



Infinigate Microsoft

Securing the future together



May 2024
Wouter de Blank – GTM Cybersecurity 
Microsoft



The Security Landscape is Tumultuous

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

Russian SolarWinds hackers launch email attack on government agencies

Microsoft says group targeted more than 150 American and foreign organisations using USAid account

EDITORS' PICK | Feb 11, 2020, 10:41am EST | 7,753 views

Estee Lauder Database Exposed; Customer Data Not Involved

White-Hat-Hacker finden beim Spital Thun kritische Lücken

Von **Reto Vogt**, 14. März 2024 um 08:45

Auch beide Basel von Hackerangriff auf Software-Anbieter betroffen

TECH

Microsoft's big email hack: What happened, who did it, and why it matters

PUBLISHED TUE, MAR 9 2021 4:30 PM EST | UPDATED TUE, MAR 9 2021 8:12 PM EST

Daten der Stadt Baden von Hackern im Darknet veröffentlicht

FireEye, one of the world's largest security firms, discloses security breach

FireEye suspects it was the victim of a nation-state hacking group.

Auch beide Basel von Hackerangriff auf Software-Anbieter betroffen

Auch Stadt Luzern von Hackerangriff auf Software-Anbieter betroffen

Jedes neunte Ransomware-Opfer bezahlt Lösegeld

23 Millionen Cyber-Angriffe auf die Stadt Bern in einem Jahr

The State of Cybercrime: key developments

80-90%

of all successful ransomware compromises originate through unmanaged devices.

A return on **mitigation (ROM) framework** is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.

70%

of organizations encountering human-operated ransomware had fewer than 500 employees.



Human-operated ransomware attacks are up more than **200%**



Password based attacks spiked in **2023**



Last year marked a **significant shift** in cybercriminal tactics

With threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is out best defense, due to the scale needed to mitigate the largest attacks

Organizations today face an industrialized attacker economy

Ransomware Kits
\$66 upfront (or 30% of the profit / affiliate model)

Stolen Passwords
\$0.97 per 1,000 (average)
(Bulk: \$150 for 400M)

Denial of Service
\$766.67 per month

Compromised PCs / Devices
PC: \$0.13 to \$0.89
Mobile: \$0.82 to \$2.78

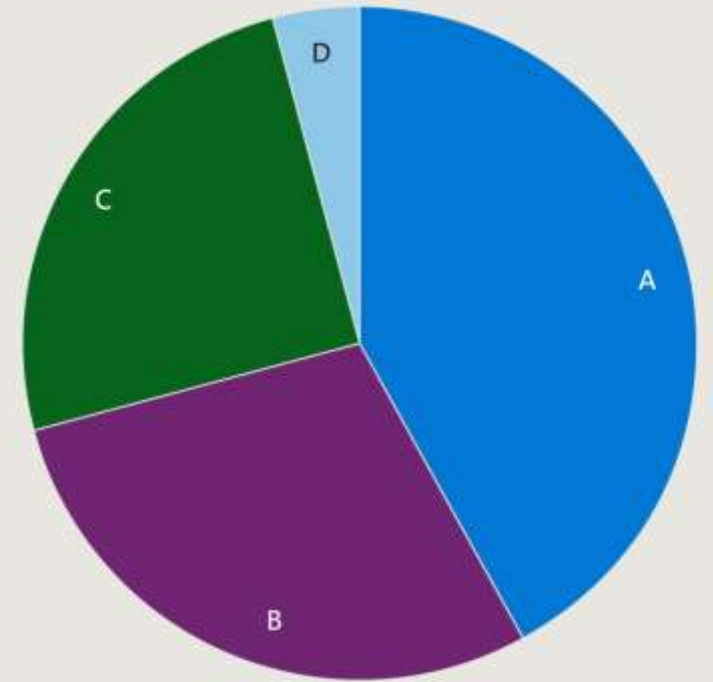
Spearphishing for hire
\$100 to \$1,000 (per successful account takeover)

Attacker for hire (per job)
\$250 per job (and up)


What we're seeing in attack notifications

- > Successful identity attacks
- > Ransomware encounters
- > Targeted phishing attempts leading to device or user compromise
- > Business email compromise

Distribution of top four attack progression notifications



Telemetry sources: Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, Azure AD Identity Protection, Microsoft Defender Threat Intelligence




Hello finance,
Your password for finance@victimdomain.com expires today
11/09/2023, 21:35:15 AM

You can change your password or keep the current one by
using the link below

[Keep Current Password](#)

Please note: this link expires in 24 hours. Please review
security requirements within 24 hours to avoid interruption.

Microsoft. All rights reserved. (c) 2023




Hello finance,
Your password for finance@victimdomain.com expires today
11/09/2023, 21:35:15 AM

You can change your password or keep the current one by
using the link below

[Keep Current Password](#)

Please note: this link expires in 24 hours. Please review
security requirements within 24 hours to avoid interruption.

Microsoft. All rights reserved. (c) 2023



Hello finance,
Your password for finance@victimdomain.com expires today
11/09/2023, 21:35:15 AM

You can change your password or keep the current one by
using the link below

[Keep Current Password](#)

Please note: this link expires in 24 hours. Please review
security requirements within 24 hours to avoid interruption.

