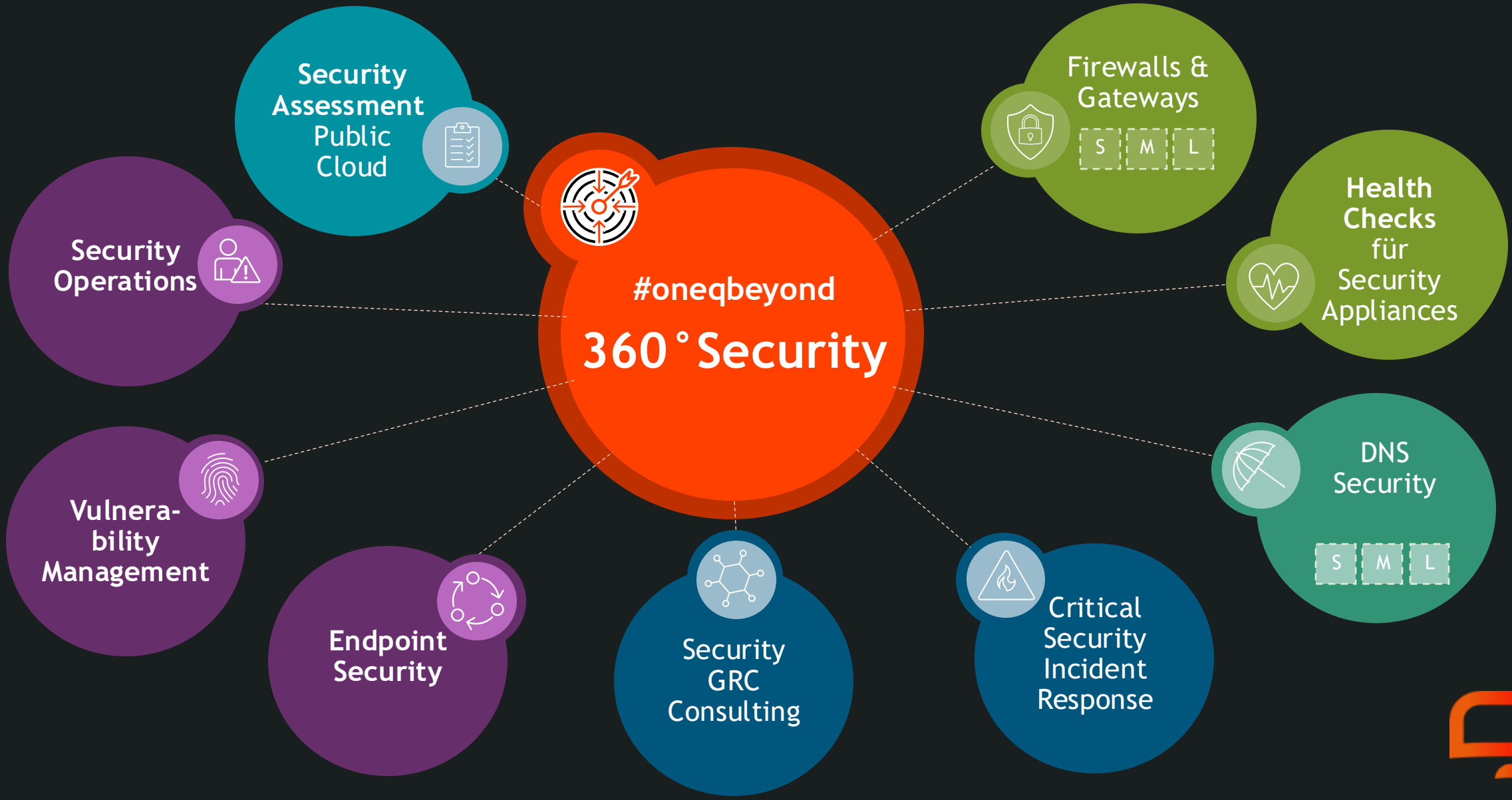
