inetum realdolmen

Positive digital flow

"La Cybersecurité, une vaccination pour votre environment digital”

General program introduction

30/03/2022

Program overview

1 Security market watch “Understanding the trends, challenges & threats”

Goal: Understanding the challenges and risks you face by clarifying and becoming aware of the impact and likelihood of threats

By: Inetum-Realdolmen – Thomas Tardieux

2 Security vision ”How to navigate your security transformation”

Goal: Gaining practical insights in how you can approach your digital security transformation journey to improve your security posture and support the hospital business objectives

By: Inetum-Realdolmen – Thomas Tardieux

3 Achieving adequate cybersecurity in Healthcare with Microsoft technology

Goal: Gaining insights in achieving adequate cybersecurity in healthcare

By: Microsoft – Jonathan Jacqmin & Nadia Aime

Parvenir à une cybersécurité adéquate dans le secteur des soins de santé

Nadia Aimé – Spécialiste technique en Cybersécurité chez Microsoft

Jonathan Jacqmin – Spécialiste du poste de travail moderne dans l'équipe santé chez Microsoft

Résumé

Ensemble, nous réaliserons ce moment.

La sécurité des actifs et des technologies des hôpitaux est essentielle à la prospérité future des soins de santé.

La récente augmentation exponentielle des incidents de cybersécurité reflète l'importance de cette tâche et constitue **un pas en avant unificateur** pour notre gouvernement et notre industrie des soins de santé dans la lutte contre les menaces en constante évolution et de plus en plus sophistiquées dans l'ensemble de l'écosystème numérique.

Avec une **feuille de route éprouvée** en main, Microsoft Healthcare est prêt à s'associer aux agences de soins de santé pour conduire cette nouvelle ère en matière de cybersécurité.

En utilisant les informations et les ressources rassemblées ici, les agences de soins de santé peuvent mieux comprendre les jalons à court et à long terme;

- élaborer une réponse stratégique alignée sur les priorités de modernisation de la sécurité et les exigences spécifiques de l'industrie des soins de santé;
- déterminer comment les partenaires technologiques peuvent aider à accélérer cette transformation

Protéger le cyber-paysage des soins de santé

Le secteur de la santé en un coup d'œil

- Le secteur est confronté à **des cyberattaques de plus en plus sophistiquées** et ciblées qui menacent leurs actifs les plus critiques, leurs processus durables, ainsi que la sécurité et la confidentialité des employés et des patients du secteur de la santé. Nous avons besoin d'une réponse nationale concertée qui rassemble les esprits les plus brillants et les technologies les plus avancées des secteurs public et privé pour **protéger l'industrie des soins de santé** contre les cyber-acteurs malveillants.
- Pour améliorer la cybersécurité et protéger les réseaux de soins de santé, il est nécessaire de **prendre des mesures audacieuses** pour reconnaître la cybersécurité comme une priorité nationale et **fournir des recommandations concrètes** pour faire face aux menaces en constante évolution et de plus en plus sophistiquées.
- L'objectif est de **moderniser l'infrastructure** informatique du fournisseur de soins de santé avec **un ensemble de normes** qui lui permettront de **faire face de manière proactive** aux menaces et de renforcer sa posture globale en matière de cybersécurité.
- En faisant progresser les capacités clés soulignées par cette ambition, le secteur de la santé peut relever ce grand défi. L'amélioration de la cybersécurité à l'échelle de l'industrie est réalisable grâce à **une collaboration étroite entre le secteur de la santé et l'industrie privé**, en tirant parti des **technologies modernes,** en utilisant **des stratégies de cybersécurité agiles** essentielles pour fonctionner dans l'environnement de menace d'aujourd'hui et demain.

Capacités de cybersécurité critiques mises en évidence dans le secteur de la santé

- Adoption accélérée du modèle Zero Trust
- Mise en œuvre de l'authentification multifacteur
- Défense d'entreprise pré- et post-violation unifiée
- Développement de logiciel sécurisé des applications d'entreprise

Protéger le cyber-paysage des soins de santé

Pour parvenir à une posture de cybersécurité qui réponde aux défis actuel et futur, Microsoft estime qu'il est essentiel que les organisations de soins de santé adoptent une approche qui donne la **priorité à trois domaines principaux**

Pour les agences de soins de santé, de nombreuses exigences à court terme doivent être satisfaites dans les semaines et mois à venir. Les délais ne doivent pas être considérés comme un effort de conformité « à cocher la case »; ils visent plutôt à **améliorer la posture de sécurité globale du secteur** et devraient s'inscrire dans **une stratégie à long terme**.