Microsoft. All rights reserved. (c) 2023

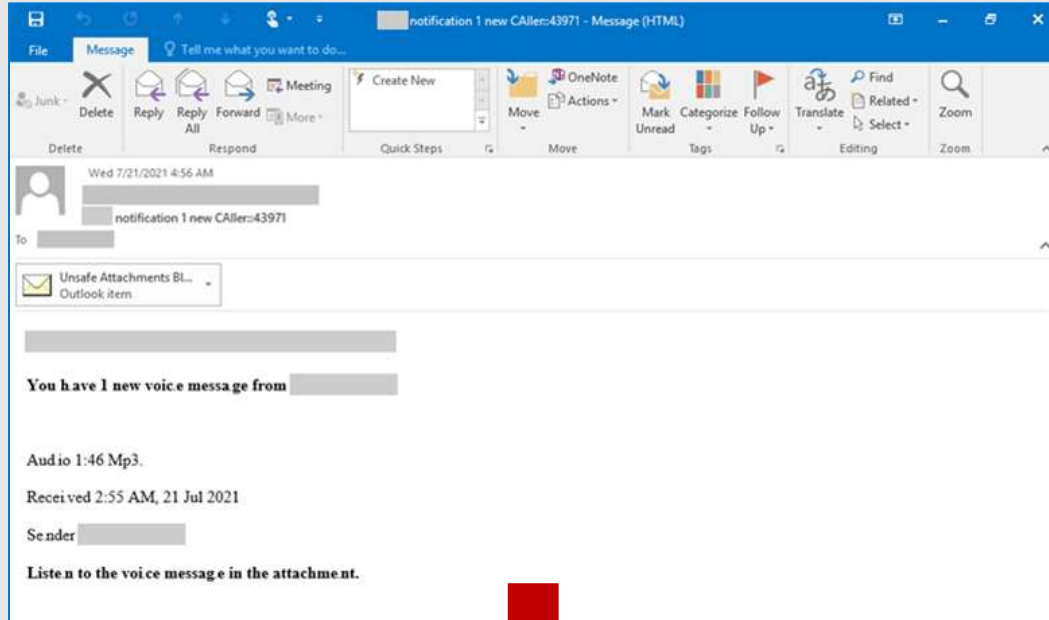
Increasing complexity to detect



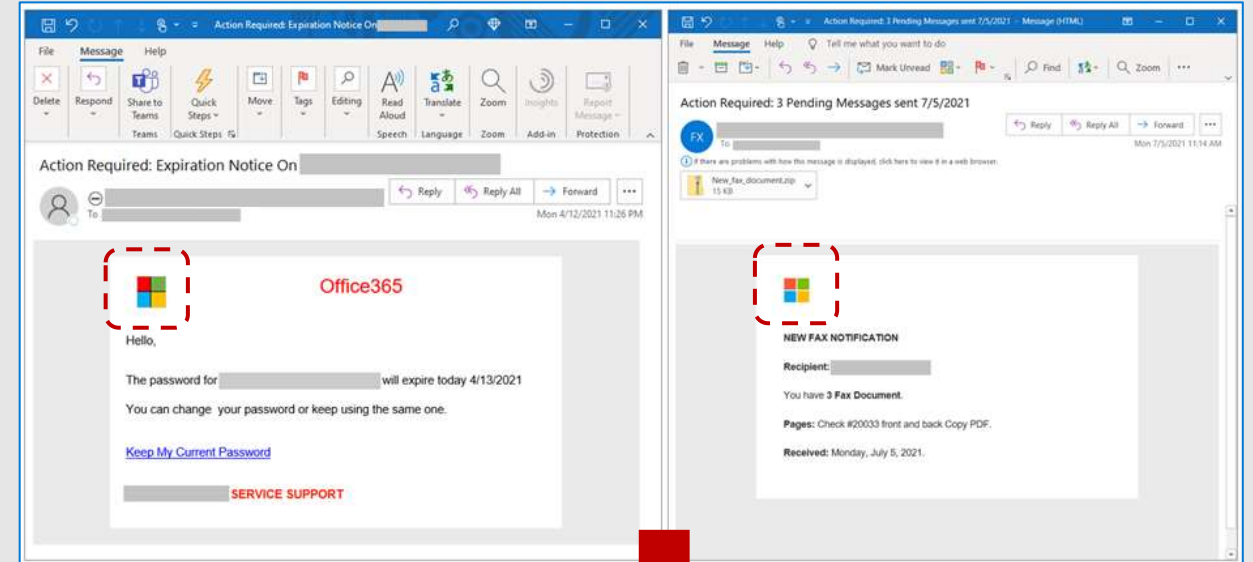
How modern phishing emails hide in plain sight

Hidden, zero-width letters added to break up keywords that might otherwise have been caught by a basic content filter.

Attackers using HTML tables to imitate the logos and branding of trusted organizations.

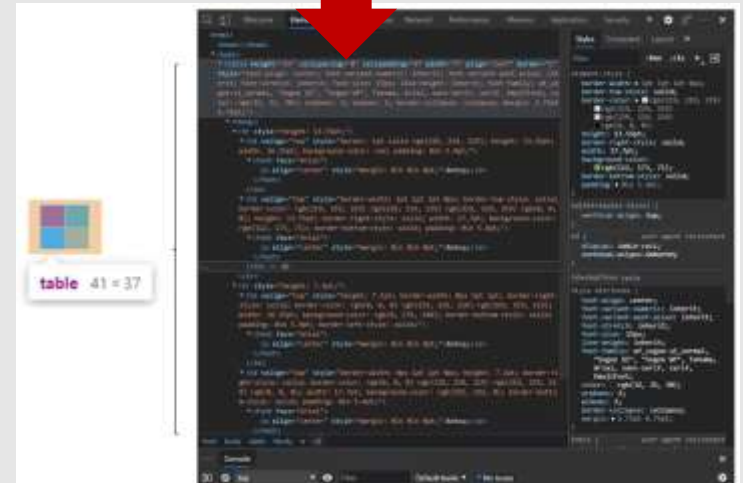


```
<html> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8"> </head>
<body>
[redacted]
<p><b>You hspan
spanave 1 new voicspan
spane messaspan
spange from [redacted].</b></p> &nbsp;
<p>Audspanio 1:46 Mp3.</p> <p>Receispan
spanved 2:55 AM, 21 Jul 2021</p> <p>Sespan
spannder [redacted]</p> <p><b>Listespan
spann to the voispan
spance messagspan
spane in the attachmespan
spannt.</b></p> </div> </body> </html>
```



Color Value

| |
|-----------------|
| Red |
| rgb(112,173,71) |
| rgb(0,176,240) |
| #ffc000 |



Attackers morph the way they reference the colour, or slightly changing the colour values to try and evade detection.