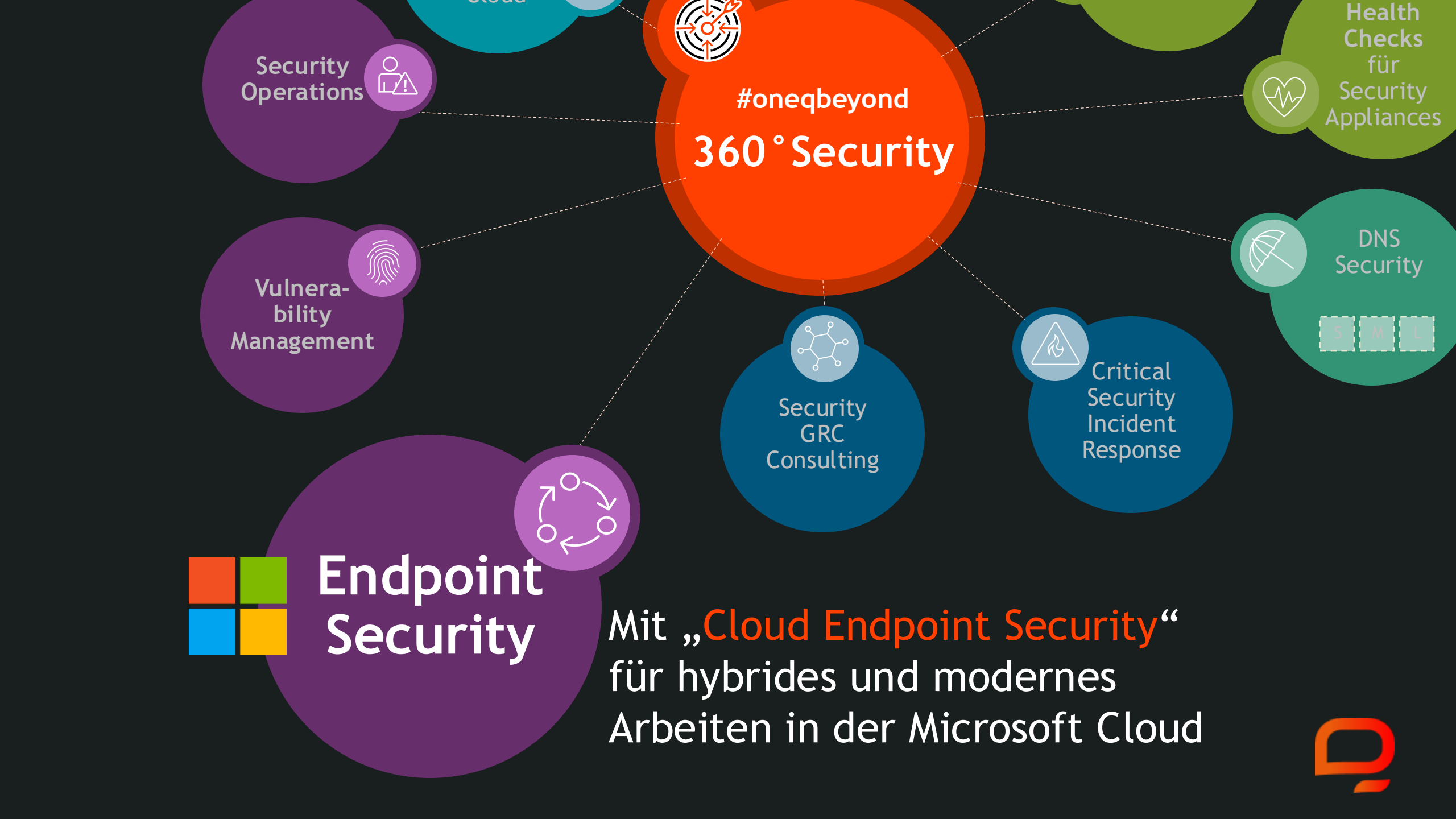
Cloud Endpoint Security