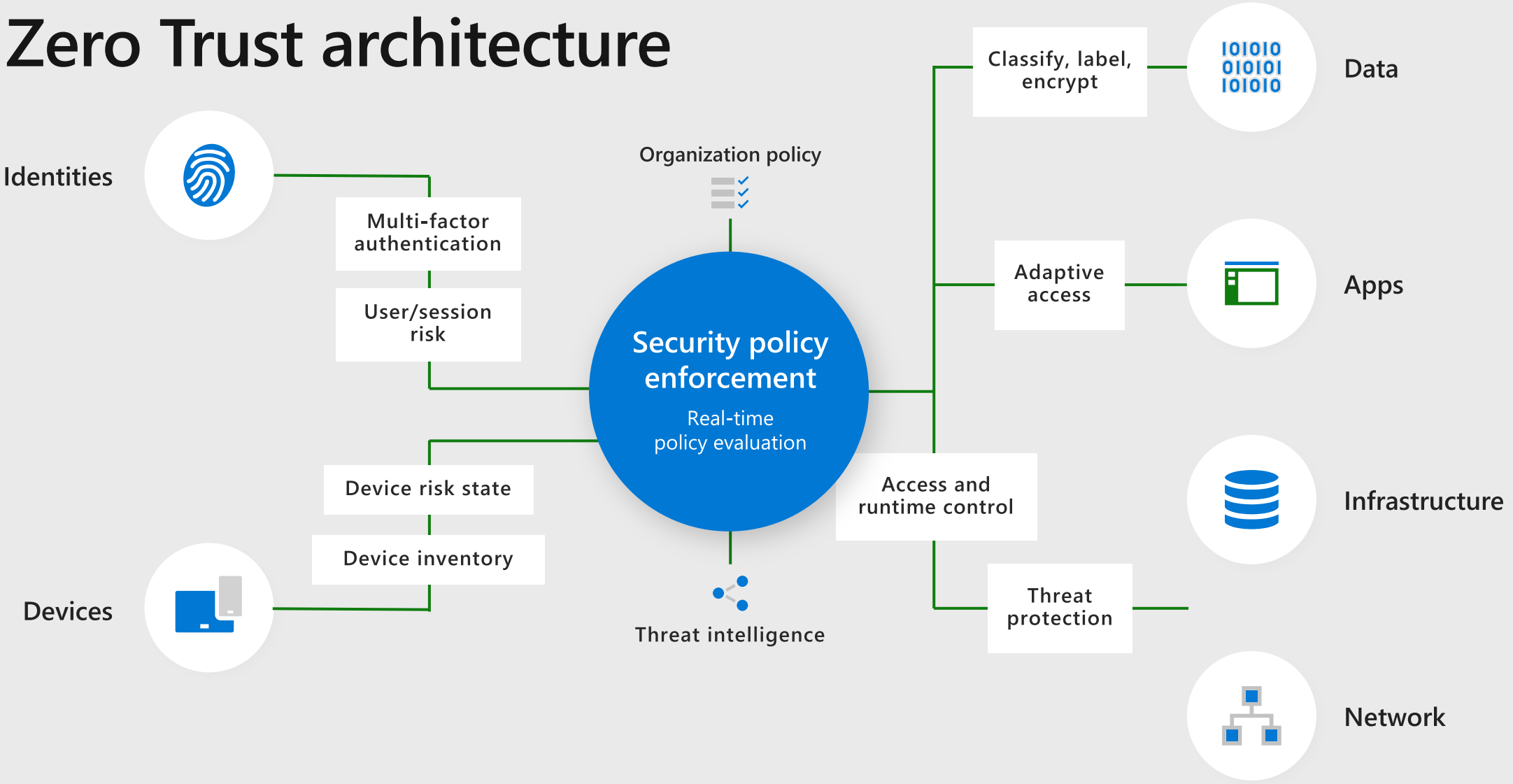
Un plan de déploiement pour améliorer les capacités et les résultats en matière de cybersécurité des agences de soins de santé

Le travail de modernisation de l'informatique est déjà en cours et une grande partie des bases de sécurité pour soutenir les agences de santé a été posée. En fait, de nombreuses organisations ne réalisent peut-être pas qu'ils ont déjà une technologie en place qui doit simplement être activée ou affinée pour répondre aux exigences de l'industrie.

