Microsoft Security

Microsoft Security for SMB

Comprehensive security in the age of AI

Martin Janisch
23 05 2024

The New York Times

Once, Superpower Summits Were About Nukes. Now, It's Cyberweapons.

But with the ease of denying responsibility and the wide range of possible attackers, the traditional deterrents of the nuclear age no longer work.

POLITICO

CYBERSECURITY

Chinese hackers nab 60,000 emails in State Department breach

Among the most sensitive information stolen, the staffer said, were victims' travel itineraries and diplomatic deliberations.

The New York Times

In Cyberattacks, Iran Shows Signs of Improved Hacking Capabilities

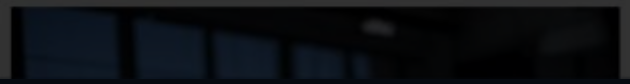
A monthslong hacking campaign targeted the governments of regional rivals, including Israel, and marked a turn, a new report says, as the attacks were used to collect intelligence, not just disrupt services.

The Washington Post

TECH POLICY

Cybersecurity faces a challenge from artificial intelligen

While defenders
progress



CYBERCRIME MAGAZINE

Cybercrime To Cost the World $10.5 Trillion Annually by 2025

If it were measured as a country, then cybercrime – which is predicated to inflict dames totaling $6 trillion USD globally in 2021 – would be the world's third largest economy after the U.S. and China.

THE WALL STREET JOURNAL.

The Chinese groups accused of hacking

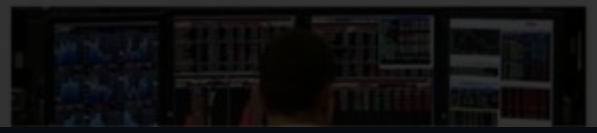
Security is a defining challenge of our time

FINANCIAL TIMES

Cyber Security

ECB tells banks to run cyber stress tests after rise in hacker attacks

Lenders will assess online resilience after 'significant increase' in incidents since outbreak of Ukraine war



The Washington Post

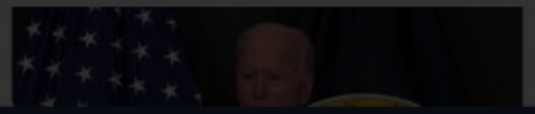
Think ransomware gangs won't thrive this year? Think again, experts say

Welcome to The Cybersecurity 202! And greetings from Qui

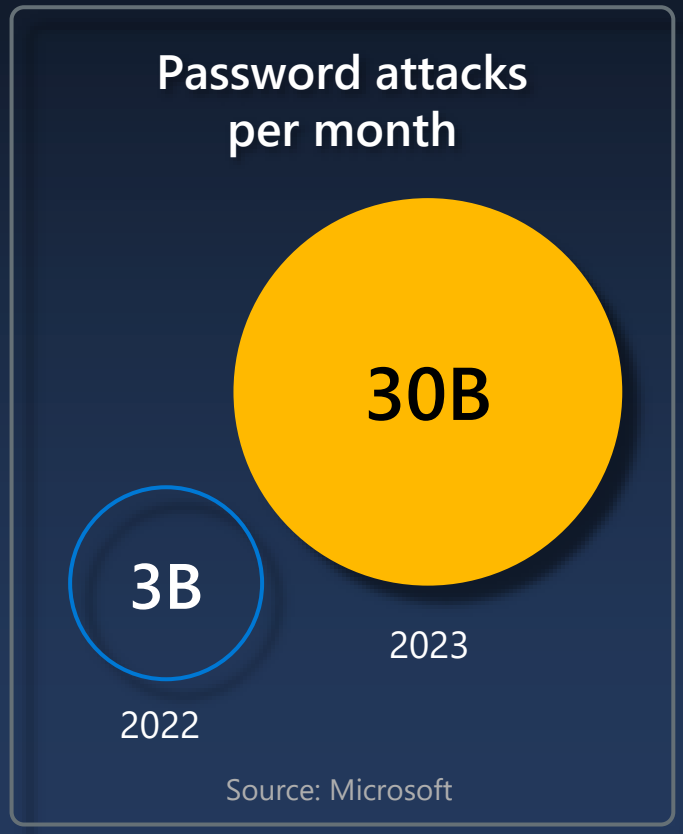
REUTERS

World

Biden: If U.S. has 'real shooting war' it could be result of cyber attacks



Sophistication, speed, and scale of cyber attacks are increasing



Operational complexity is also increasing

Organizations use an average of 80 security tools

Source: Microsoft

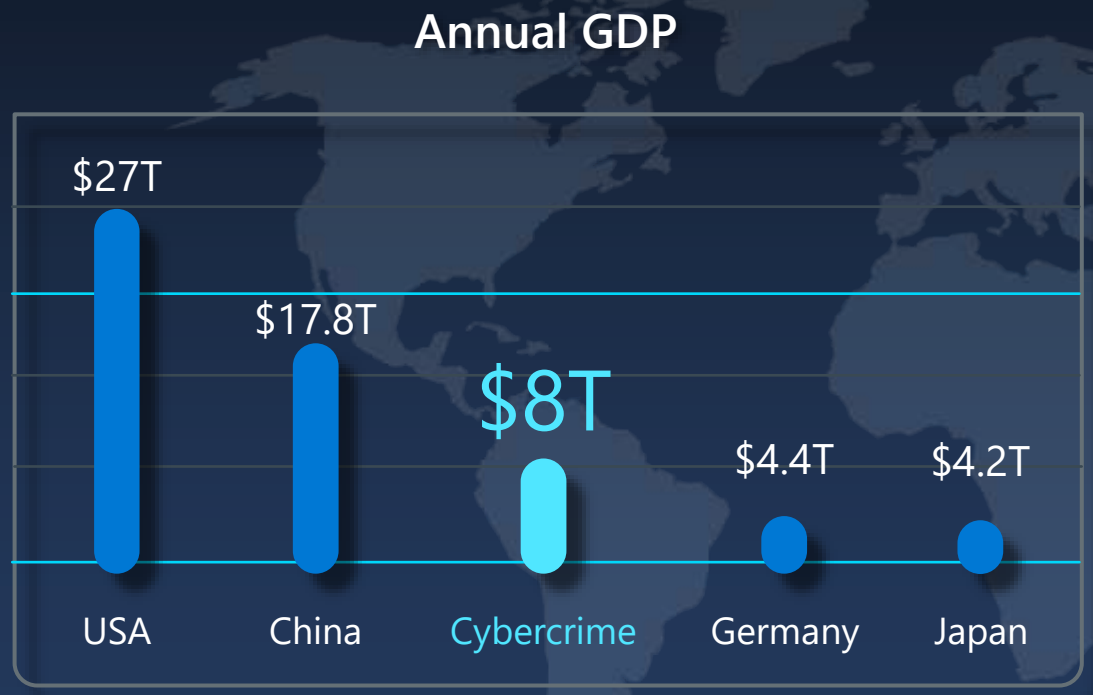
Open jobs worldwide

Source: (ISC)[2]

