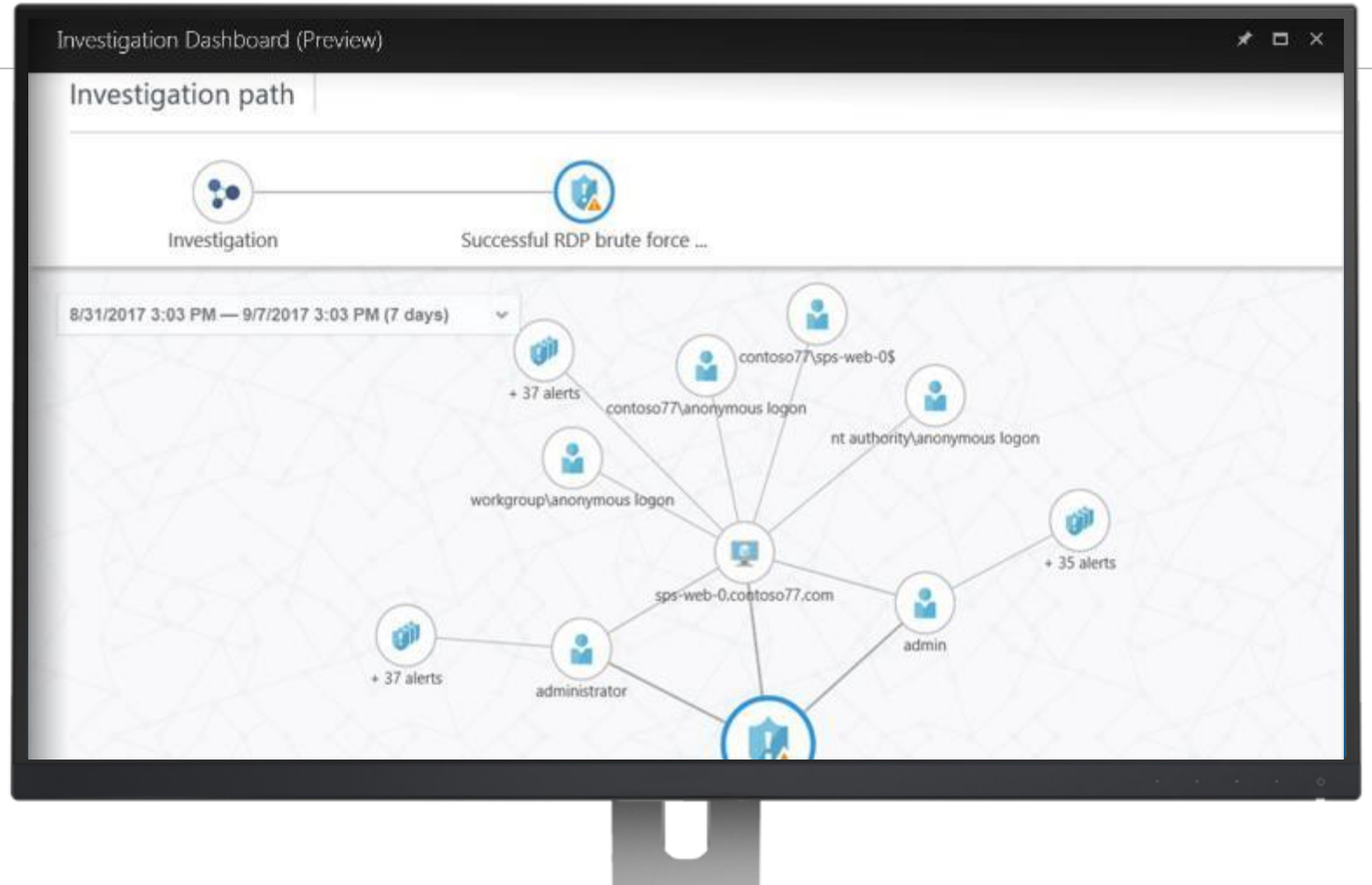
- **Erhalten Sie priorisierte Sicherheitswarnungen**
  - Einzelheiten zu erkannten Bedrohungen und Empfehlungen
- **Erkennen Sie Bedrohungen in der Kill-Chain**
  - Kill-Chain-Mustern entsprechende Warnungen werden in einem Incident zusammengefasst

Gewinnen Sie wertvolle Erkenntnisse über Angreifer

- **Visualisierung der Angriffsquelle in einer interaktiven Karte**
  - Analysiert die Daten aus den Protokollen Ihrer Computer und Firewalls
- **Gewinnen Sie Erkenntnisse aus Bedrohungsberichten**
  - Die bekannten Ziele, Taktiken und Techniken der Angreifer

Vereinfachen Sie den Sicherheits-betrieb und die Untersuchungen

- **Schneller Zugriff auf den Umfang und die Auswirkungen des Angriffs**
  - Interaktives Erlebnis mit Verknüpfungen zu Warnungen, Computern und Anwendern
  - Verwenden Sie vordefinierte oder ad-hoc-Abfragen für tiefergehende Untersuchungen



Reagieren Sie schnell auf Bedrohungen

Automatisieren und organisieren Sie Routine-Workflows für die Sicherheit

- Entwickeln Sie Playbooks mit der Intergration von Azure Logic Apps
- Lösen Sie Workflows aus allen Warnungen aus, um bedingte Maßnahmen zu ermöglichen

Routine-Workflows

- Leiten Sie die Warnungen an ein Ticketingsystem weiter
- Erfassen Sie zusätzliche Informationen
- Wenden Sie zusätzliche Sicherheitskontrollen an
- Bitten Sie einen Anwender, eine Aktion zu validieren
- Sperren Sie verdächtige Benutzerkonten
- Beschränken Sie den Datenverkehr von einer IP-Adresse