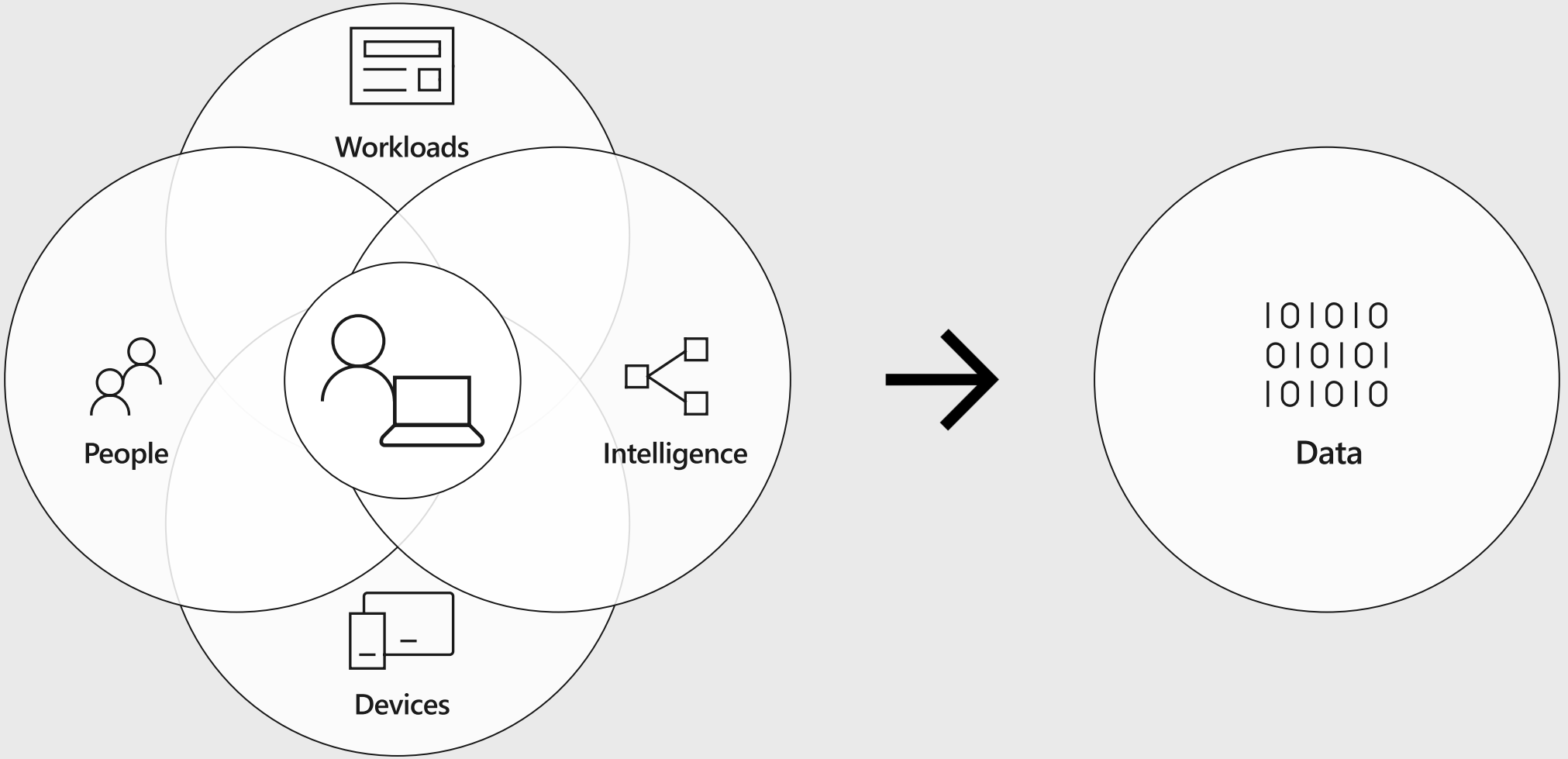
L'architecture de référence Cyber Security de Microsoft

Pour mettre en œuvre les stratégies, tactiques et solutions, Microsoft a développé une architecture de référence utilisant une série d'actifs de cybersécurité. Grâce aux ressources ci-dessous, les organismes peuvent répondre aux exigences spécifiques de chaque section et au-delà.

Zero Trust architecture



Comment démarrer avec Zero Trust



http://aka.ms/zero-trust

Microsoft 365 Defender

Arrêtez les attaques et réduisez la charge de travail des opérations de sécurité de 50 % grâce à la sécurité inter-domaines automatisée

- Sécurisez tous les clouds, toutes les plateformes
- Bénéficiez d’une protection intégrée de pointe
- Offrez une réponse rapide et intelligente

Budgétisation pour Microsoft Defender XDR et Zero Trust Security

- La création d'un cadre de sécurité Zero Trust avec plus de 20 fournisseurs n'a aucune chance de succès.
- C'est pourquoi la budgétisation de Microsoft Defender XDR pour Zero Trust Security doit être à l'avant-garde d'une stratégie de cybersécurité moderne pour les organisations de toute taille qui s'exécutent sur des plates-formes et des solutions Microsoft.
- Microsoft Defender XDR vous permet de consolider plus de 27 fournisseurs de sécurité en une seule plate-forme intégrée.
- Cela signifie qu'un fournisseur pour les appels de support, un seul panneau de verre pour effectuer une analyse médico-légale numérique et toute la suite est connectée via microsoft Intelligent Security Graph.
- (Sans parler de l'intégration transparente à la suite de productivité que des millions d'entre vous utilisent chaque jour.)

