Microsoft

Cyberkriminalität auf dem nächsten Level: Wie Sie Ihren Arbeitsplatz vor KI-Angriffen schützen

Stratos Komotoglou, Microsoft 365 Business Group,
Microsoft Deutschland GmbH

stratosk@microsoft.com

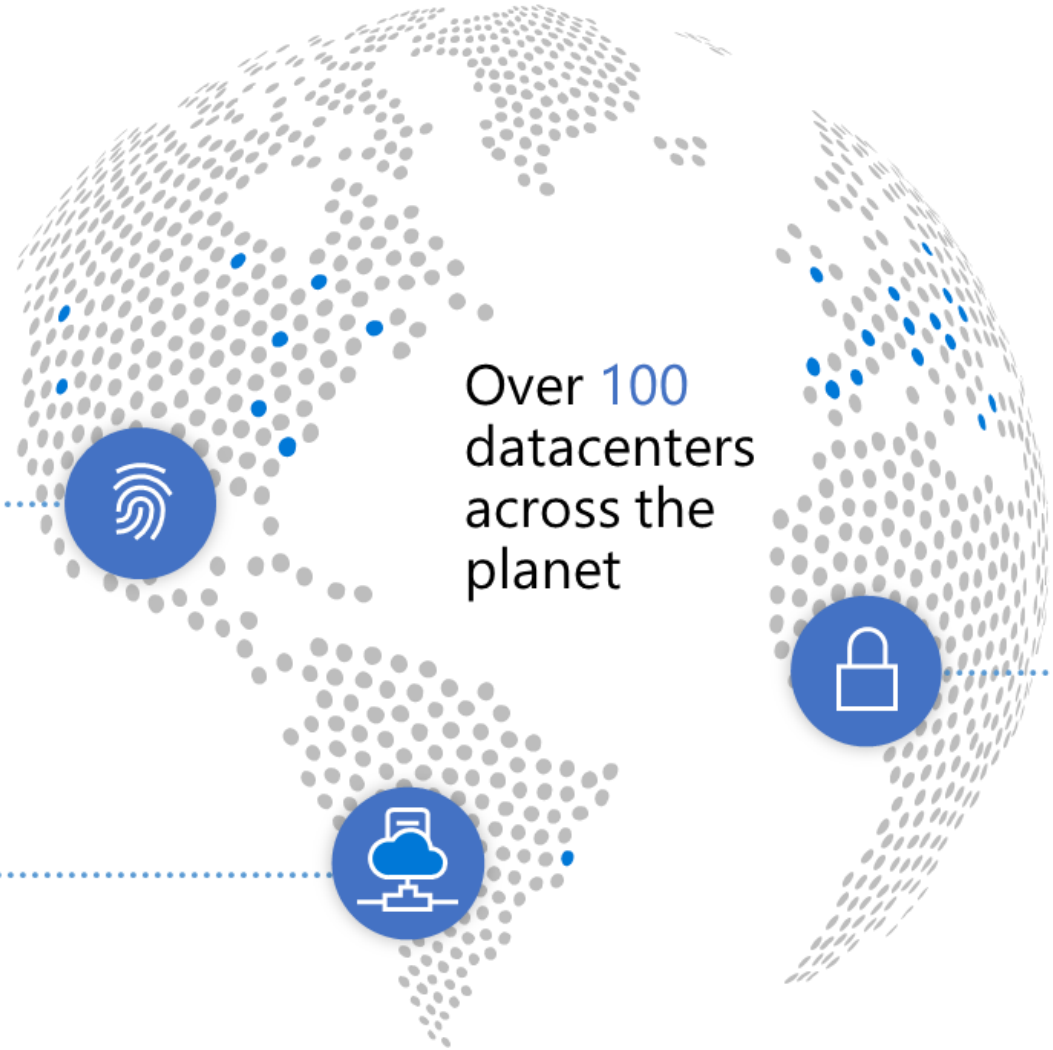
In Vertretung: **Ralf Wigand**, National IT Compliance Officer

ralf.wigand@microsoft.com

Drei Hauptgefahren – Trends aus dem Jahr 2018

- Ransomware vs. crypto-currency mining
- Phishing attacks
- Supply chain compromises