How can we protect against 99% of attacks?

99%

Basic security hygiene still protects against 99% of attacks.

How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.*



Enable multifactor authentication (MFA)



Apply Zero Trust principles



Use extended detection and response (XDR) and antimalware



Keep up to date



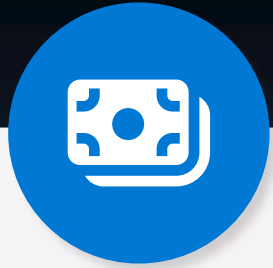
Protect data

Outlier attacks on the bell curve make up just 1%



“Security is our top priority and we are committed to working with others across the industry to protect our customers.”

Satya Nadella, Chief Executive Officer, Microsoft Corporation



\$20B+
in revenue



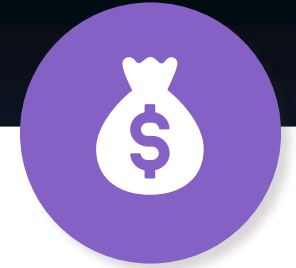
1M
customers



120
countries



Continuous
innovation



\$20B
of investment
commitment

Three key lessons

Innovation



We need to use the latest innovations, such as AI, to supercharge our cyber defense.

Partnerships



We need to work together with all stakeholders – be they public or private.

Skills



According to LinkedIn data, EU cyber skills demand is up by 22%. A clear skills gap is here.

Governments, Corporations and Citizens are asking for 4 things....

1

Help us be more secure

Assessing your current security landscape, reviewing architecture and capabilities to recommend future state solutions

2

Lower our TCO

3

A safe and rapid migration

4

Ongoing proof of value

**Governments,
Corporations
and Citizens are
asking for
4 things....**

1

Help us be more secure

Assessing your current security landscape, reviewing architecture and capabilities to recommend future state solutions