Microsoft's Platform Approach

Identity & access management

Secure identities to reach zero trust

Threat protection

Help stop damaging attacks with integrated and automated security

Information protection and governance

Locate, classify and govern information through integration

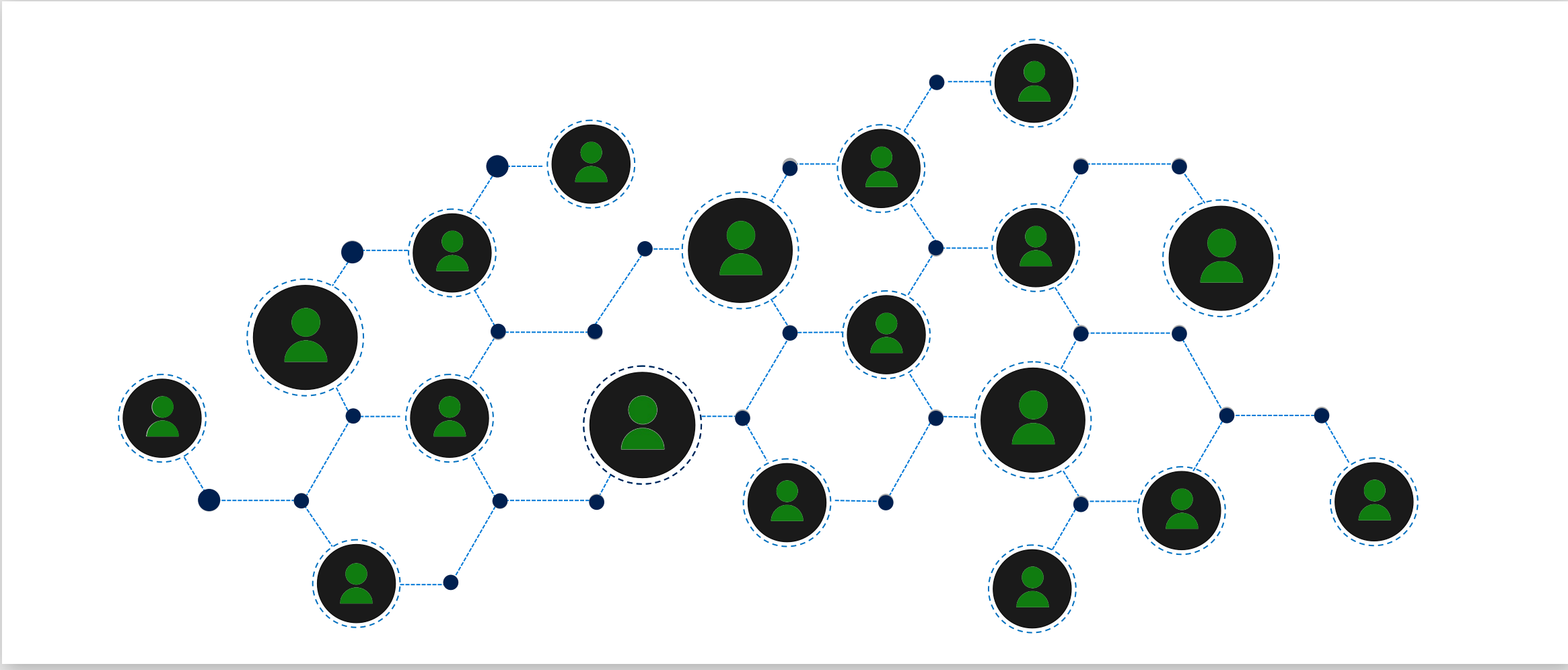
Security management

Strengthen your security posture with insights and guidance