Lösungsangebot

q.beyond

q.beyond 360° Security Services:
Auf Dauer Verlässlichkeit, Effizienz und Sicherheit erhalten





Mit „Cloud Endpoint Security“ für hybrides und modernes Arbeiten in der Microsoft Cloud

Security Herausforderungen durch „Modern Work“ und „modern Workers“

q.beyond

Moderne und flexible Arbeitsformen erfordern eine Anpassung der Endpoint Strategie

Flexible Arbeitsregelungen und die weit verbreitete Unterstützung von BYOD-Programmen haben branchenübergreifend zu erhöhten Risiken für die Endpunktsicherheit geführt.

Eine Datenschutzverletzung kostet durchschnittlich 4,4 Millionen US-Dollar[1] und signalisiert die Notwendigkeit, die Sicherheit zu optimieren.

IT-Führungskräfte fühlen sich angesichts der wirtschaftlichen Unsicherheit unter Druck gesetzt, ihre Produktivität zu steigern.

67 % der **IT-Administratoren** sind jedoch bereits mit der Verwaltung flexibler Arbeit **überfordert**[2].

Die Menge an Daten, E-Mails, Besprechungen und Benachrichtigungen hat die Fähigkeit des Menschen, alles zu verarbeiten, überholt.

64 % der Mitarbeiter geben an, dass sie **nicht genug Zeit** haben, um ihre Arbeit zu erledigen[3].

1. IBM, “Cost of a data breach 2022.” Accessed June 7, 2023. https://www.ibm.com/reports/data-breach
2. JumpCloud. “IT Trends Report: Remote Work Drives Priorities in 2021.” Accessed June 7, 2023. https://jumpcloud.com/resources/it-trends-report-remote-work-security-cloud-services.
3. Microsoft, Work Trend Index Annual Report: Will AI Fix Work?, May 9, 2023. https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work

Flexibles Arbeiten generiert Herausforderungen … und Chancen

Bieten Sie einen **sicheren Zugriff auf die IT-Umgebung** des Unternehmens mit **personalisiertem Schutz** und ermöglichen Sie gleichzeitig flexibles Arbeiten.

Vereinfachen Sie das Endpunktmanagement und senken Sie die Support- und Lizenzkosten, die mit der Verwaltung von Geräten und virtuellen Desktop-Umgebungen verbunden sind, und beschleunigen Sie gleichzeitig die Wertschöpfung.

Sorgen Sie für außergewöhnliche Produktivität auf jedem Endpunkt,

Stellen Sie Ihren Mitarbeitern vielseitige, zugängliche moderne Geräte zur Verfügung

und unterstützen Sie BYOD-Programme, ohne die Sicherheit zu beeinträchtigen.

Die Welt des hybriden Arbeitens entwickelt sich weiter...

38%

der Menschen arbeiten bereits hybrid

52%

der Menschen erwägen den Übergang zu Remote- oder Hybridarbeit

50%

der Menschen nutzen ein privates Gerät für die Arbeit

Und das gilt auch für die Bedrohungen und Herausforderungen

83%

der Unternehmen haben mindestens einen Firmware-Angriff in den letzten 2 Jahren erlebt

25%

der Unternehmen haben den unbefugten Zugriff auf vertrauliche Daten als größte Sicherheits-bedrohung identifiziert

921

Passwörter werden je Sekunde angegriffen

Die Menschen arbeiten an mehr Orten, mit mehr Flexibilität und mehr Geräten

Es braucht Antworten auf die wesentlichen Fragen:

Wie sichern Sie Ihre Endgeräte zuverlässig ab?

Wie reduzieren Sie die Komplexität von IT-Workloads?

Wie gewährleisten Sie den Schutz und ermöglichen gleichzeitig Flexibilität und Produktivität der Mitarbeiter?

Technologie muss dafür sorgen, dass wir in Verbindung und produktiv bleiben, während sie gleichzeitig unsere Sicherheitslage in einer immer anspruchsvolleren und komplexeren Welt stärkt.

Unsere Antwort

Die fünf Komponenten einer modernen Endpoint Lösung

Devices

Die spezifische Jobanforderungen erfüllen

Operating system

Das ist sicher, zuverlässig, von den Mitarbeitern akzeptiert und einfach zu verwalten und zu aktualisieren