Insights auf globalem Niveau– 6.5 Billionen Signale pro Tag



Each physical datacenter protected with world-class, multi-layered protection

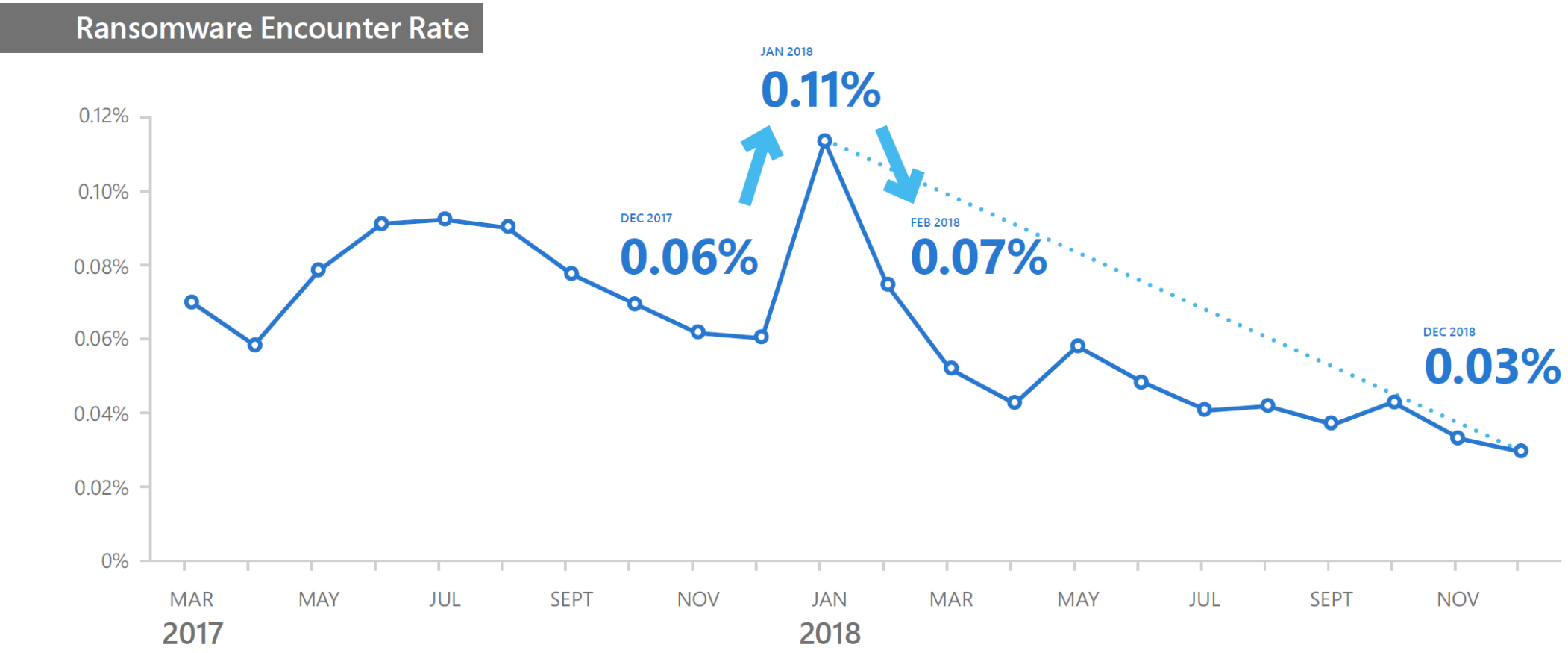
Over 100 datacenters across the planet

Secured with cutting-edge operational security

- Restricted access
- 24x7 monitoring
- Global security experts

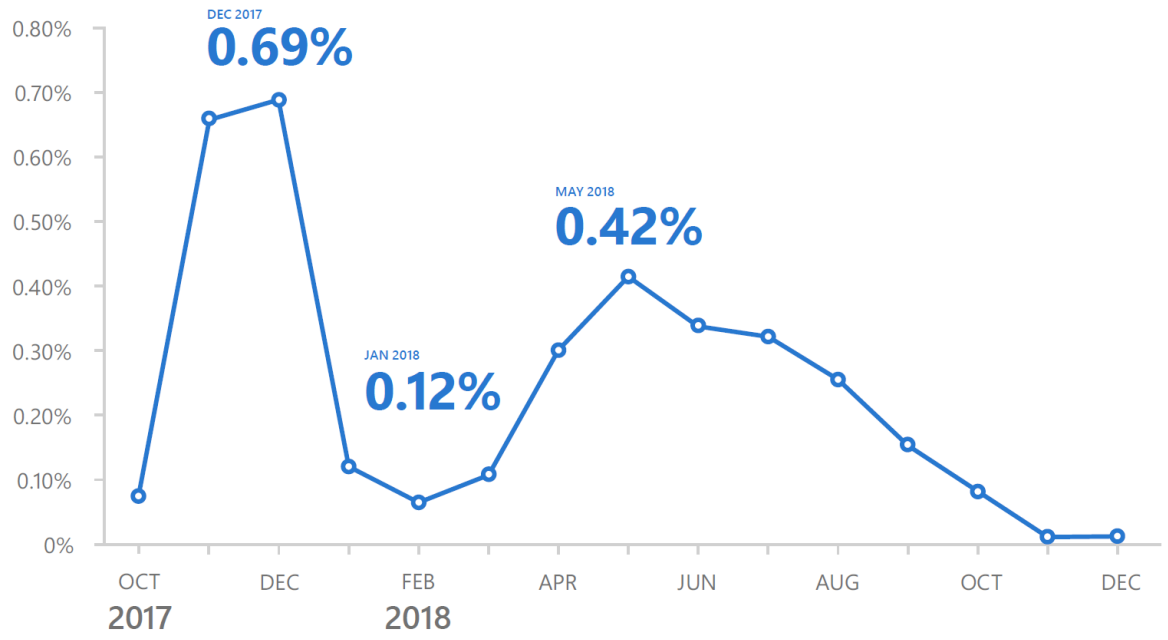
Global cloud infrastructure with custom hardware and network protection