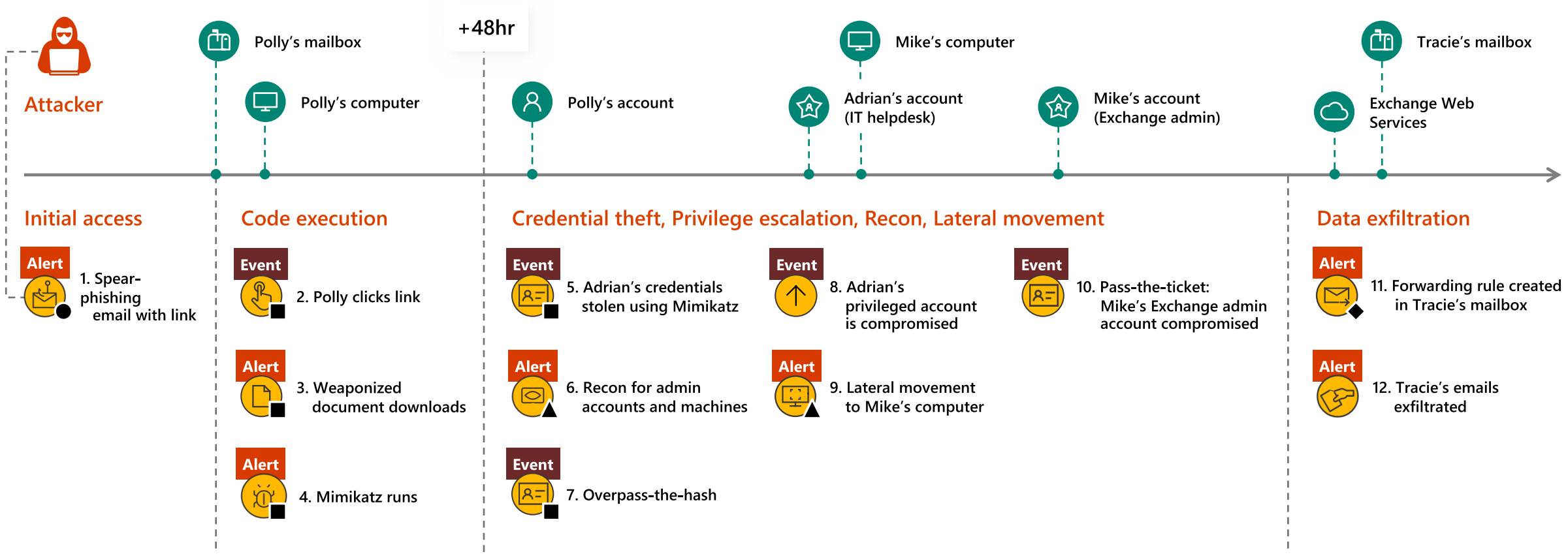
Infrastructure security

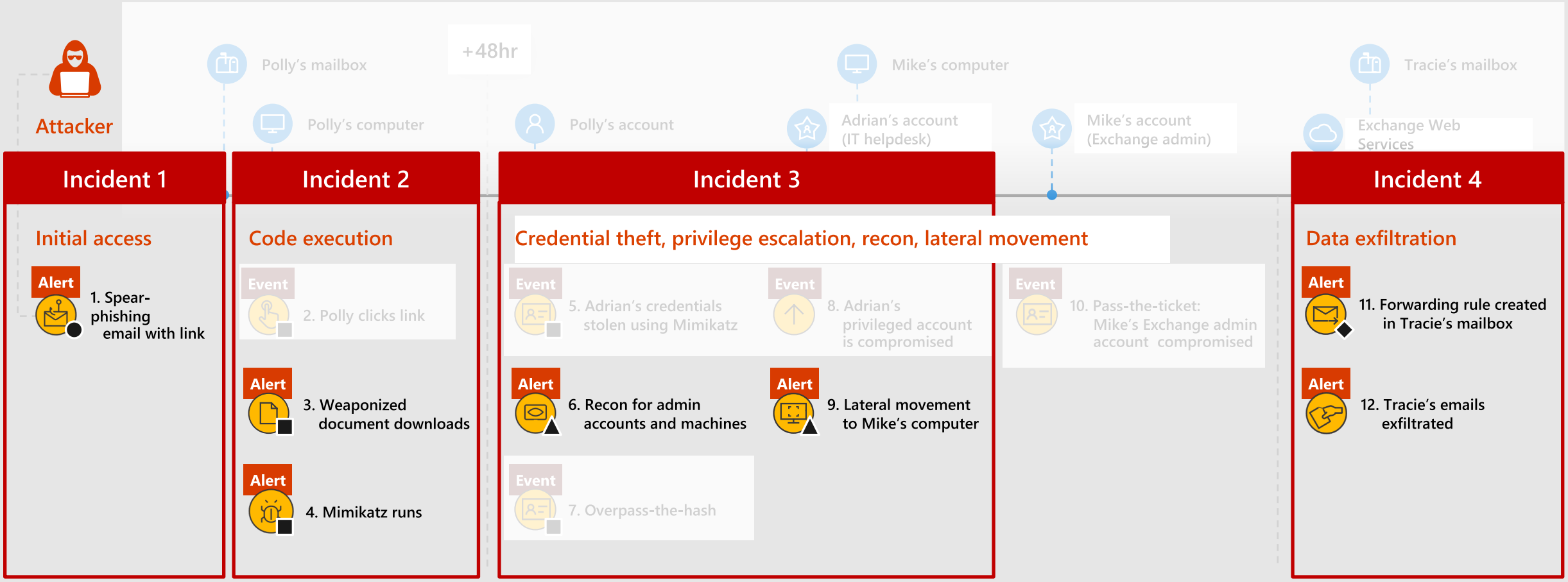
Un nouveau périmètre de sécurité : l'identité de l'utilisateur

Les utilisateurs sont le nouveau périmètre, et un seul utilisateur compromis peut entraîner un arrêt de l'entreprise, mais un utilisateur sécurisé peut être votre meilleure protection