Endpoint security

Die vor Cyberangriffen über mehrere Plattformen hinweg schützt

Management

Entwickelt für einen gesamten Gerätebestand, einschließlich persönlicher Geräte

AI-powered productivity apps

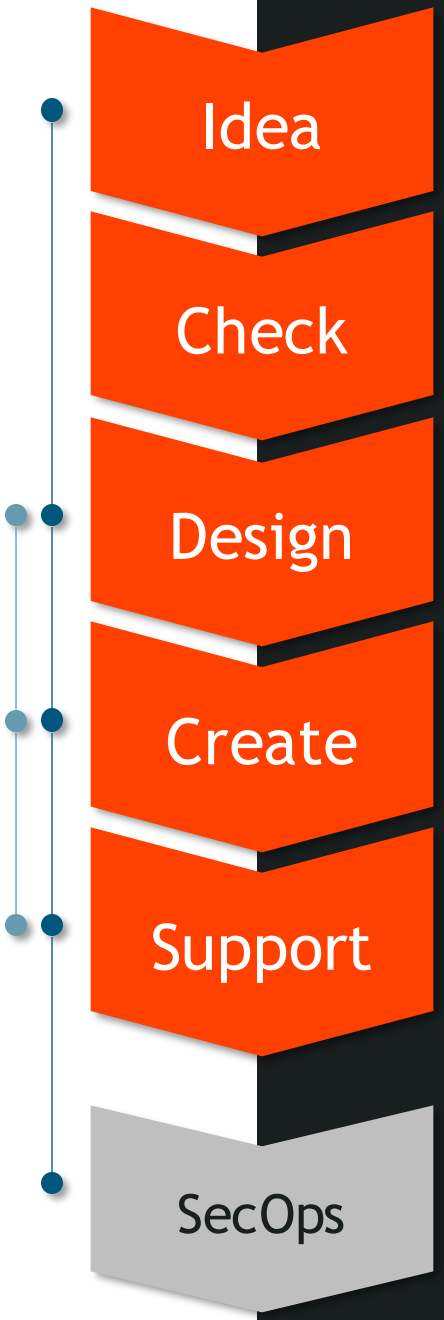
Die über alle Geräte und Geschäftsszenarien hinweg funktionieren

Microsoft liefert die komplette technische Lösung …

… als SaaS und damit immer auf dem neuesten Stand

Devices	Surface OEM	Windows 365 Cloud PC
Operating system	Windows 11 Enterprise	
Endpoint security	Entra ID Defender	Purview
Management	Intune & Intune Suite	Windows Autopatch
AI-powered productivity apps	Microsoft 365 Apps & Copilot	Microsoft Teams

q.beyond begleitet jede Phase der Journey für sicheres, flexibles und produktives Arbeiten



Was ist mit Microsoft‘s aktuellen Technologien zum Thema Endpoint möglich

Aktuelle Situation analysieren und bewerten, entwickeln eines Maßnahmenplans

Technisches Konzept für Ihre zukünftige Lösung entwickeln

Aufbau der Lösung in Ihrer Umgebung

Unterstützung bei Problemen oder Konfigurationsänderungen, kontinuierlich Best Practise

Sprechen Sie uns auch zu unserem Lösungspaket Managed SecOps an, um von unseren 7/24 Experten zu profitieren, die Ihre Umgebung überwachen

Idea

Endpoint Management with Security

DRAFT

Microsoft 365

Zielgruppe

- IT C-Level (CIO, Security, Technology)
- Endpoint Management Verantwortlicher
- Architekten, Engineers, Operations

Ziel des Workshops

Ermöglichen Sie es Benutzern, auf jedem Gerät produktiv und sicher zu arbeiten ohne die IT-Sicherheit zu beeinträchtigen

Organisatorisches

Laufzeit:
4 Wochen

Folgemaßnahmen

Umsetzung der identifizierten Maßnahmen zur Risikominimierung

Inhalt des Workshops

In diesem Workshop erfahren Sie, wie Sie intelligente Sicherheit, risikobasierte Kontrollen, Zero-Touch-Bereitstellung, erweiterte Analysen und eine tiefe Integration in die Microsoft-Produkte nutzen können, die Sie bereits verwenden. Durch Ihre Teilnahme können Sie:

- Erfahren Sie, wie Sie Ihre Verwaltungsfunktionen mit Microsoft Intune verbessern können.
- Ermitteln und schützen Sie Ihre Endpunkte, indem Sie Richtlinien durchsetzen und Sicherheitstools bereitstellen.
- Schützen Sie die Identitäten Ihrer Benutzer mit Multi-Faktor-Authentifizierung und bedingtem Zugriff von jedem Gerät aus.
- Ermöglichen Sie Ihren Benutzern, mit den Anwendungen, die sie benötigen, auf den gewünschten Geräten produktiv zu sein.

Check

Cybersecurity Assessment

DRAFT

Microsoft 365

Zielgruppe

- IT C-Level (CIO, Information Security, Risk)
- IT Security Architekten, Administratoren, Operations (Sec Ops)

Ziel des Workshops

Verstehen, wie gut ein Unternehmen auf gängige Sicherheitsbedrohungen vorbereitet ist und welche Maßnahmen ggf.erforderlich/sinnvoll sind

Organisatorisches

Laufzeit:
5 Wochen

Folgemaßnahmen

Umsetzung der identifizierten Maßnahmen zur Risikominimierung

Inhalt des Workshops

Während dieses Workshops erarbeiten wir mit Ihnen zusammen einen Ansatz, um die Cybersicherheit Ihres Unternehmens zu stärken. Wir helfen Ihnen, besser zu verstehen, wie Sie potenzielle Angriffe priorisieren und abwehren können. Dies umfasst u.a.