Ransomware Trefferraten gingen zwischen März 2017 und Dezember 2018 **um rund 60% zurück**



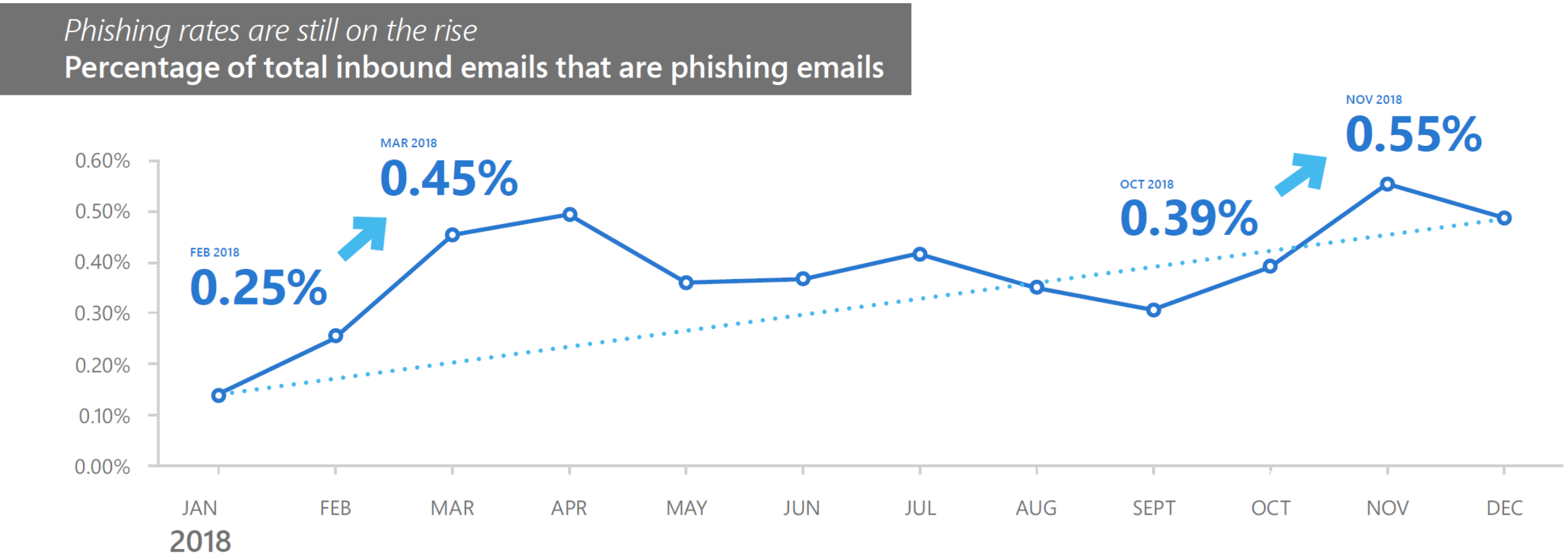
Der Abbau von Bitcoins ist weiterhin lukrativ
Trefferquoten verschieben sich mit Kryptowährungskursen