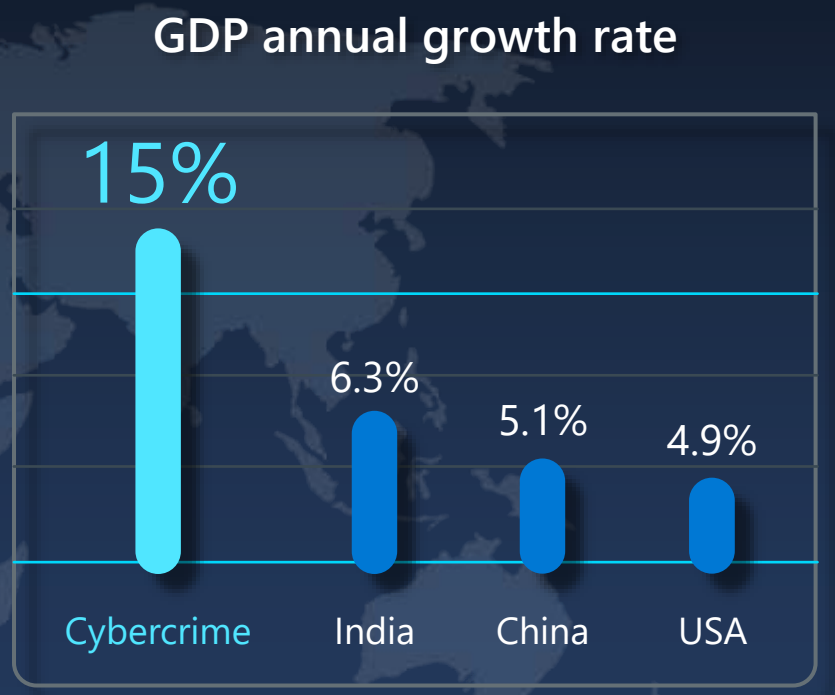
Business leaders concerned about data or IP loss due to improper use of AI