- Einblicke in häufige Cybersicherheitsbedrohungen und die Auswirkungen, die sie auf den Geschäftsbetrieb haben können
- Analyse der Ausrichtung Ihres Unternehmens auf gemeinsame Cybersicherheitsziele und Verbesserungsmaßnahmen, die dazu beitragen sollen, Ihre Position gegen von Menschen betriebene Ransomware und Datenlecks durch Insider-Bedrohungen zu stärken
- Einblick in die Integrität Ihres Endpunkts und Microsoft 365-Daten mithilfe von Scans von Microsoft-Sicherheitstools
- Langfristige Empfehlungen von Microsoft-Experten zu Ihrer Sicherheitsstrategie mit wichtigen Initiativen und taktischen nächsten Schritten.

Idea

Einstieg in Microsoft Defender for Endpoint/Server

Microsoft 365

Zielgruppe

- Entscheider: innen (IT)
- Administrator: innen

Ziel des Workshops

Ziel dieses Workshops ist es, die Teilnehmenden mit Microsoft Defender for Endpoint/Server vertraut zu machen und mögliche Einsatzszenarien zu identifizieren

Organisatorisches

Dauer: 2 PTage (1 Tag Workshop / 1 Tag Konzept)

Teilnehmendenzahl:
max. 5 Personen

Folgemaßnahmen

Projekt-Angebot zur Implementierung von Defender for Endpoint/Server auf Basis des individuellen Grobkonzeptes

Inhalt des Workshops

1. Vorstellung der Ziele des Workshops und Klärung der Erwartungen
2. Präsentation der Funktionalitäten von Defender for Endpoint/Server (P1 + P2)
3. Geräte Onboarding, Tagging und Gerätegruppen
4. Einblick in das Defender Security Portal
5. Defender for Endpoint/Server Konfigurationsmöglichkeiten
6. Besprechung der nächsten Schritte

Idea

SIEM und XDR: Kombinierter Schutz vor Ransomware

Microsoft 365

Zielgruppe

- CSO, CISO, CSO
- IT-Security, IT-Administrator:innen

Ziel des Workshops

Wie sich die Sicherheitstools der nächsten Generation von Microsoft nutzen lassen

Organisatorisches

Laufzeit:
5 Wochen

Teilnehmendenzahl:
max. 10 Personen

Folgemaßnahmen

Umsetzung der identifizierten Maßnahmen zur Risikominimierung

Inhalt des Workshops

Weiß das Unternehmen, wie viele Phishing-Angriffe es bereits erhalten hat? Ob die Mitarbeitenden das richtige Passwortprotokoll verwenden? Ob persönliche Daten preisgegeben werden? Kurzum, ist die Cloud-Umgebung des Unternehmens so sicher, wie die Verantwortlichen es glauben?

Im Rahmen des Workshops werden Maßnahmen identifiziert, um die Sicherheitslage im Unternehmen zu verbessern.

1. Analyse
   - Bedrohungen durch Cyberangriffe analysieren, die auf das Unternehmen abzielen
2. Empfehlungen
   - Sofortigen Entschärfung der festgestellten Bedrohungen
3. Detaillierte Bewertung
   - IT- und Sicherheitsprioritäten und - initiativen, direkt von Cyber-Security-Profis
4. Einblick
   - Ganzheitlicher Sicherheitsansatz von Microsoft und wie er sich auf das Unternehmen auswirkt
5. Demonstrationen
   - Integrierte Sicherheit, einschließlich der neuesten Tools und Methoden
6. Langfristige Empfehlungen
   - Sicherheitsstrategie, mit Schlüsselinitiativen und taktischen nächsten Schritten

Support

Microsoft 365 Operation

DRAFT

Microsoft 365

Zielgruppe

- IT Operations

Ziel

- Jederzeit verlässliche und kompetente Unterstützung in der alltäglichen Nutzung von M365
- Zugang zu Expertenwissen und Best Practises

SLA

- **Servicezeit:** Mo-Fr 9-17 Uhr, 7/24 optional verfügbar
- **Reaktionszeit:** 4 Stunden