Brocoiner Encounter Rate

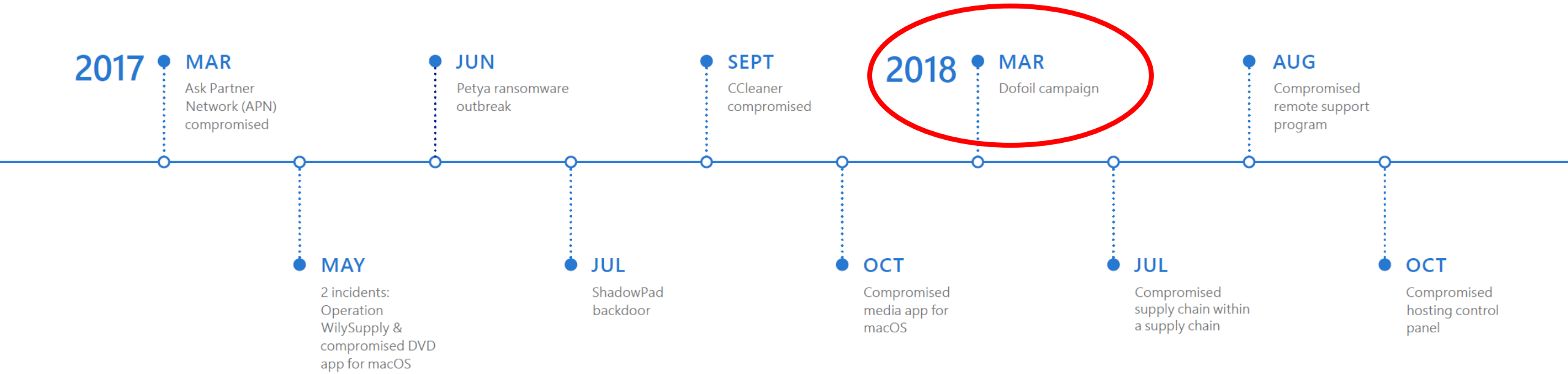


Bitcoin prices

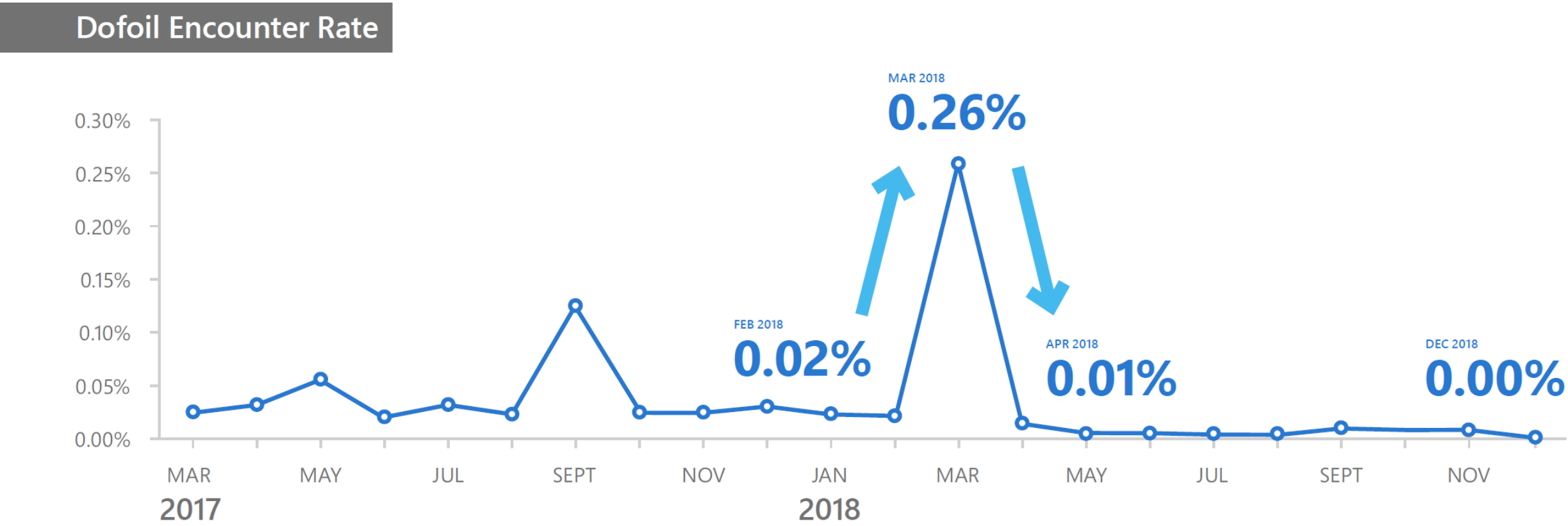
Eingehende E-Mails, bei denen es sich um Phishing-Nachrichten handelte, stiegen zwischen Januar und Dezember 2018 um 250% an