2

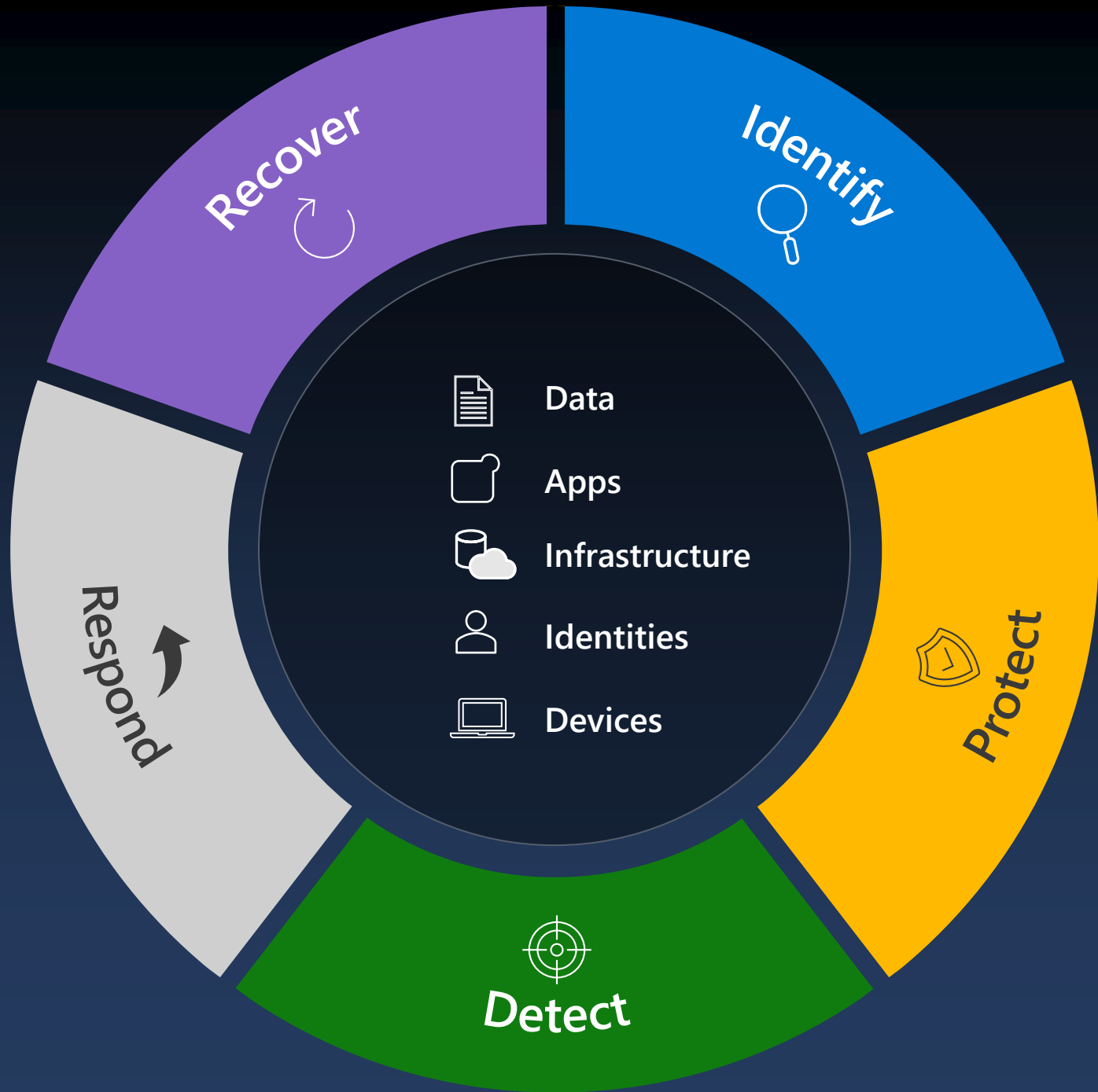
Lower our TCO

3

A safe and rapid migration

4

Ongoing proof of value



The Microsoft advantage



Large-scale data
and threat intelligence

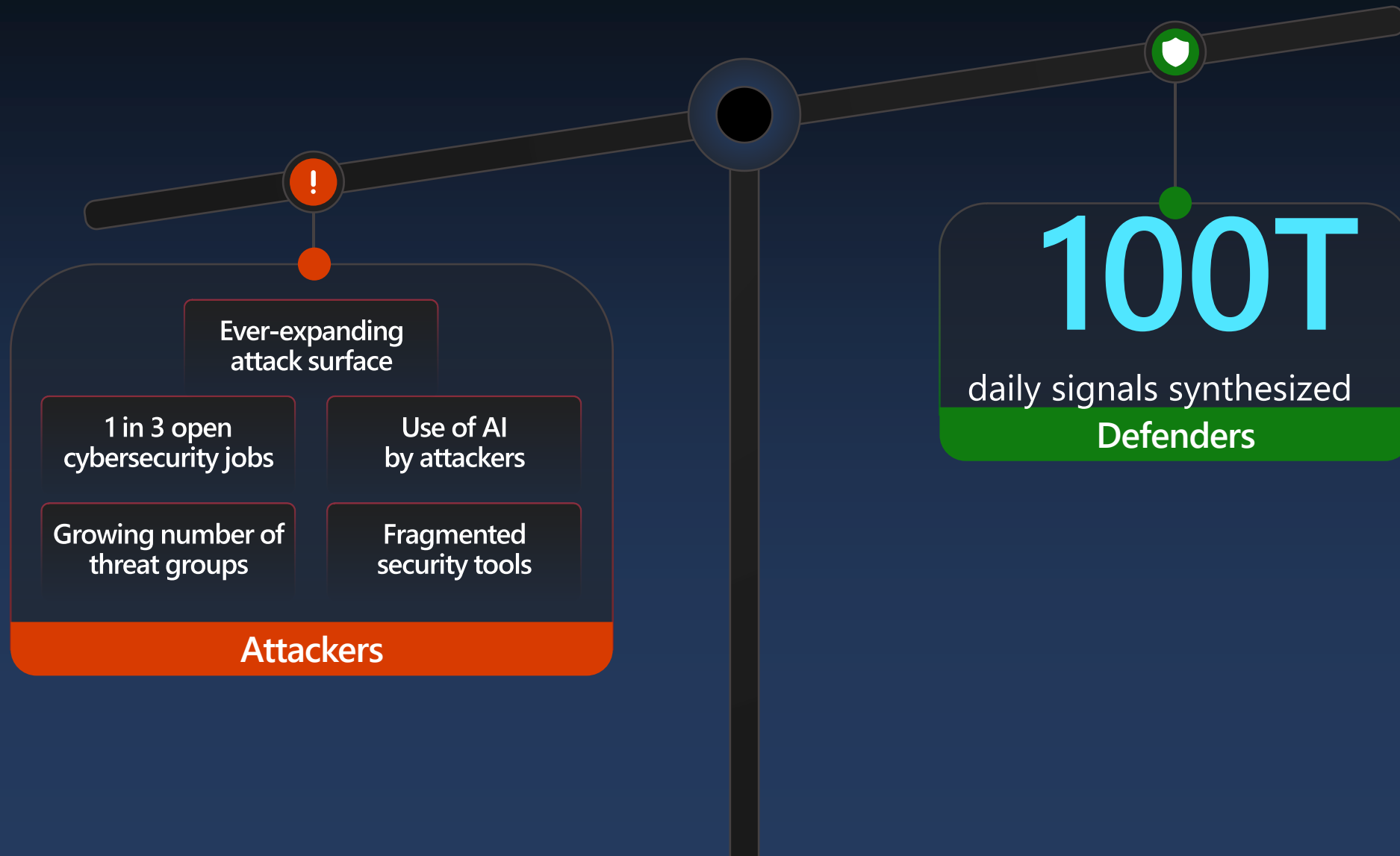


Most complete, integrated,
end-to-end protection

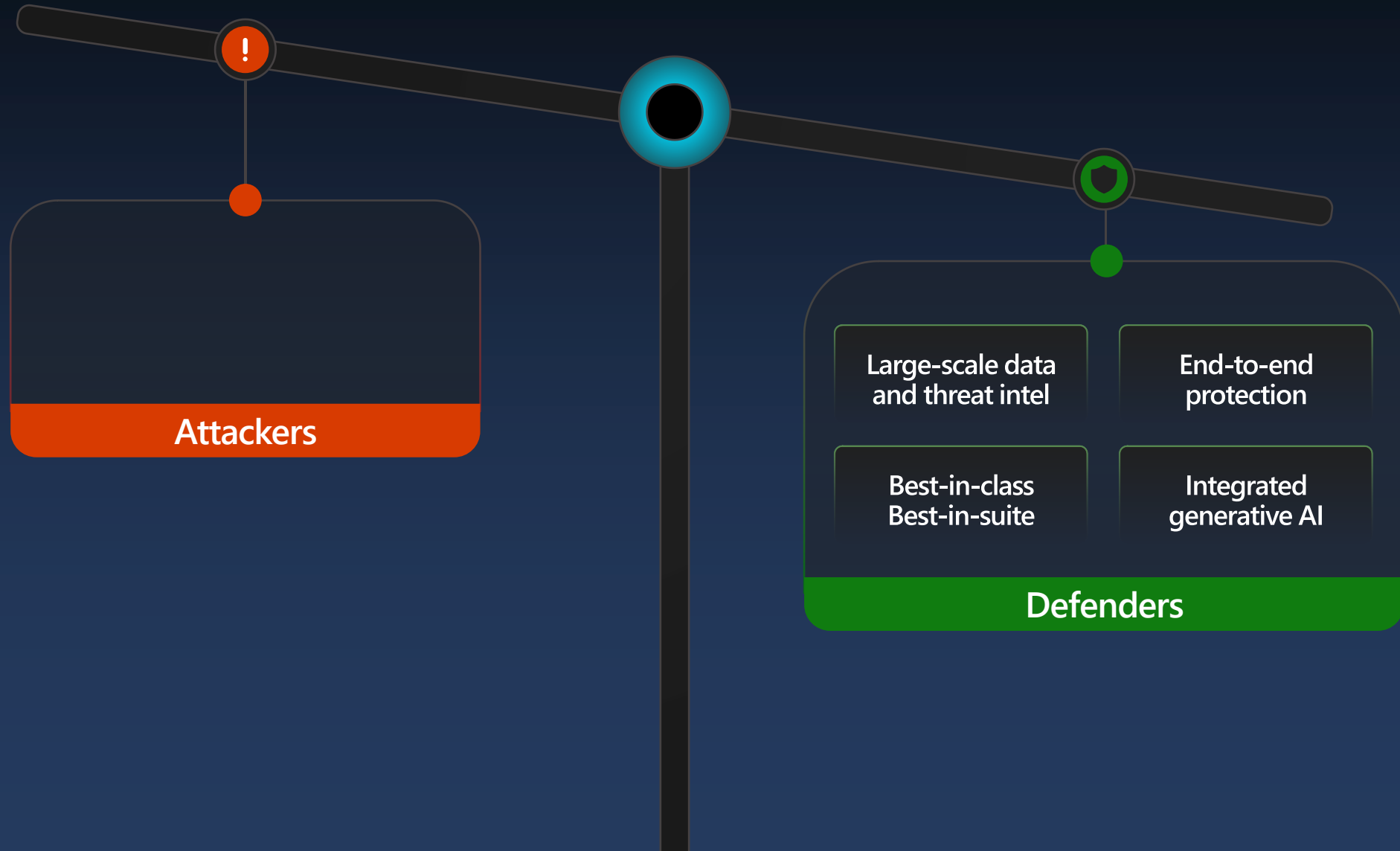


Industry-leading
responsible and secure AI

Attackers have an asymmetric advantage



Microsoft tips the scale in favor of defenders



**Governments,
Corporations
and Citizens are
asking for
4 things....**

1

Help us be more secure

Assessing your current security landscape, reviewing architecture and capabilities to recommend future state solutions

2

Lower our TCO

3

A safe and rapid migration

4

Ongoing proof of value

Simplify Vendor Management

Consolidate security with Microsoft's cost-effective solution

Replace up to

50 Products Categories

\$0 built in Cloud Security Posture Management with Microsoft Defender for Cloud

Up to **62%** savings with Microsoft 365 E5 Security and Microsoft 365 E5 Compliance¹

Savings on Automation & Process Improvements

Safeguard your multi-cloud resources and provide your organization with secure access for a connected world

reduced risk of material breach **60%**

less time to investigate threats **65%**

less time responding to threats with Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender for Cloud¹ **88%**

reduction in noise, elevating the most critical issues with Microsoft Sentinel⁴ **90%**

less time spent monitoring potential suspicious activity with Microsoft Purview³ **96%**

million additional end user productivity from automation and process improvements in Microsoft 365 Defender² **\$10.5**

**Governments,
Corporations
and Citizens are
asking for
4 things....**

1

Help us be more secure

Assessing your current security landscape, reviewing architecture and capabilities to recommend future state solutions