Source: IDC

Cybercrime today equals the 3rd largest economy in the world and growing fast

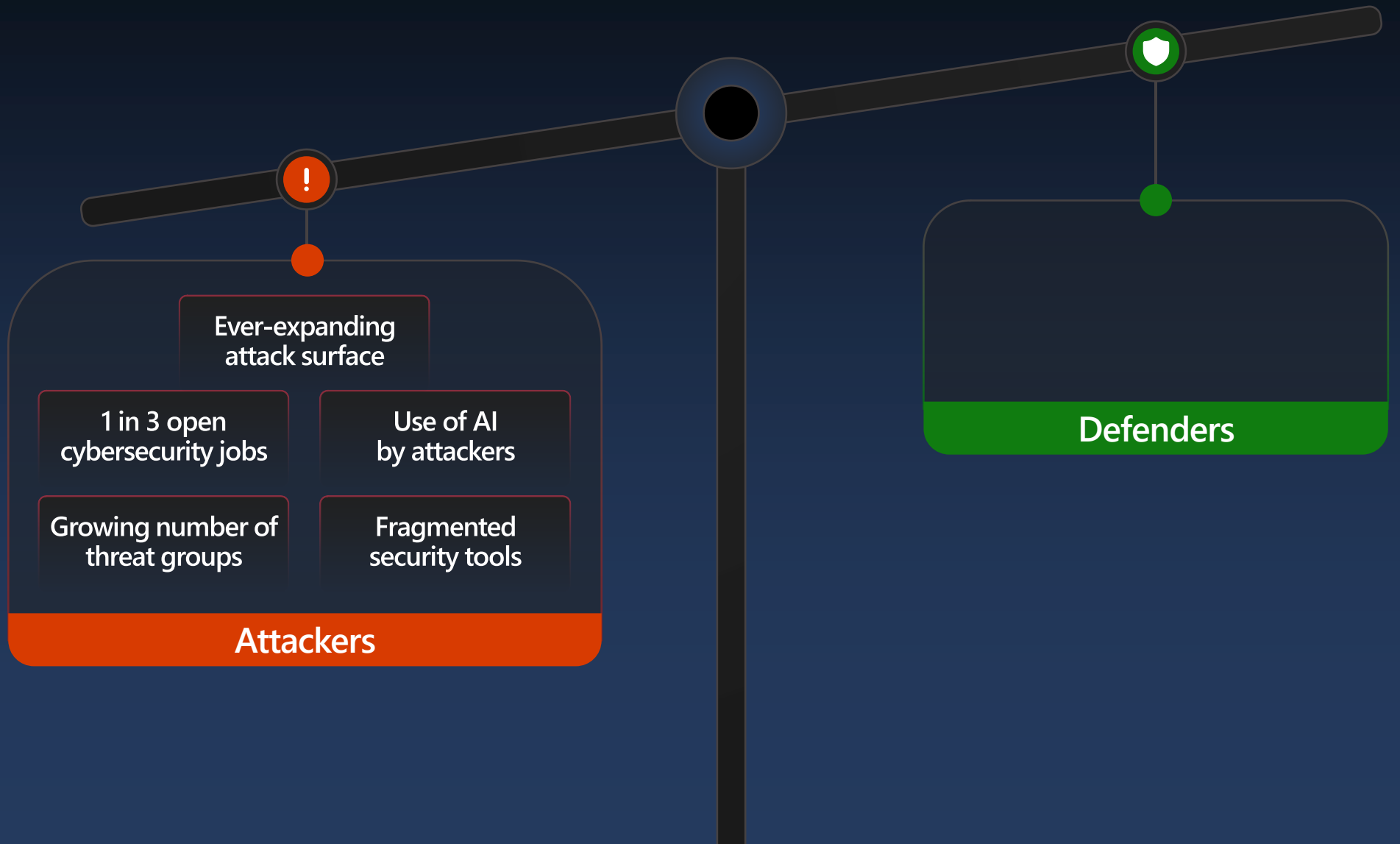


Source: Statistica



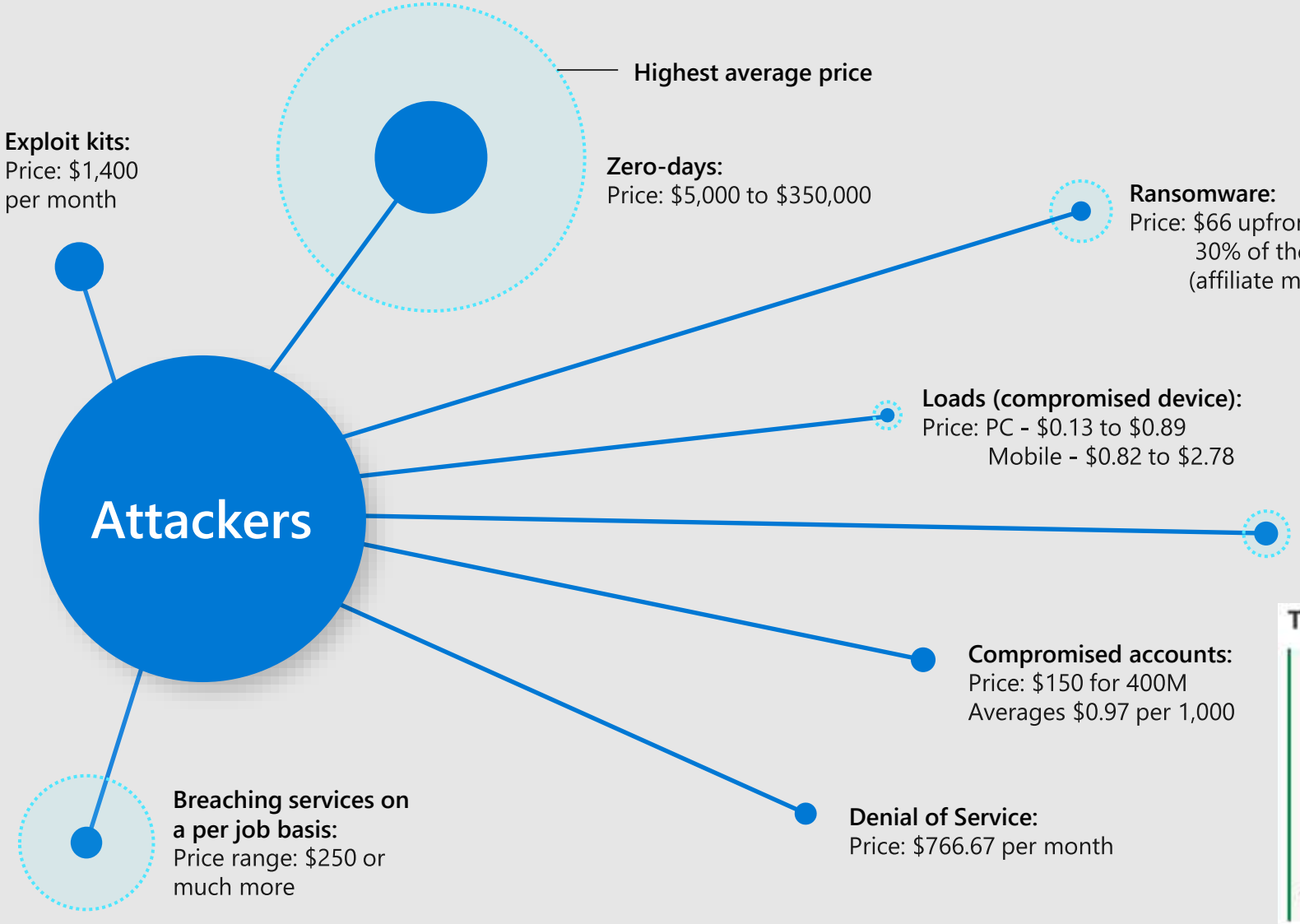
Source: Statistica

Attackers have an asymmetric advantage



Threat Actor Techniques and Costs

More details at https://aka.ms/CISOWorkshop



The top 10 most common passwords list in 2024:

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

Most Common Passwords 2024 - Is Yours on the List? | CyberNews, based on 15.212 B from publicly leaked data breaches; last accessed on May 22nd , 2024

The State of **Cybercrime**

Key developments

80-90%

of all successful ransomware compromises originate through unmanaged devices.

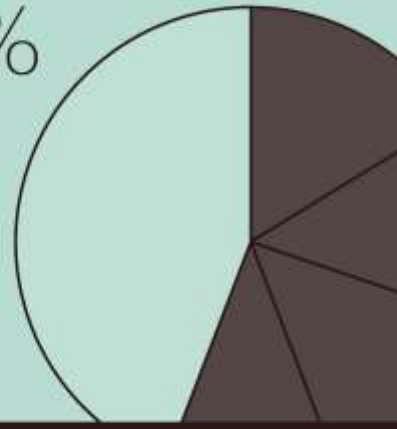
A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.

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

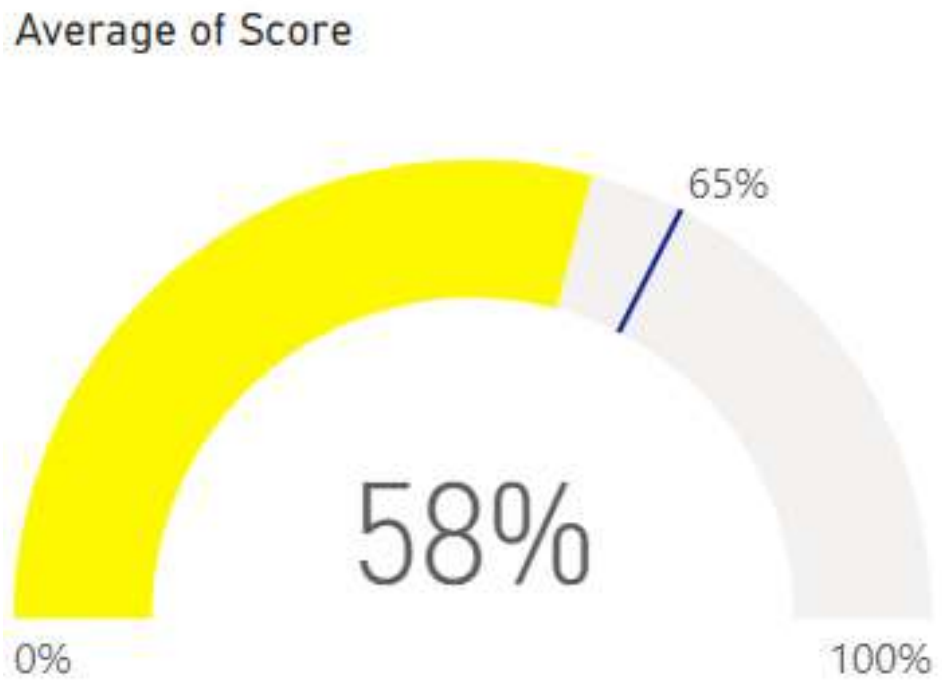
Last year marked a significant shift in cybercriminal tactics

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 our best defense, due to the scale needed to mitigate the largest attacks.

Source: Microsoft Digital Defense Report 2023 (MDDR)

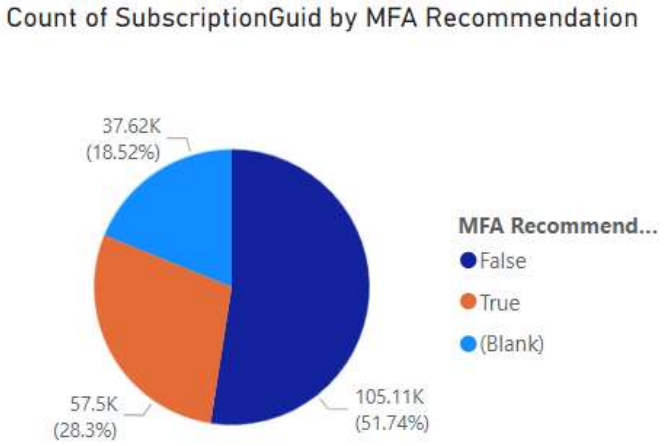
Local Quantitative Situation in Switzerland (Az Subs)

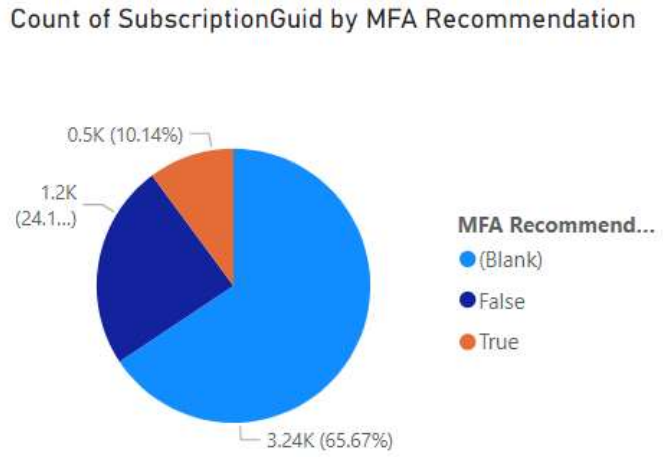
Secure Score



PartnerSubsidiary	Count of SubscriptionGuid
Switzerland	78498
Total	**78498**

PartnerSubsidiary	Count of SubscriptionGuid
Switzerland	4862
Total	**4862**





Automatic CA policies enforced by Microsoft

- [Automatic Conditional Access policies in Microsoft Entra streamline identity protection | Microsoft Security Blog]

- Those policies can be turned off after provisioning, but highly recommended to keep them!