Angriffe auf die Software-Lieferketten nahmen in den letzten Jahren zu



Über 400.000 Infektionsversuche mit Dofoil wurden weltweit in den ersten 12 Stunden erkannt und geblockt



Empfehlungen

Präventive Kontrollmechanismen

- Security Hygiene ist entscheidend
- Implementieren Sie Zugangskontrollen und Identitätsschutz
- Behalten Sie Backups
- Seien Sie aufmerksam und handeln Sie

Empfehlungen

Erkennung und Reaktion

- Die SOC-Entwicklung kann auf jede Stufe des Observe Orient Decide Act (OODA) abgebildet werden.

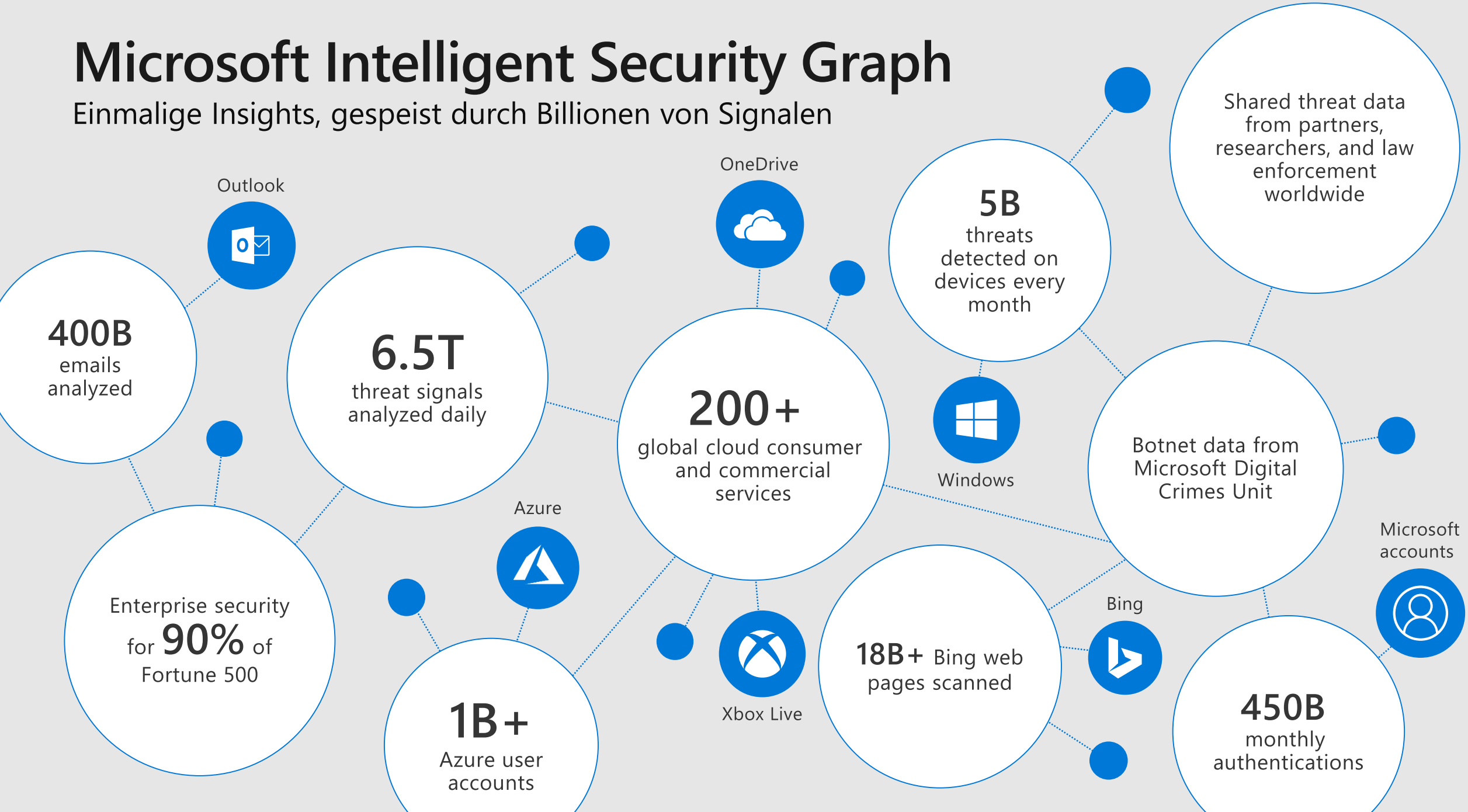
- Andere Trends, die für einen modernen SOC gelten
  - Qualität über Quantität von Alert-Feeds
  - Das Gesetz der Datengravitation nutzen
  - Hohe Kontexterkennung