2

Lower our TCO

3

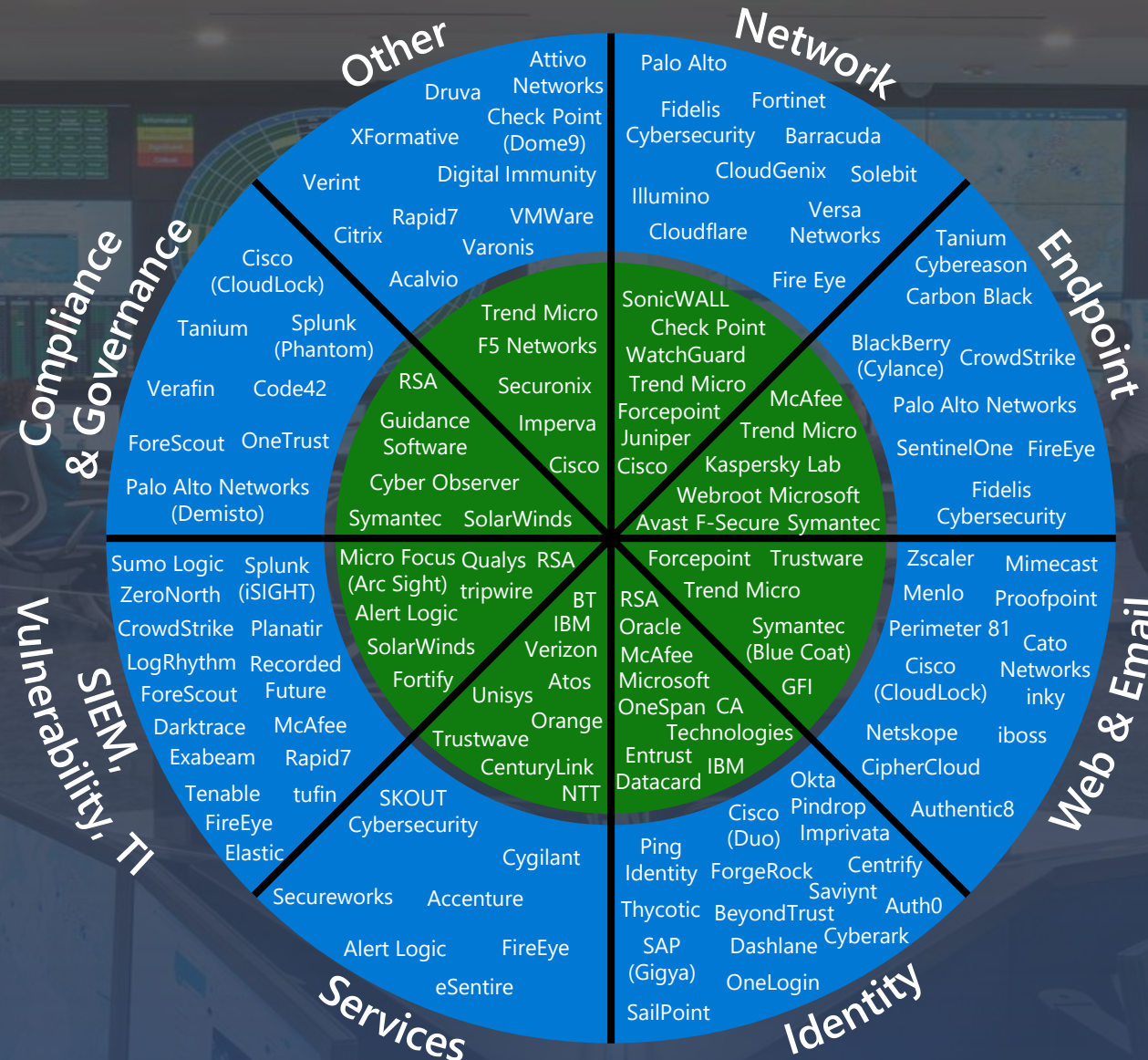
A safe and rapid migration

4

Ongoing proof of value

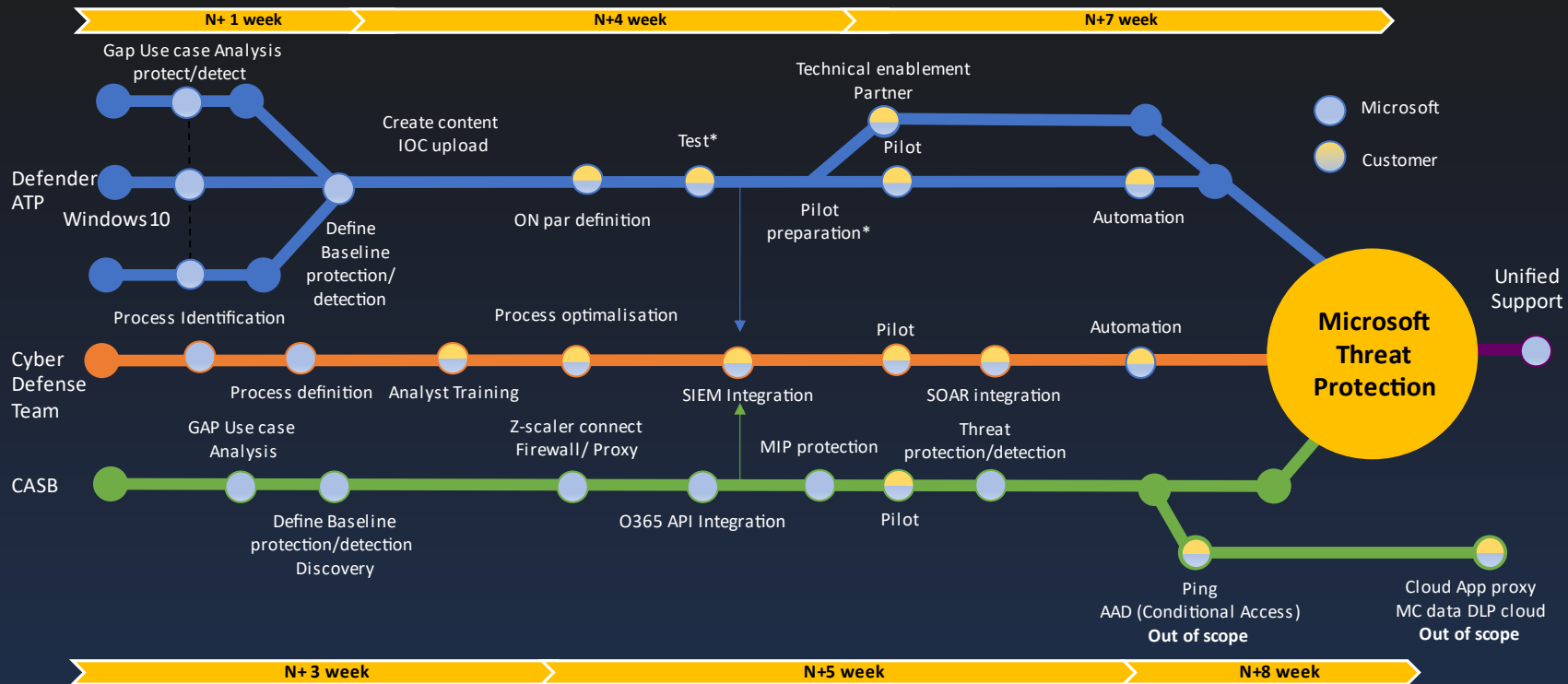
Current state

...how customers solve it today



Next-Gen Technology Companies

Legacy Technology Companies



Current state

Future state

| | |
|-------------------|---------------------|
| Skilled Resources | MSFT/ MSFT Programs |
| | Customers |
| | Partners |

Governments, Corporations and Citizens are asking for 4 things....