Policy	Who it's for	What it does
Require multifactor authentication for admin portals	All customers	This policy covers privileged admin roles and requires multifactor authentication when an admin signs into a Microsoft admin portal.
Require multifactor authentication for per-user multifactor authentication users	Existing per-user multifactor authentication customers	This policy applies to users with per-user multifactor authentication and requires multifactor authentication for all cloud apps. It helps organizations transition to Conditional Access.
Require multifactor authentication for high-risk sign-ins	Microsoft Entra ID Premium Plan 2 customers	This policy covers all users and requires multifactor authentication and reauthentication during high-risk sign-ins.

Data and threat intelligence

Microsoft has more insight into attacker behaviors than anyone

100T+

Signals synthesized per day

10K

Security and threat intelligence experts

1M

Microsoft Security customers

15K

Partners

Integrating 50+ product categories

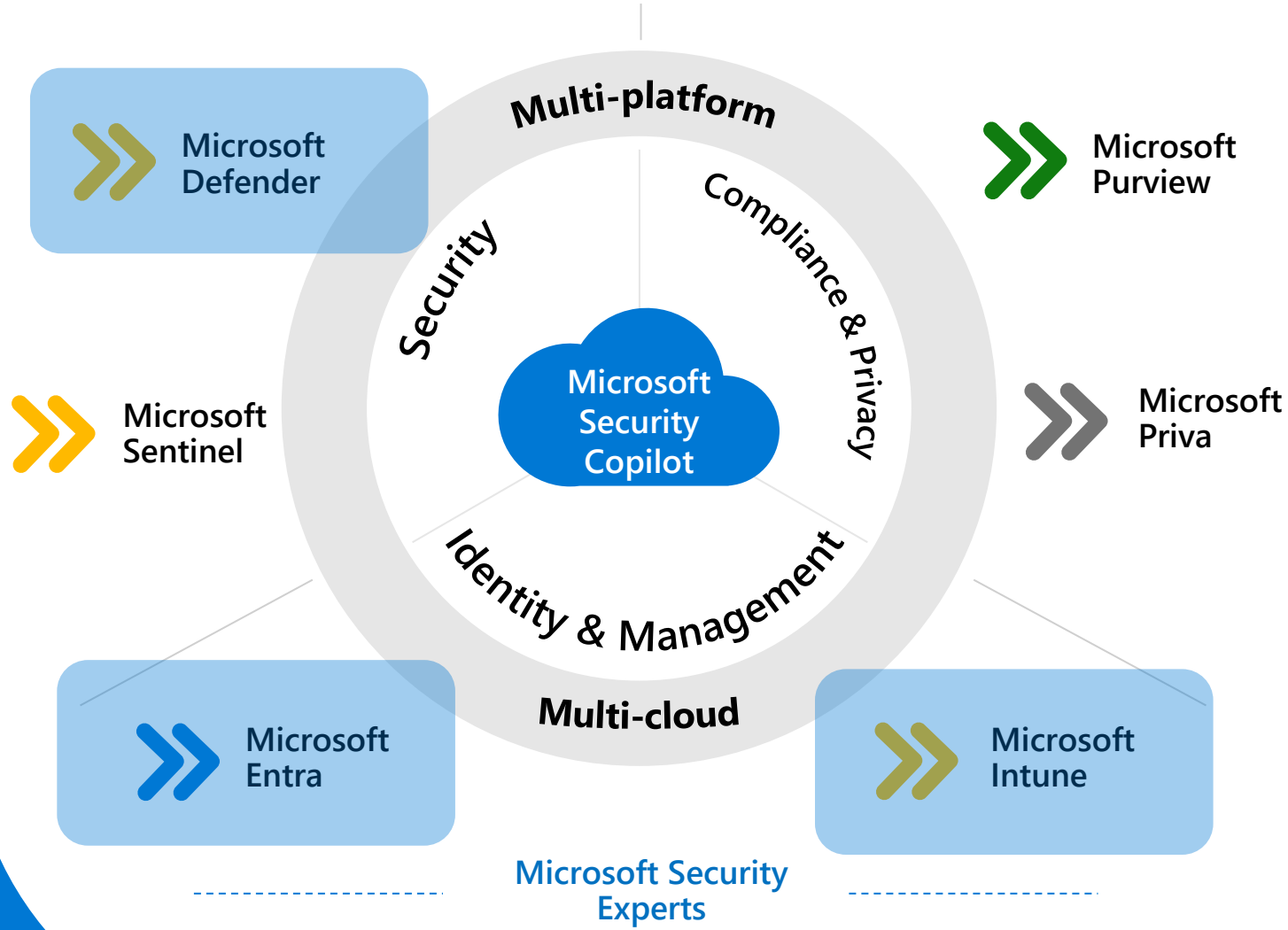
True end-to-end protection

Multicloud

Multiplatform

Portfolio overview

Six product families integrating over 50 product categories



KMU Hero Workloads

Entra ID Plan 1

Identity and access management across your digital landscape

- Risk-based adaptive policies
- Seamless experience for any user
- Unified identity management and access to any app
- Simpler identity and access lifecycle

Defender for Business

Stop threats across your entire organization

- Secure all clouds, all platforms
- Get leading integrated protection
- Deliver rapid, intelligent response