Microsoft

Künstliche Intelligenz als Teil moderner Security Werkzeuge

Microsoft Intelligent Security Graph

Einmalige Insights, gespeist durch Billionen von Signalen

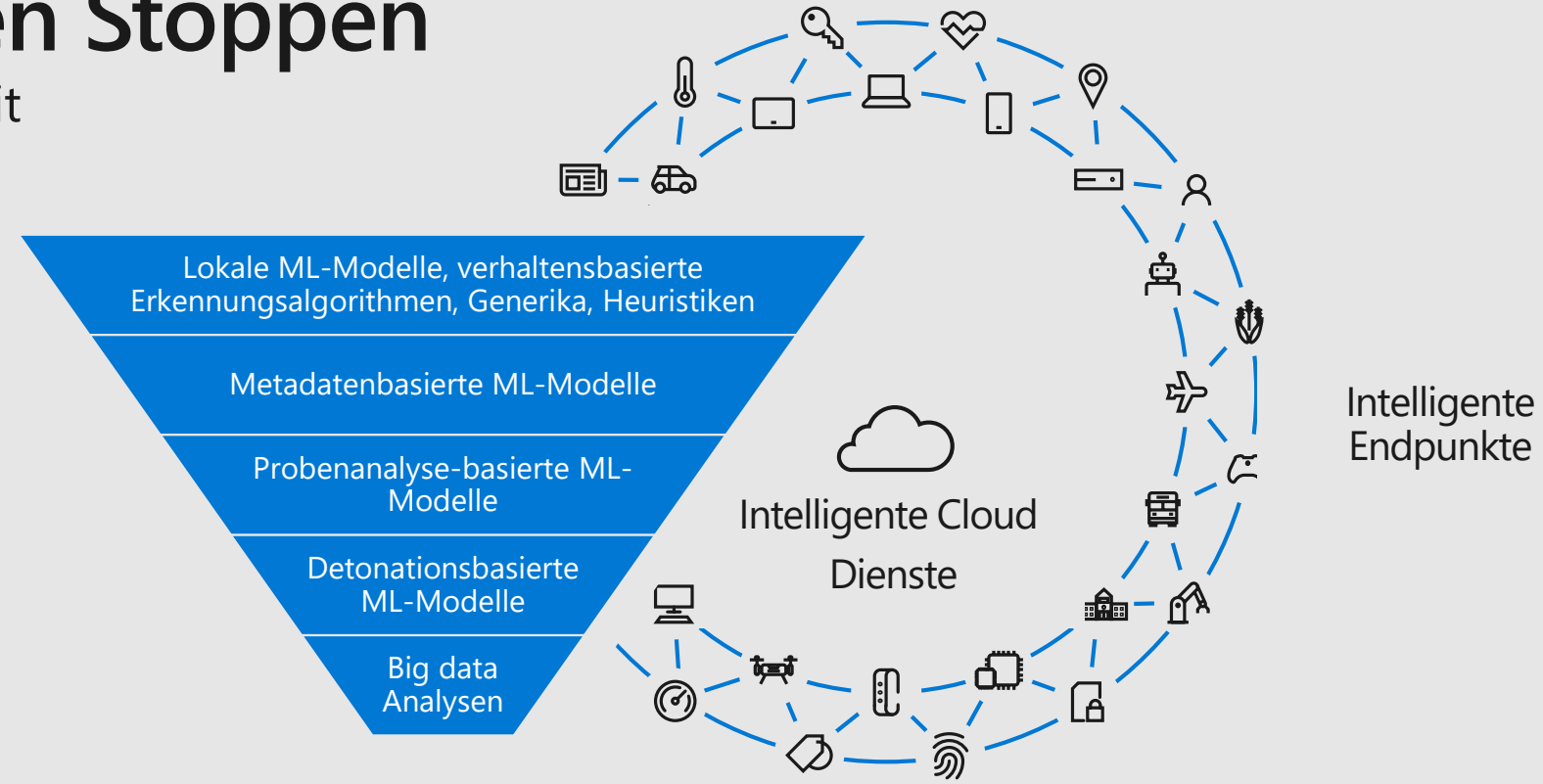


Mit Microsoft KI den Bedrohungen immer einen Schritt voraus

- → Täglich werden über 6,5 Billionen Signale analysiert, um einen beispiellosen Einblick in die Bedrohungslandschaft zu erhalten
- → mehr als 3500 Mitarbeiter arbeiten an Entwicklung und Verbesserung
- → Stärkung des führenden Partner-Ökosystems für intelligente Sicherheitstools

Cyberattacken Stoppen

Intelligenz bei der Arbeit



2017

Oktober 2017 - Cloud-basierte Detonation ML-Modelle identifizierten Bad Rabbit und schützten Benutzer 14 Minuten nach der ersten Begegnung.