Pricing

Preis pro User, abhängig von dem konkreten Nutzungsumfang von M365 (z. B. E3 oder E5)

Leistungsumfang

Microsoft 365 Operation umfasst folgende Leistungsbestandteile:

- Administrative Konfiguration von Microsoft 365 (Request Fulfillment)
- Überwachung der Kernfunktionen von Microsoft 365 durch unabhängige Werkzeuge
- Incident Management bei Störungen oder Problemen mit Microsoft 365

Ihre Vorteile

Eine einheitliche Lösung für die Verwaltung von Endpunkten an jedem Ort

Vereinfachen Sie die Verwaltung

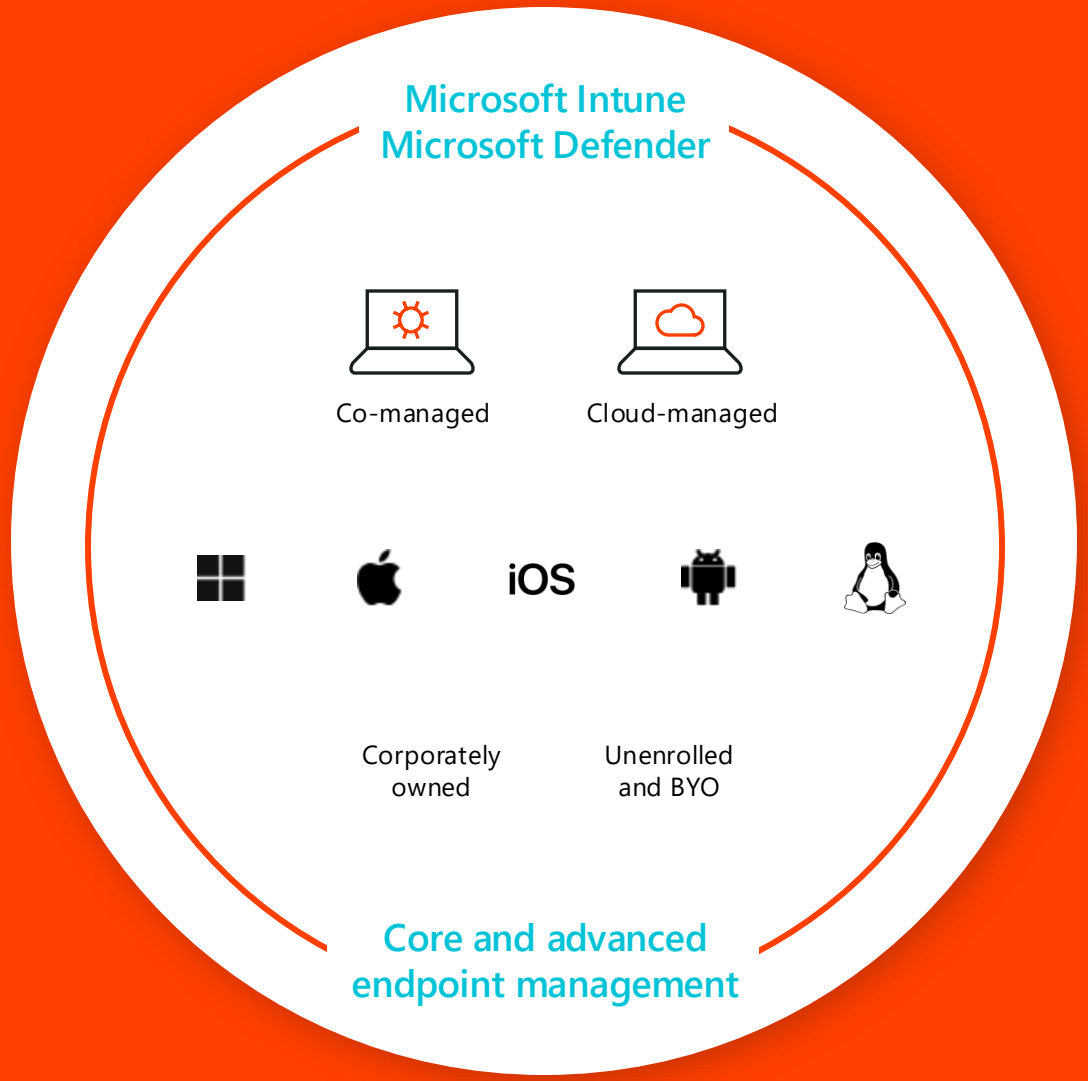
Ermöglichen Sie den Wechsel zum Cloud-Management und nutzen Sie umfassende Einblicke in Endpunktanalysen und Cloud-basierte Bereitstellung.