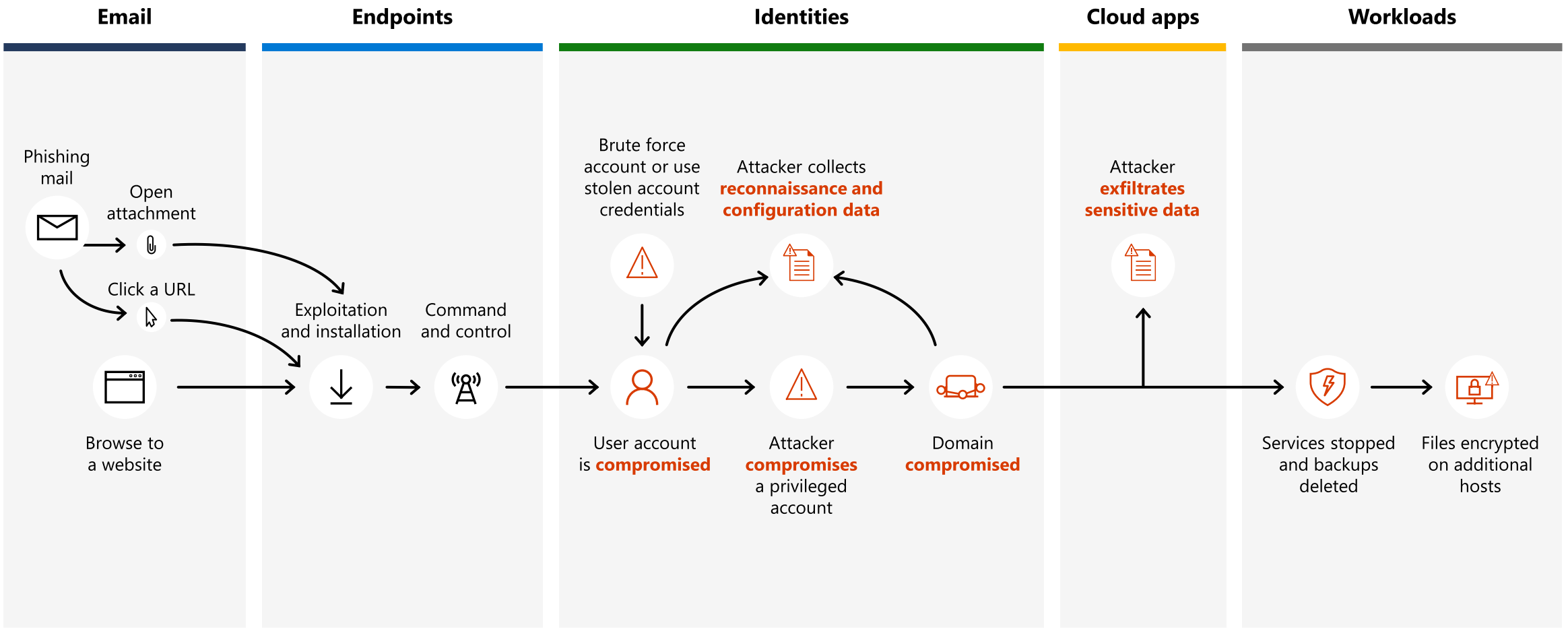
Intune Plan 1 for Business

State of the art MDM and MAM to secure endpoints

- Manage your identities even more granularly
- Manage devices and secure them
- App security, deployment and updates
- Self-Service and simplified user experience

Why is defense so difficult today?

Typical human-operated ransomware campaign



What is Microsoft 365 Business Premium

Securing each & every layer of productivity seamlessly

Microsoft 365 Business Premium

Identity Security

User

- Entra ID Features like MFA
- Self Service Password Reset
- Conditional Access

Device Security

Device

- Microsoft Defender AV
- Full Centralized Management of Mobile and Laptops with Intune
- Remote wipe of data of lost & stolen devices
- BitLocker Encryption
- Enforce Strong Pin requirements along with WiFi, VPN profiles

Application Security

Application

- Restrict copy/paste/save corp data to personal apps
- Accessing sensitive apps securely (Windows Virtual Desktop)

Email Security

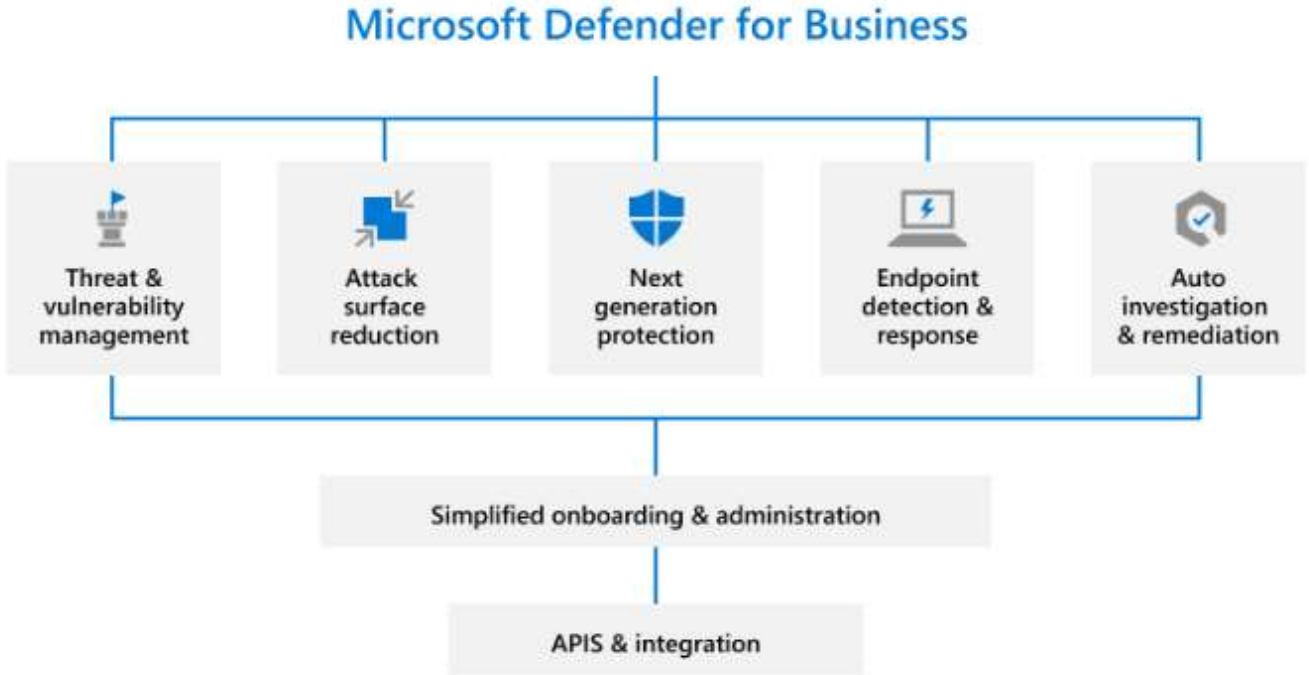
Email

- Advanced Threat Protection for protection against malware and zero day attacks
- Data Loss Prevention to monitor sensitive data from being transmitted
- Email restrictions like “Do Not Forward” or “Encrypt Email”

Document Security

Document

- Azure Information Protection protects, classifies Documents for secure sharing
- Revoke access to Documents
- Track Sensitive documents


Microsoft Defender for Business
Threat & vulnerability management
Attack surface reduction
Next generation protection
Endpoint detection & response
Auto investigation & remediation
Simplified onboarding & administration
APIS & integration


Microsoft Defender for Endpoint
Threats are no match.
Vulnerability management
Attack surface reduction
Next generation protection
Endpoint detection & response
Auto investigation & remediation
Microsoft Security Experts
Centralized configuration & administration
APIs & integration

Microsoft 365 Lighthouse with Defender for Business and Microsoft Business Premium

View security incidents, alerts and devices from **Defender for Business** in the dashboard and get the detail from the Incidents queue*. Additional security management capabilities are constantly added.