3. Februar - Client-Algorithmen für maschinelles Lernen haben den Malware-Angriff Emotet automatisch in Echtzeit gestoppt.

6. März - Verhaltensbasierte Erkennungsalgorithmen blockierten mehr als 400.000 Instanzen des Dofoil-Trojaners.

August 2018 - Cloud-Algorithmen für maschinelles Lernen blockierten eine gezielte Kampagne, um Ursnif-Malware an weniger als 200 Ziele zu liefern

2018

Microsoft KI in der Praxis

Identitäts- und Zugriffsverwaltung

Intelligente Sicherheitsfunktionen nutzen Echtzeitsignale, um Identitäten zu sichern und „zero trust“ zu erreichen

Adaptive Algorithmen und Heuristiken für maschinelles Lernen werden zur Authentifizierung der Benutzeranmeldung verwendet

Azure Active Directory-Identitätsschutz verwendet adaptives maschinelles Lernen, um Anomalien zu erkennen, die auf potenziell gefährdete Identitäten hinweisen

User and location

Device

Apps

Real-time risk

Die Analyse von Echtzeitsignalen wird verwendet, um zu bestimmen, wann der Zugriff auf Organisationsdaten, Anwendungen und das Netzwerk zulässig ist

Sicherheitsprotokolle werden über das Intelligente Sicherheitsdiagramm gemeinsam genutzt, um die Korrelation und Untersuchung von Sicherheitswarnungen in der gesamten Bedrohungslandschaft zu unterstützen

Schutz vor Bedrohungen

Korrelieren Sie Sicherheitswarnungen über Angriffsvektoren hinweg, um Bedrohungen effektiver zu erkennen und darauf zu reagieren

Sensoren erkennen schädliche E-Mails und Malware-Anhänge

Bedrohungsinformationen aus einem böswilligen Anhang werden mit der Cloud Protection Engine geteilt

Office 365 blockiert diesen Anhang und entfernt die Datei aus allen anderen Postfächern

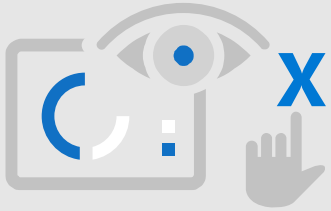
Windows Defender ATP leitet eine automatische Untersuchung aller geschützten Geräte ein

Informationsschutz

Automatisieren Sie die Klassifizierung vertraulicher Daten und wenden Sie Schutzmaßnahmen an, die den Daten überall dort folgen, wo sie übertragen werden

Sensible Daten können beim Erstellen automatisch identifiziert und klassifiziert werden

Richtlinienschutz verhindert automatisch nicht autorisierte Aktionen wie nicht genehmigten Zugriff oder Überfreigabe



Erweiterte Untersuchungstools helfen Administratoren, schnell auf Sicherheitswarnungen zu reagieren

Sicherheitsmanagement

Stärken Sie Ihre Sicherheitslage mit integrierter Intelligenz, die umsetzbare Sicherheitsinformationen für Ihr digitales Unternehmen liefert

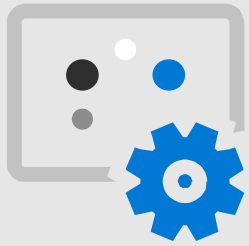
Mithilfe des maschinellen Lernens automatisiert die Angriffsflächenreduzierung (Attack Surface Reduction, ASR) die Durchsetzung von Regeln, um eine dynamische Erkennung und Reaktion auf Bedrohungen zu ermöglichen

Die Überwachung und Berichterstellung mithilfe des intelligenten Sicherheitsdiagramms unterstützt Sie beim Verbinden der Punkte über ASR-Ereignisse, Computer und Geräte sowie Netzwerke hinweg

Mit Impact-Simulatoren können Administratoren die Auswirkung einer neuen Regel auf die Produktivitätsanforderungen der Benutzer messen

App Entwicklung

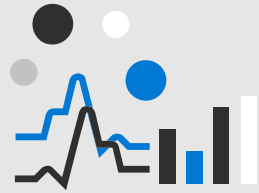
Finden Sie kritische Sicherheitslücken in Software mit einem intelligenten Fuzz-Testdienst, der auf dem Microsoft Intelligent Security Graph basiert