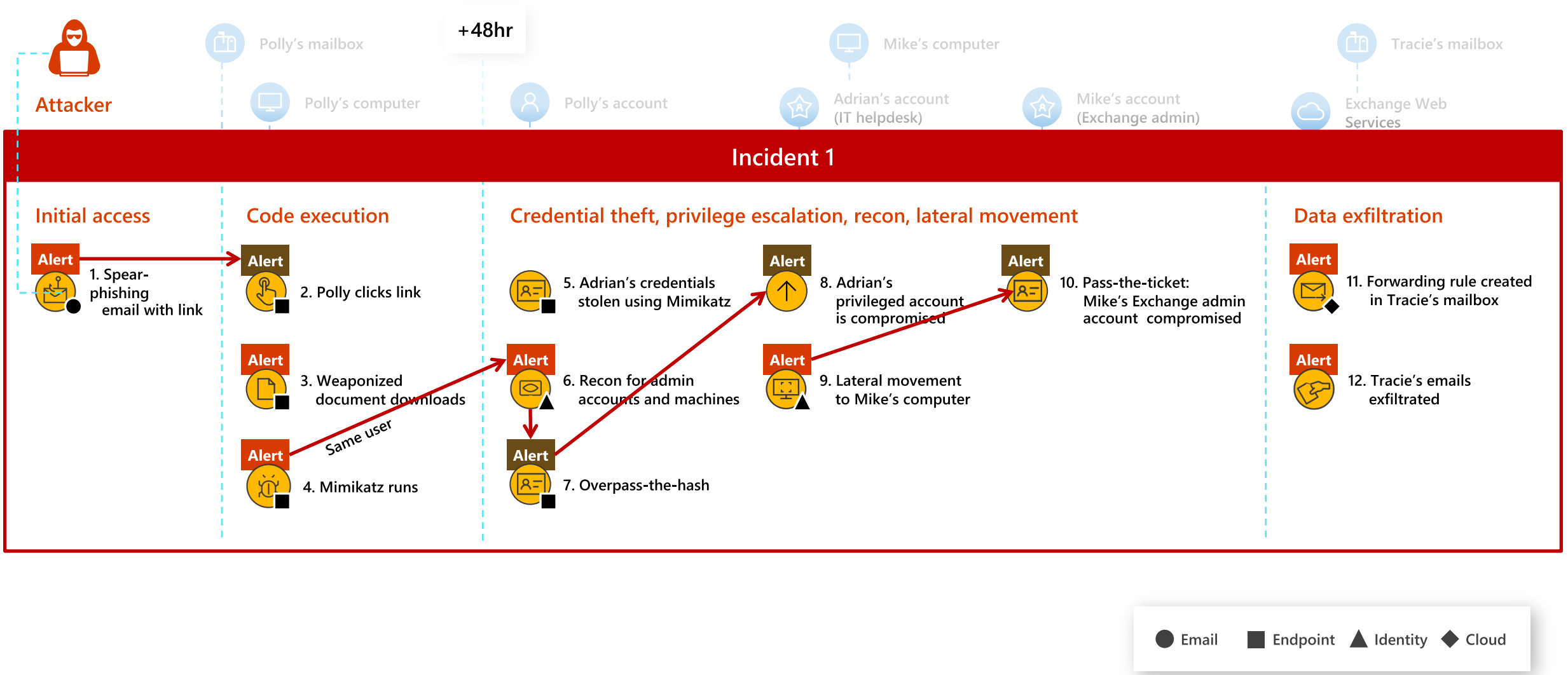


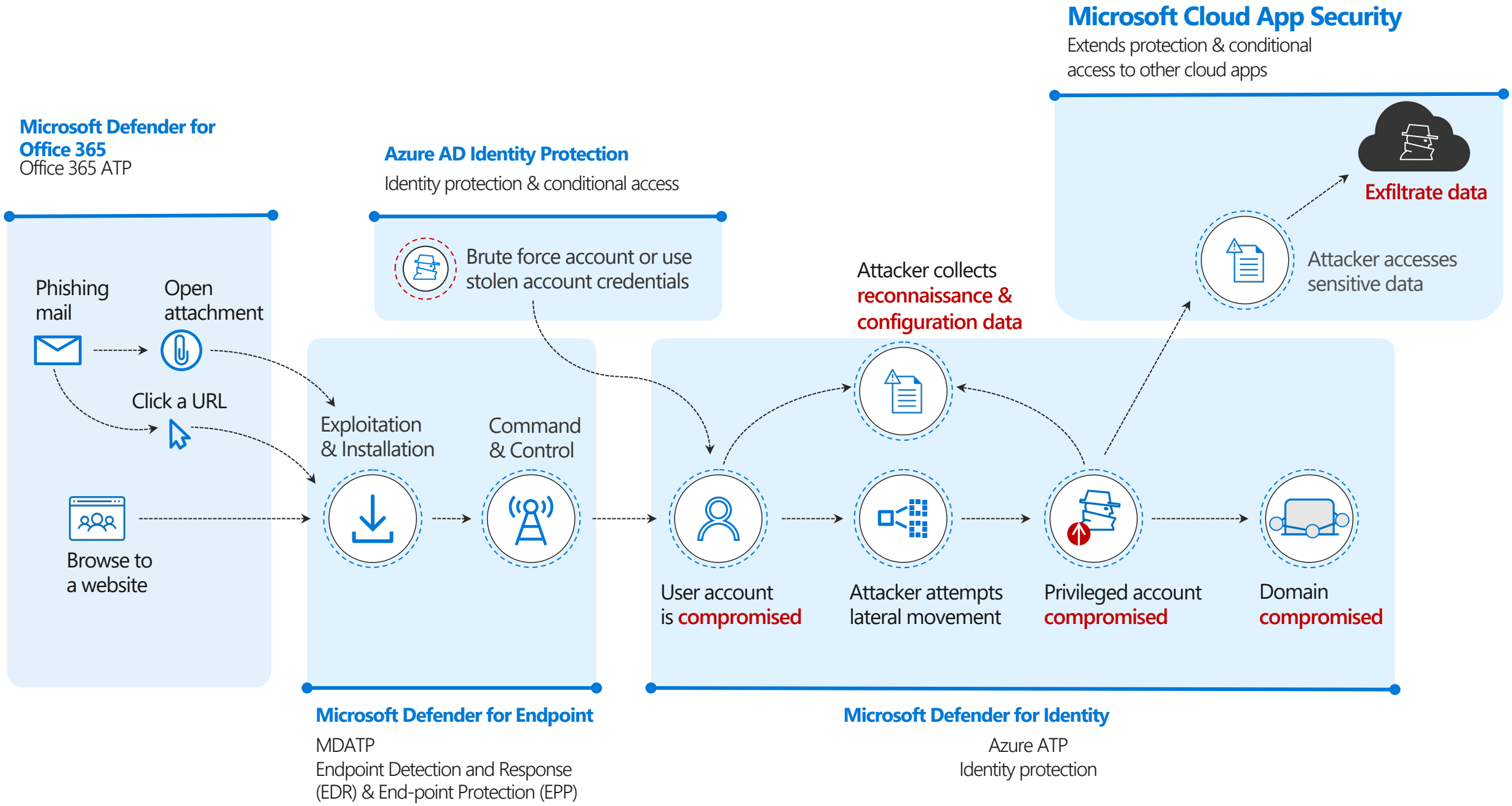
Pourquoi est-ce difficile?




Attacker
Polly's mailbox
+48hr
Mike's computer
Tracie's mailbox
Polly's computer
Polly's account
Adrian's account (IT helpdesk)
Mike's account (Exchange admin)
Exchange Web Services
Incident 1
Initial access
Alert
1. Spear-phishing email with link
Incident 2
Code execution
Event
2. Polly clicks link
Alert
3. Weaponized document downloads
Alert
4. Mimikatz runs
Incident 3
Credential theft, privilege escalation, recon, lateral movement
Event
5. Adrian's credentials stolen using Mimikatz
Event
8. Adrian's privileged account is compromised
Event
10. Pass-the-ticket: Mike's Exchange admin account compromised
Alert
6. Recon for admin accounts and machines
Alert
9. Lateral movement to Mike's computer
Event
7. Overpass-the-hash
Incident 4
Data exfiltration
Alert
11. Forwarding rule created in Tracie's mailbox
Alert
12. Tracie's emails exfiltrated

Security Solutions part of a Microsoft Platform




Microsoft Cloud App Security
Extends protection & conditional access to other cloud apps
Exfiltrate data
Attacker accesses sensitive data
Microsoft Defender for Office 365
Office 365 ATP
Azure AD Identity Protection
Identity protection & conditional access
Brute force account or use stolen account credentials
Attacker collects reconnaissance & configuration data
Phishing mail
Open attachment
Click a URL
Browse to a website
Exploitation & Installation
Command & Control
User account is compromised
Attacker attempts lateral movement
Privileged account compromised
Domain compromised
Microsoft Defender for Endpoint
MDATP
Endpoint Detection and Response (EDR) & End-point Protection (EPP)
Microsoft Defender for Identity
Azure ATP
Identity protection