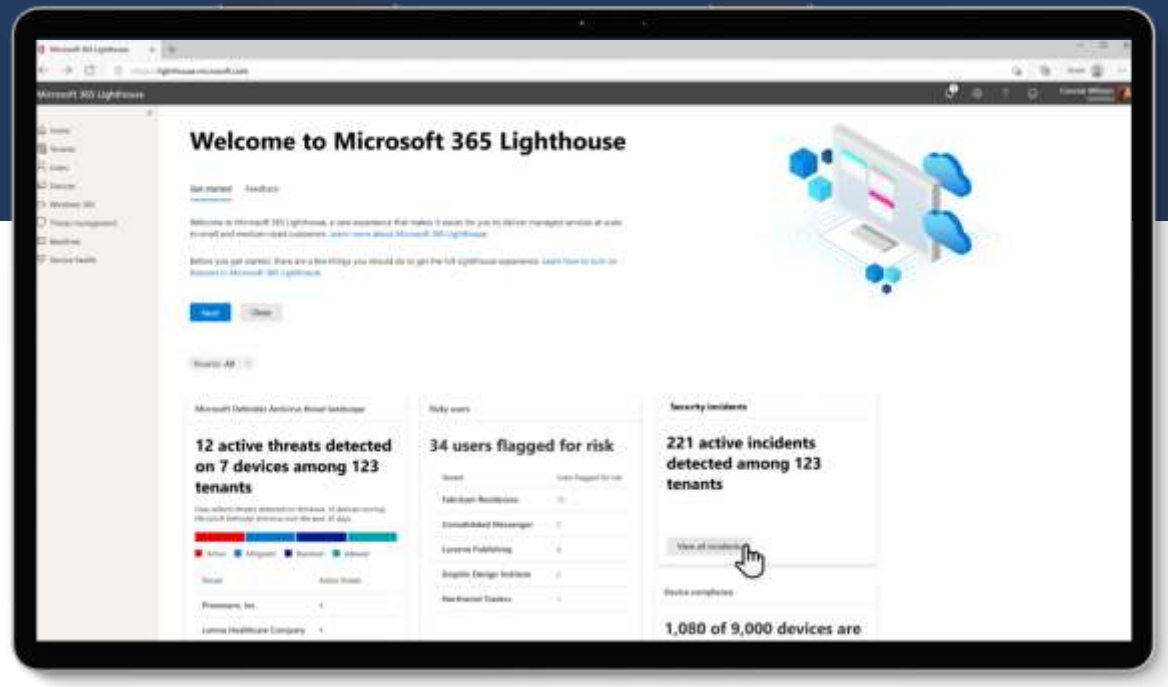


Image 1: Security incident summary on the Home dashboard

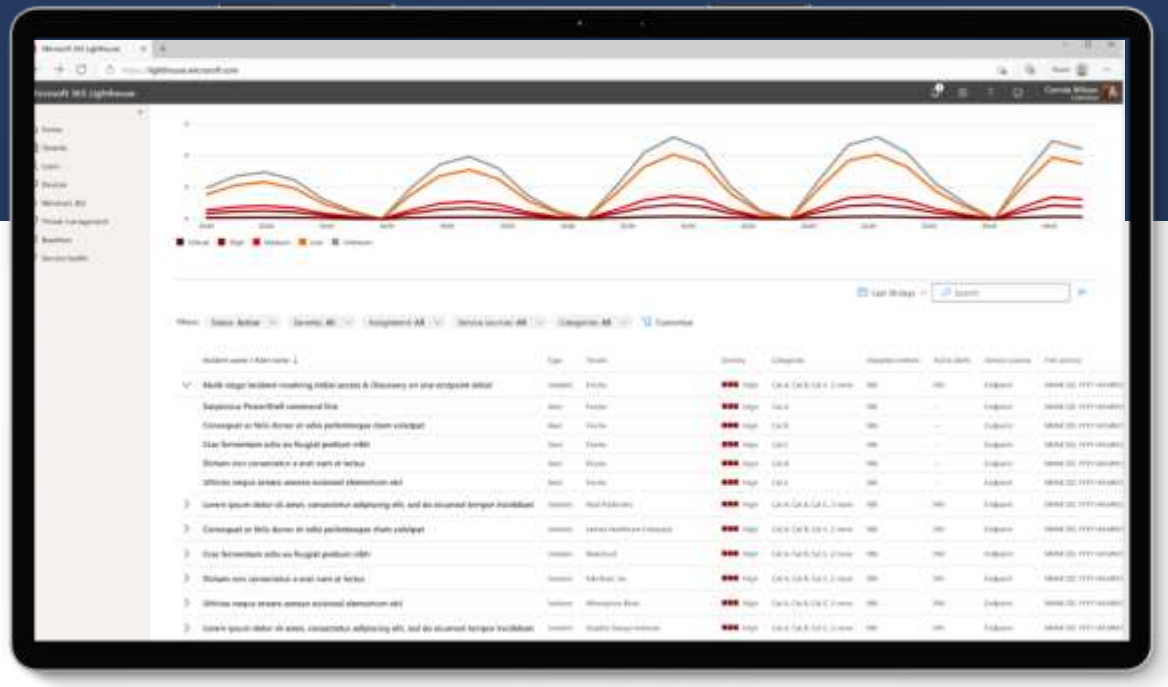
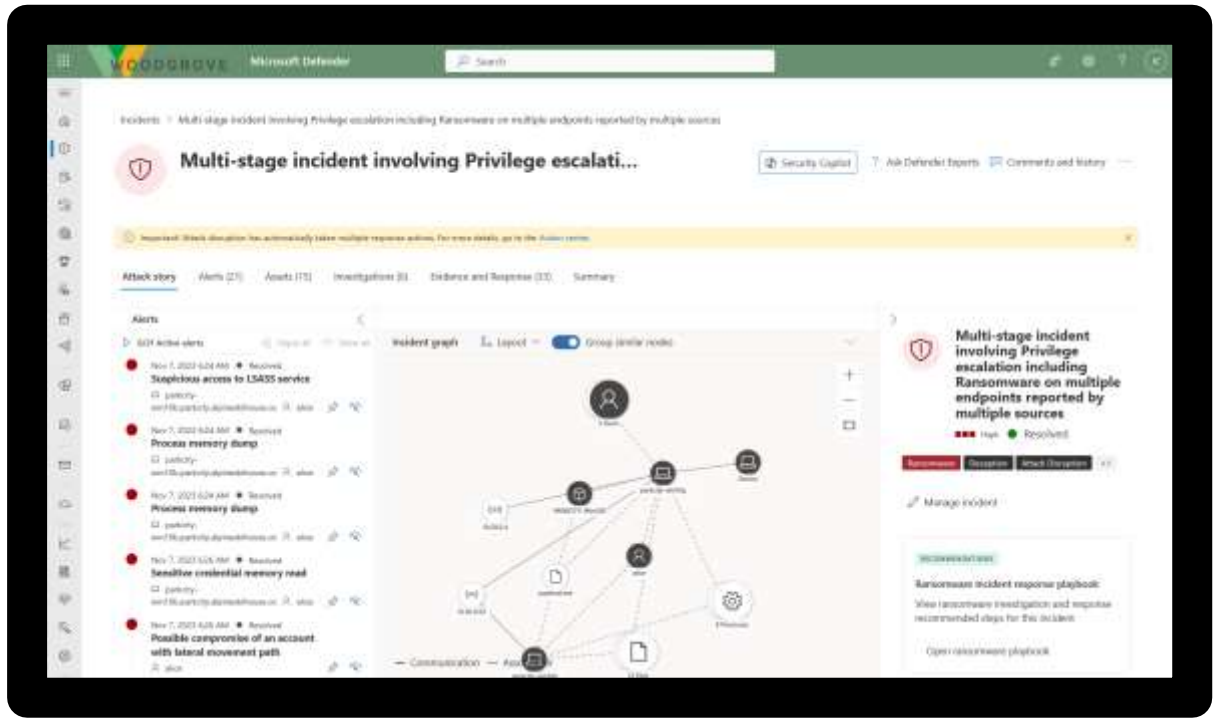