KI-gestützte Fuzz-Tests zur Aufdeckung von Sicherheitslücken in unseren Apps und Diensten

Kunden können ihre eigene Software analysieren - für Windows-, Linux- und Webanwendungen

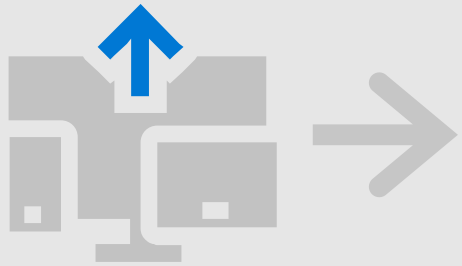
Identifiziert wertvolle Fehler und erstellt umsetzbare Testfälle zur Untersuchung und Behebung



Vulnerability Insights werden verwendet, um die AI-betriebenen Bug-Scanner zu bereichern

Intelligente Security Analytics Tools

Stellen Sie intelligente Sicherheitsanalysen für Ihr gesamtes Unternehmen bereit und entlasten Sie Ihre SecOps-Teams mit einer cloudbasierten Lösung für das Sicherheitsinformations- und Ereignismanagement (SIEM)

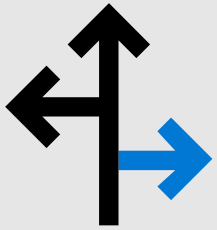


Verbinden Sie alle Ihre Sicherheitsinformationen und Ereignisquellen, um Daten für alle Benutzer, Geräte, Apps und Infrastrukturen zu sammeln

Erkennen Sie legitime Bedrohungen schnell, indem Sie mithilfe von Microsoft AI Warnungen über mehrere Dienste hinweg korrelieren und eine priorisierte Liste verdächtiger Aktivitäten erstellen

Erforschen Sie mit einer interaktiven Visualisierung, die den gesamten Umfang jedes Angriffs aufdeckt

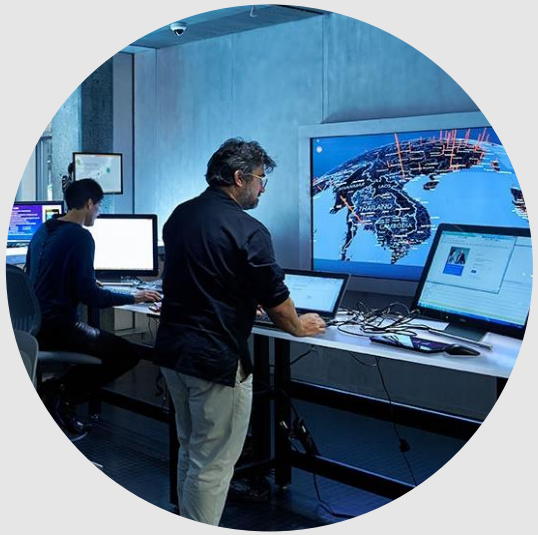
Vereinfachen Sie Sicherheitsvorgänge und beschleunigen Sie die Reaktion auf Bedrohungen durch integrierte Automatisierung und Orchestrierung gängiger Aufgaben und Workflows



Partnerschaften

Stärkung des führenden Partner-Ökosystems für intelligente Sicherheitstools

Zusammenarbeit mit Kollegen bei AI-Sicherheitstechniken



Mit Partnern intelligente Sicherheitslösungen entwickeln

Weitergabe von Sicherheitseinblicken, von denen alle profitieren

"Wir erweitern die Grenzen in Bezug auf KI, Edge-Computing und IoT und bieten umfassende Sicherheit, um jedes Unternehmen in die Lage zu versetzen, seine eigenen digitalen Fähigkeiten zu entwickeln und in dieser neuen Ära erfolgreich zu sein.

-**Satya Nadella**, CEO, Microsoft

Weiterführende Informationen

Laden Sie den vollständigen Microsoft Security Intelligence-Bericht v24 für mehr Einblicke herunter.

www.microsoft.com/sir

Weitere Informationen finden Sie im Microsoft Security Blog
Rund die neuesten Cybersicherheitsthemen

www.microsoft.com/security/blog

Allgemeine Produktinformationen zu den Microsoft 365 Sicherheitslösungen und Produkten

https://www.microsoft.com/de-de/security

Vielen Dank für Ihre Aufmerksamkeit!

Microsoft Deutschland GmbH
Walter-Gropius Straße 5
80807 München