Schutz hybrider Arbeitsmodelle

Schützen Sie Benutzer, Apps und Daten auf allen Geräten mit Defender für Endpunkt.

Bessere Benutzererfahrung

Ermöglichen Sie Benutzern die Geräte- und Anwendungsverwaltung für iOS, macOS, Linux und Android.



Do More With Less using Microsoft 365

Digital Worker schützen

Schaffen Sie überall eine sichere, flexible Arbeitsumgebung und verbessern Sie gleichzeitig die Endpunkttransparenz.

Senken Sie die Sicherheitskosten mit vorintegrierten Identitäts-, Endpunktmanagement- und Sicherheitslösungen, um die Zero-Trust-Architektur voranzutreiben.

IT Management vereinfachen

Automatisieren Sie Systemaktualisierungen, um Kosten zu senken und die IT-Administration zu optimieren.

Verbessern Sie die IT-Effizienz für neue Geräte, Anwendungen und das Datenmanagement.

Redundante Lösungen eliminieren

Konsolidieren Sie komplexe Lizenzstrukturen.

Eliminieren Sie redundante Funktionen und profitieren Sie gleichzeitig von einer nahtlosen, nativen Integration.

Microsoft Entra ID, Defender for Endpoint, Intune and Windows 11:
The value of more

Microsoft-Endpunktlösungen ermöglichen es Ihnen, mit weniger mehr zu erreichen

Infrastructure absichern

Organisationen mit M365 E3 profitieren von verbesserter Sicherheit zur Identifizierung und Behebung von Bedrohungen im Wert von 40 US-Dollar pro Benutzer[1]

Kosten im Zusammenhang mit Sicherheitsverletzungen werden um 1 Mio. US-Dollar reduziert[2]

Die standardmäßig aktivierten Sicherheitsfunktionen von Windows 11 können das Risikoprofil des Betriebssystems um 20 % bis 30 % pro Jahr verbessern[3]

Bis zu 10 % jährliche Reduzierung der Ausgaben für Sicherheitssoftware von Drittanbietern mit Windows 11 OS Environment Security[3]

Endpoint Management vereinfachen

Verkürzung der Einrichtungszeit für einen neuen Endpunkt um 75 %[1]

Verkürzung des Zeitaufwands für die Bereitstellung/Verwaltung von Software um 25 %[1]

5,2 Mio. US-Dollar für die Konsolidierung von ADV-Management-Tools[2]

Automatisierte Systemaktualisierungen können die Kosten für das IT-Management um 40 % senken und den Zeitaufwand für die Geräteverwaltung um 24 % reduzieren.[3]

Mit Windows 365 können Unternehmen Einsparungen von 40 % im Vergleich zu lokaler VDI[4] erzielen und gleichzeitig die Kosten für die Desktopbereitstellung um 88 %, die Wartung um 88 % und die Wiederherstellung um 96 % senken[5]

Produktivität steigern

Steigerung der Endbenutzerproduktivität um bis zu 15 %[3]

60 % Lizenzersparnis pro Benutzer mit M365 E3[1]

1,6 Mio. US-Dollar durch Steigerung der IT-Produktivität[2]

2,2 Mio. US-Dollar durch verbesserte Produktivität von Power-Usern[5]

Einsparungen in Höhe von 1,1 Mio. US-Dollar bei den IT-Kosten für das Onboarding von Auftragnehmern, die Gerätewartung und das Offboarding mit W365[5]

719.000 US-Dollar durch beschleunigte Produktivität für Mitarbeiter, die durch M365 A5 gewonnen wurden

1. Forrester Consulting, The Total Economic Impact™ of Microsoft 365 E3, commissioned by Microsoft, October 2022.
2. Forrester Consulting, New Technology: The Projected Total Economic Impact™ Of The Microsoft Intune Suite, commissioned by Microsoft, March 2023.
3. Forrester Consulting, New Technology: The Projected Total Economic Impact™ Of Windows 11, commissioned by Microsoft, July 2022.
4. Enterprise Strategy Group Economic Validation, Exploring the Economic Benefits of Windows 365, June 2022.
5. Forrester Consulting, The Total Economic Impact™ of Windows 365, commissioned by Microsoft, March 2023.

Question & Answers


q.beyond
expect the next