Image 2: Incident queue highlighting security incidents and alert details

Attack disruption at machine speed

XDR-level intelligence and AI automatically disrupt even the most advanced attacks



Detection

Correlates signals from multiple sources into a single, high-confidence incident

Classification

Classify attack scenario and **identify** assets controlled by the attacker

Attack disruption

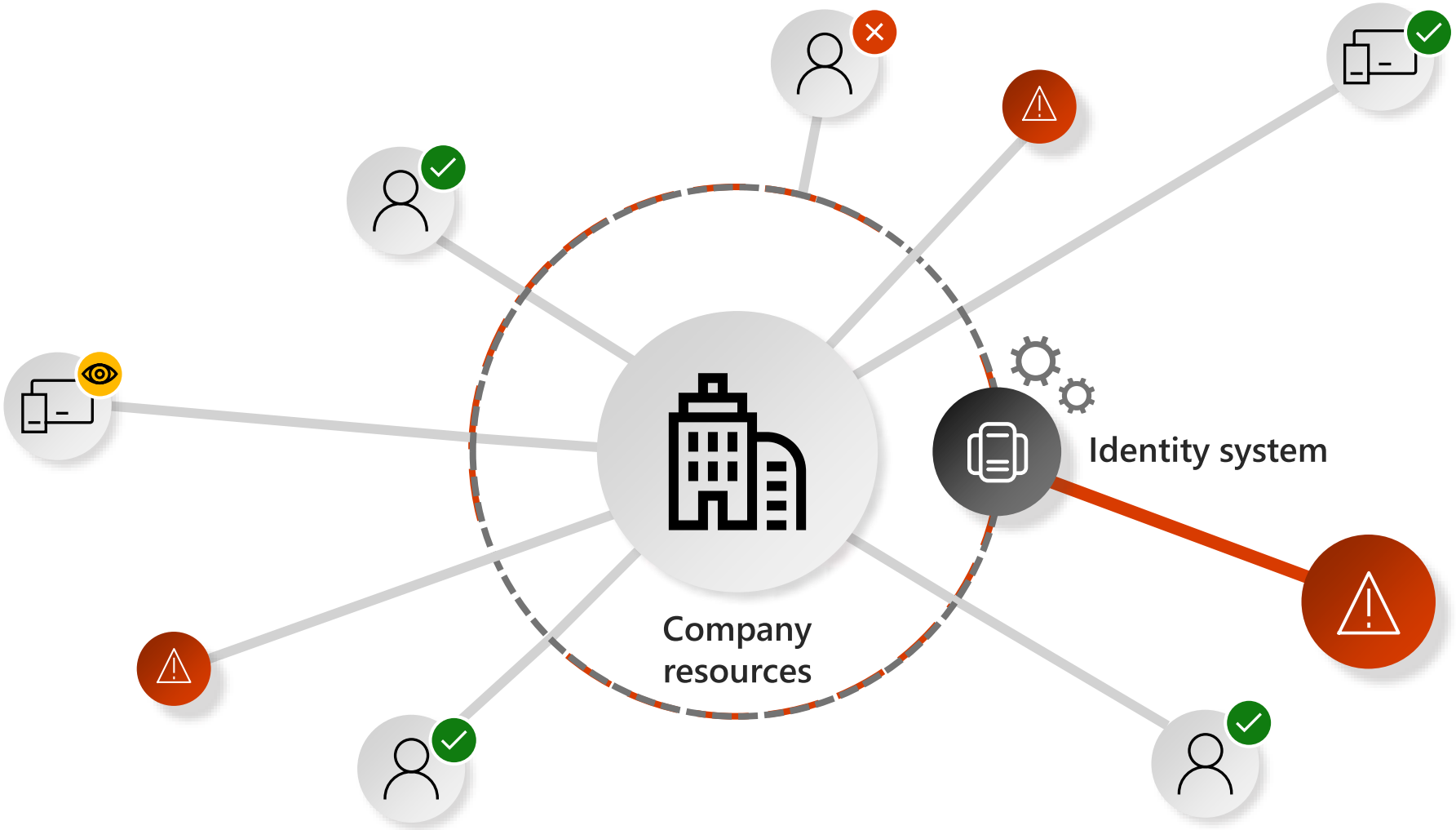
Automatically isolates infected devices and suspends compromised accounts in real-time

AI-powered **automation** disrupts lateral movement

Leaves the SOC team in full control of investigating and remediating

Reduces the overall cost and limits the impact of an attack by stopping lateral movement

Identity protection is your first line of defense



Microsoft Intune

Modern endpoint management powered by the Microsoft Cloud

Simplify endpoint management

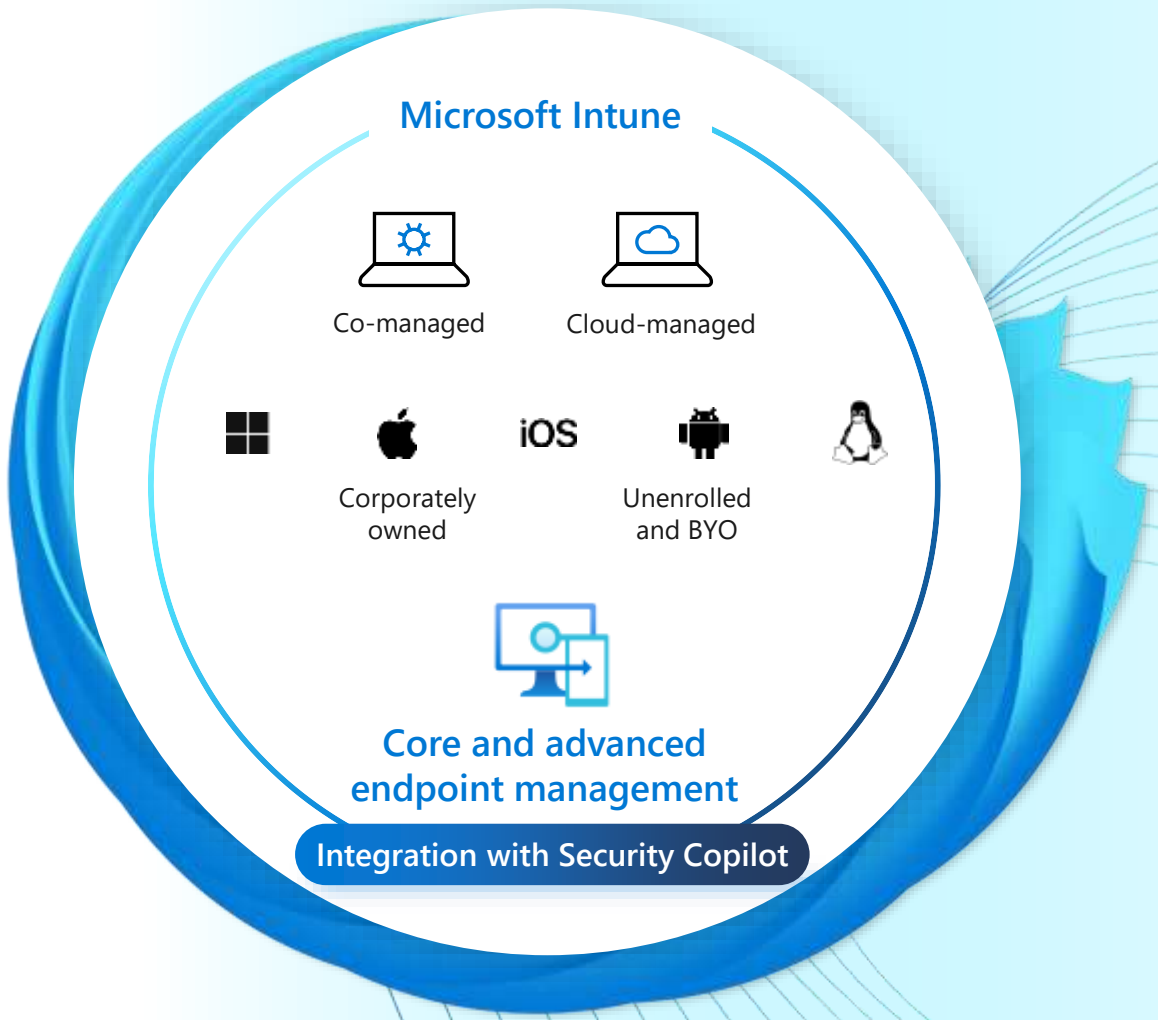
Cut cost and complexity by shifting to the cloud, unifying endpoint management and security tools in one place.