1

Help us be more secure

Assessing your current security landscape, reviewing architecture and capabilities to recommend future state solutions

2

Lower our TCO

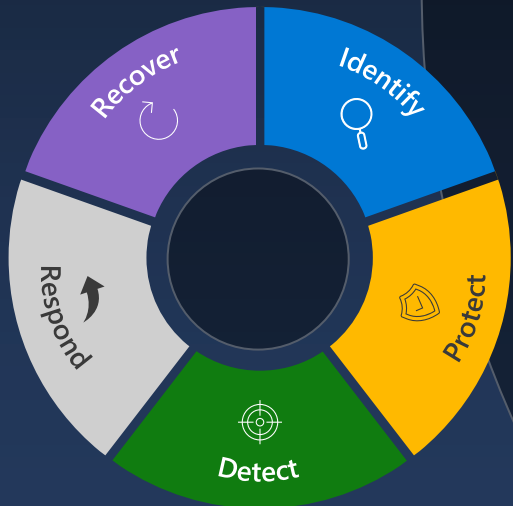
3

A safe and rapid migration

4

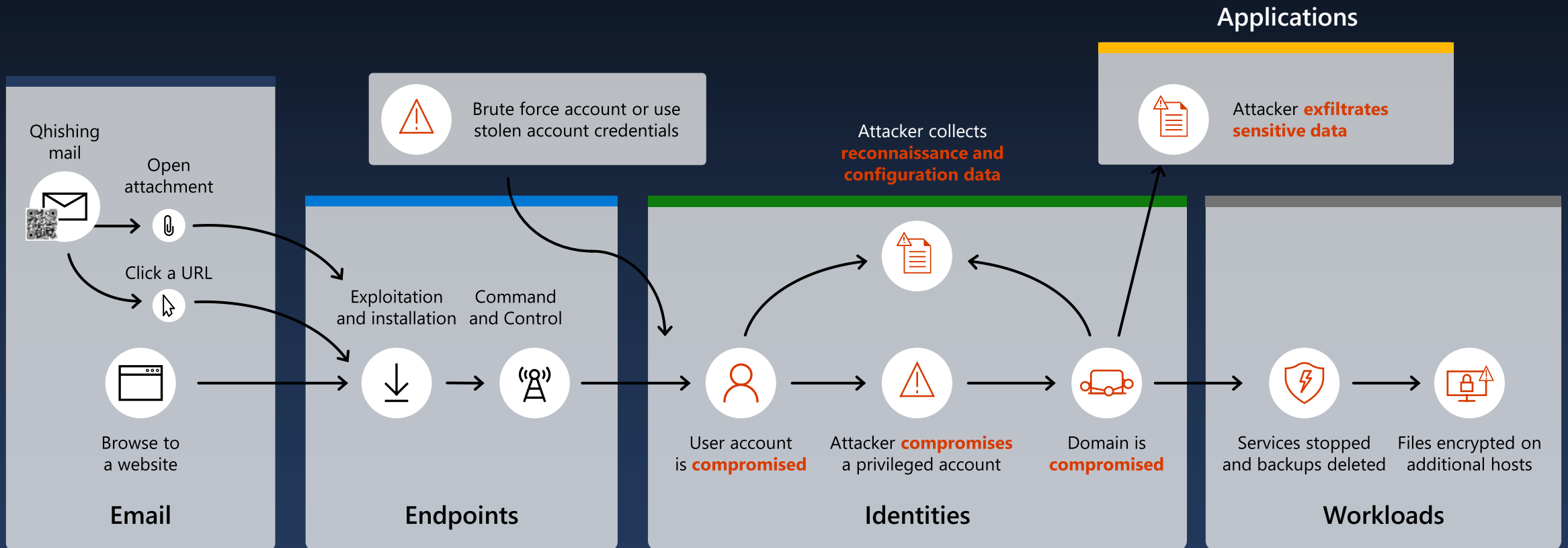
Ongoing proof of value

Customers need to find, catalog and secure data, apps, identities, users and devices