SIEM

Azure Sentinel

Cloud native, any data, any entity

Multi-cloud

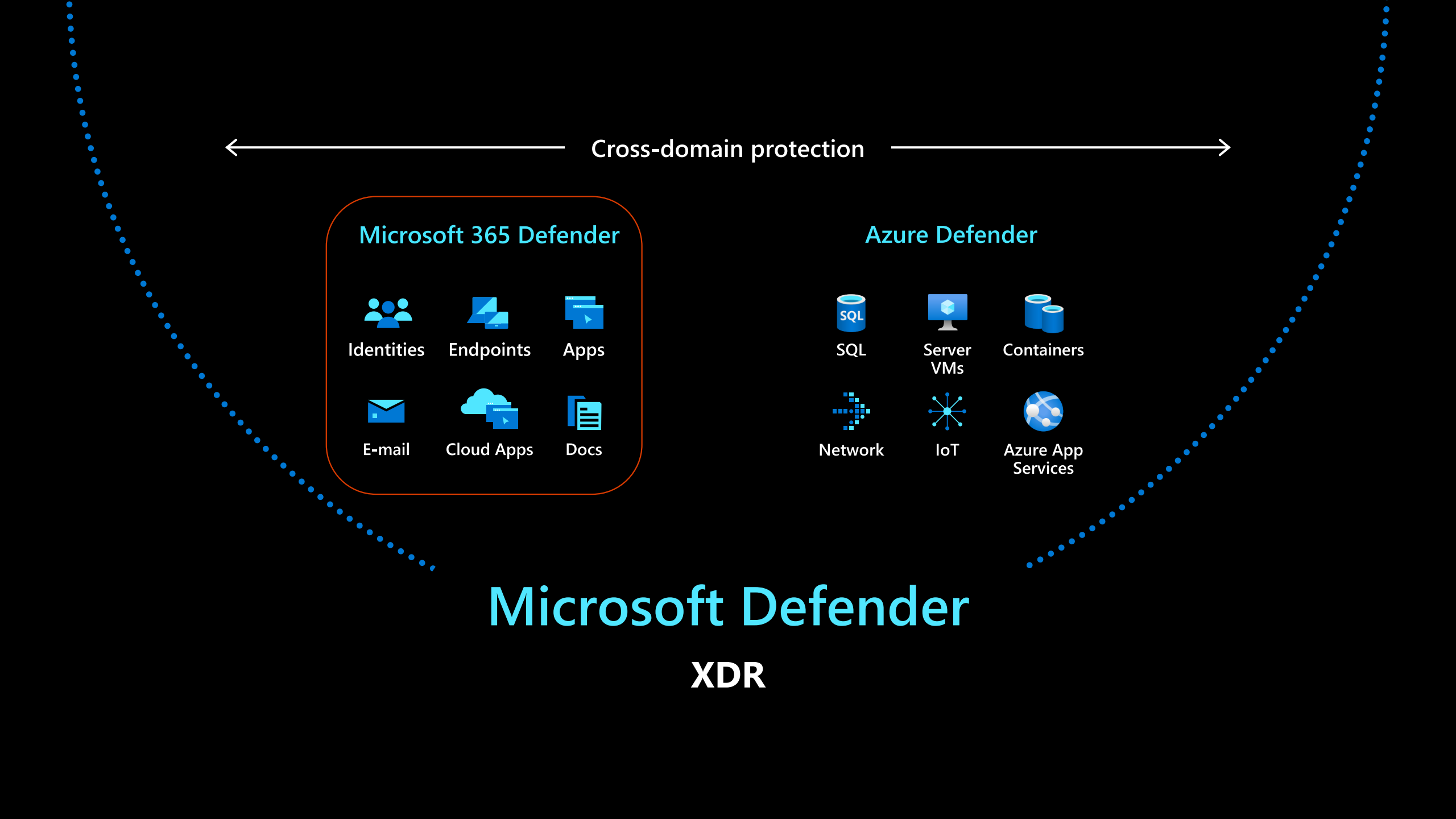
Partnerships

Cloud native

Any data

AI

Automation


Cross-domain protection
Microsoft 365 Defender
Identities
Endpoints
Apps
E-mail
Cloud Apps
Docs
Azure Defender
SQL
Server VMs
Containers
Network
IoT
Azure App Services
Microsoft Defender
XDR

Nous parlerons de...

How Microsoft 365 Defender improves the SOC's efficiency

with one best-of-breed, deeply integrated, full protection stack

>70% prévention des menaces pour l'organisation

>80% de réduction des alertes dans la file d'attente SOC

>75% d'éléments de travail résolus avec l'automatisation

L’efficacité SOC est plus importante que jamais

*© 2019 Accenture
**Cybersecurity Ventures

Comment Microsoft Defender prend en charge un SOC efficace

50

Nombre moyen d'outils de sécurité pour une organisation de taille moyenne

Complexité, changement de contexte, plus de temps d'arrêt

Portail unique pour les outils Microsoft 365 Intégration approfondie des outils

67%

Augmentation des attaques au cours des 5 dernières années*

>10 000 alertes/jour - fatigue d'alerte >, temps d'arrêt

Incidents réduire la charge de travail et faciliter les enquêtes de bout en bout

3.5m

Estimation des emplois non pourvus dans le domaine de la cybersécurité dans le monde d'ici 2021**

Ressources et compétences insuffisantes

Automatisé **Auto-guérison**
Experts en menaces Microsoft

Microsoft 365 Defender

the integrated tool for an efficient SOC across the entire protection cycle

1,000 Encounters

↓

300 Alerts

Cross detection

↓

40 Incidents

MTE

↓

10 Incidents

Go hunt

Contextual TI & mitigations

Microsoft 365 Defender

Sécurité inter-domaines automatisée

Pour en savoir plus:
aka.ms/ms365d

Vérifiez votre admissibilité :
aka.ms/ms365d-eligibility

Essayez-le dès aujourd'hui :
security.microsoft.com