Simple Mistakes Open Doors

Typical human-operated ransomware campaign



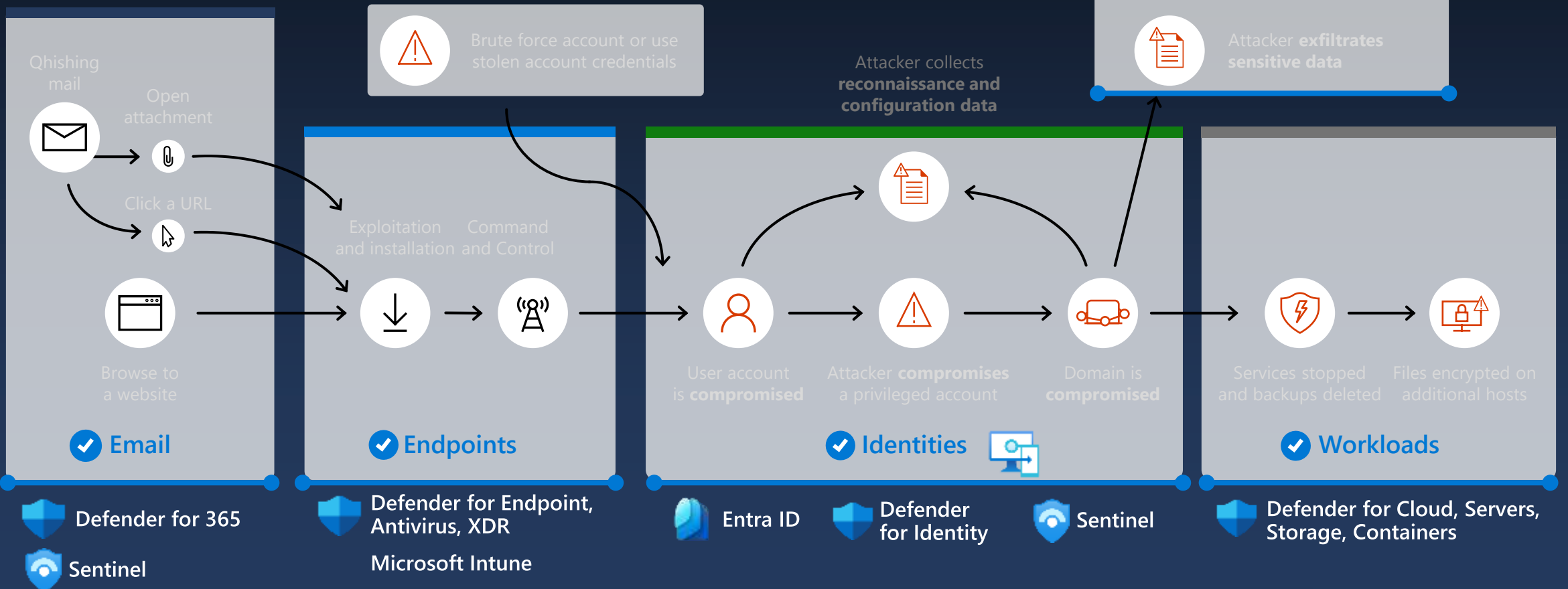
Protection across the entire kill chain

With Microsoft SIEM and XDR

 Defender for Cloud, Cloud Apps, Defender External Attack Surface

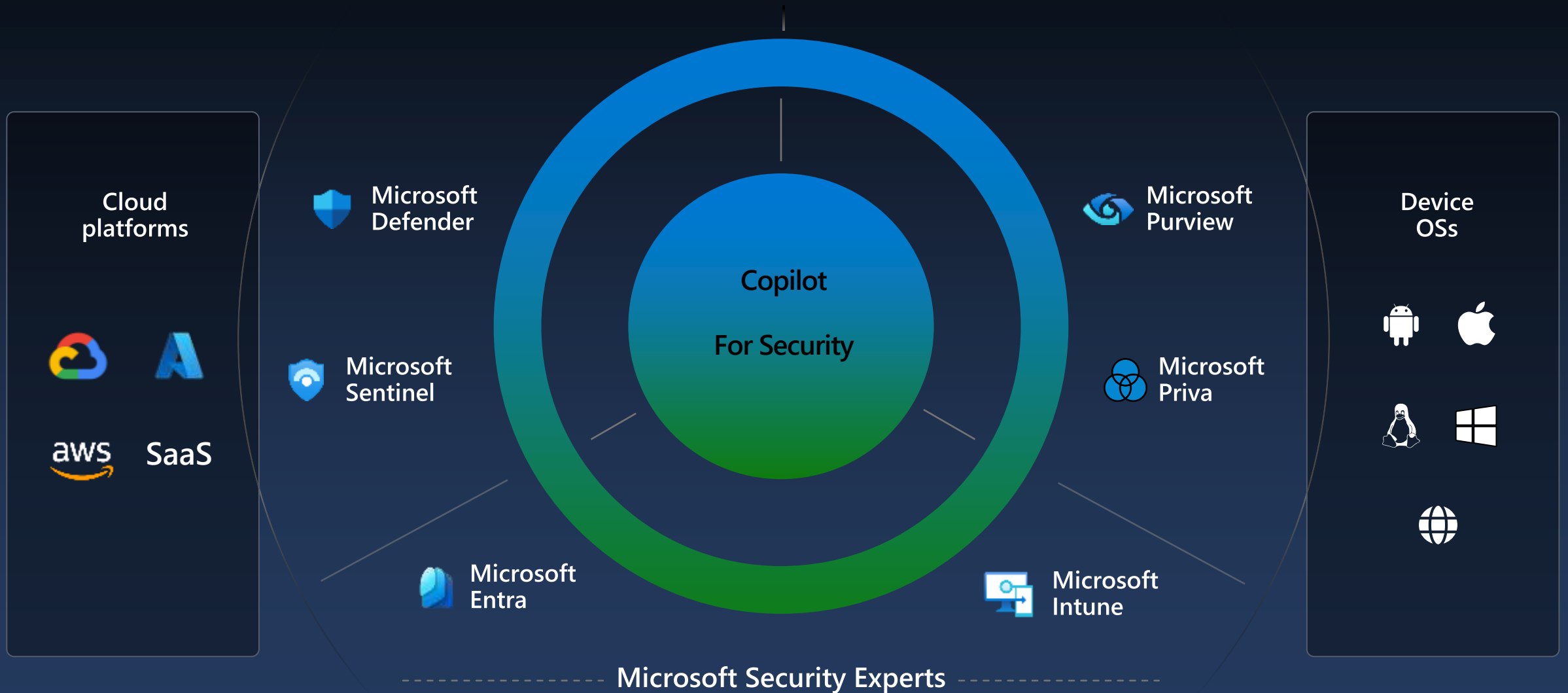
 Entra Permissions Management

 Applications



Uncover the attack end to end and take action to completely evict the attacker.

We lead with end-to-end protection





Thank You