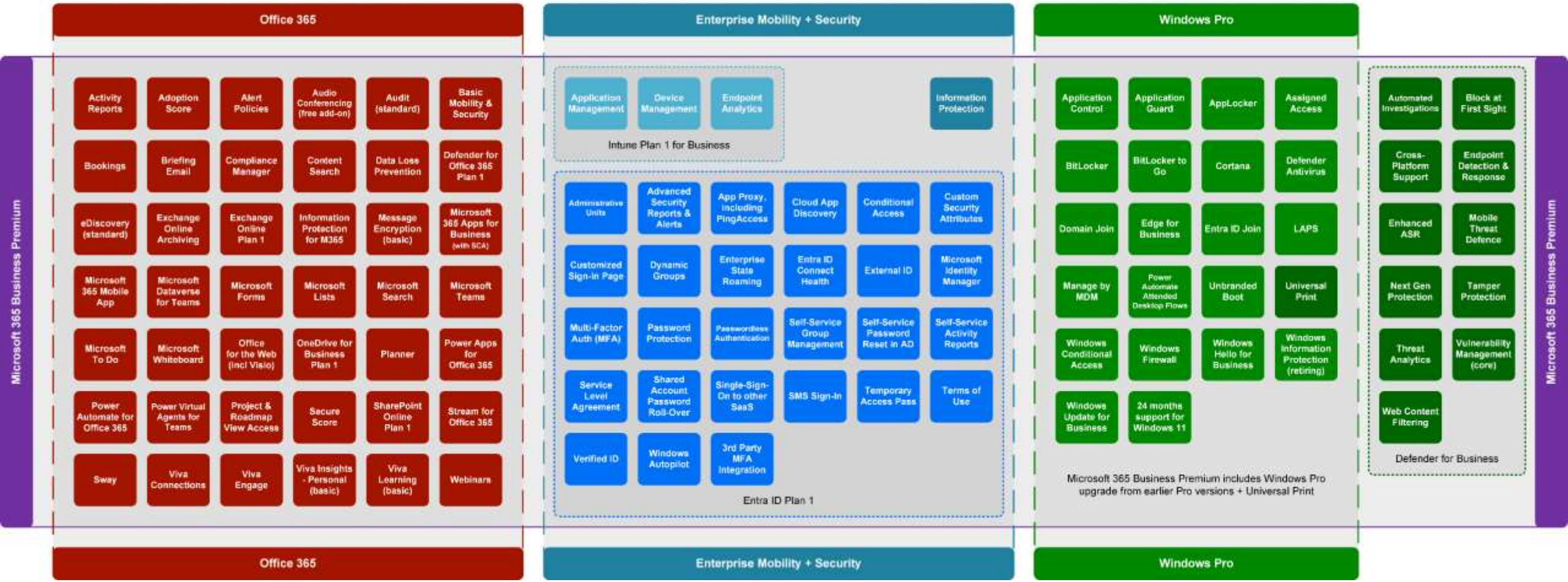
Fortify Zero Trust security

Mitigate threats and improve compliance across all devices by protecting users, devices, apps, and data.

Increase satisfaction

Proactively manage better user experiences while driving operational efficiency with data science and automation.



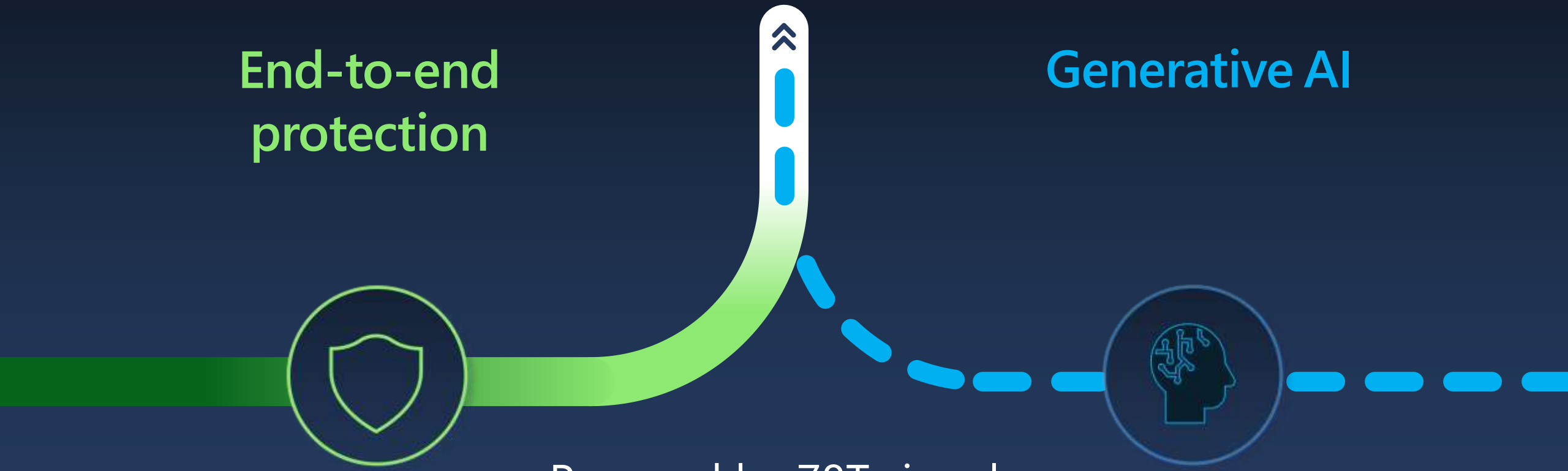


Source: [Home | M365 Maps]

End-to-end protection with generative AI is a force multiplier

End-to-end protection

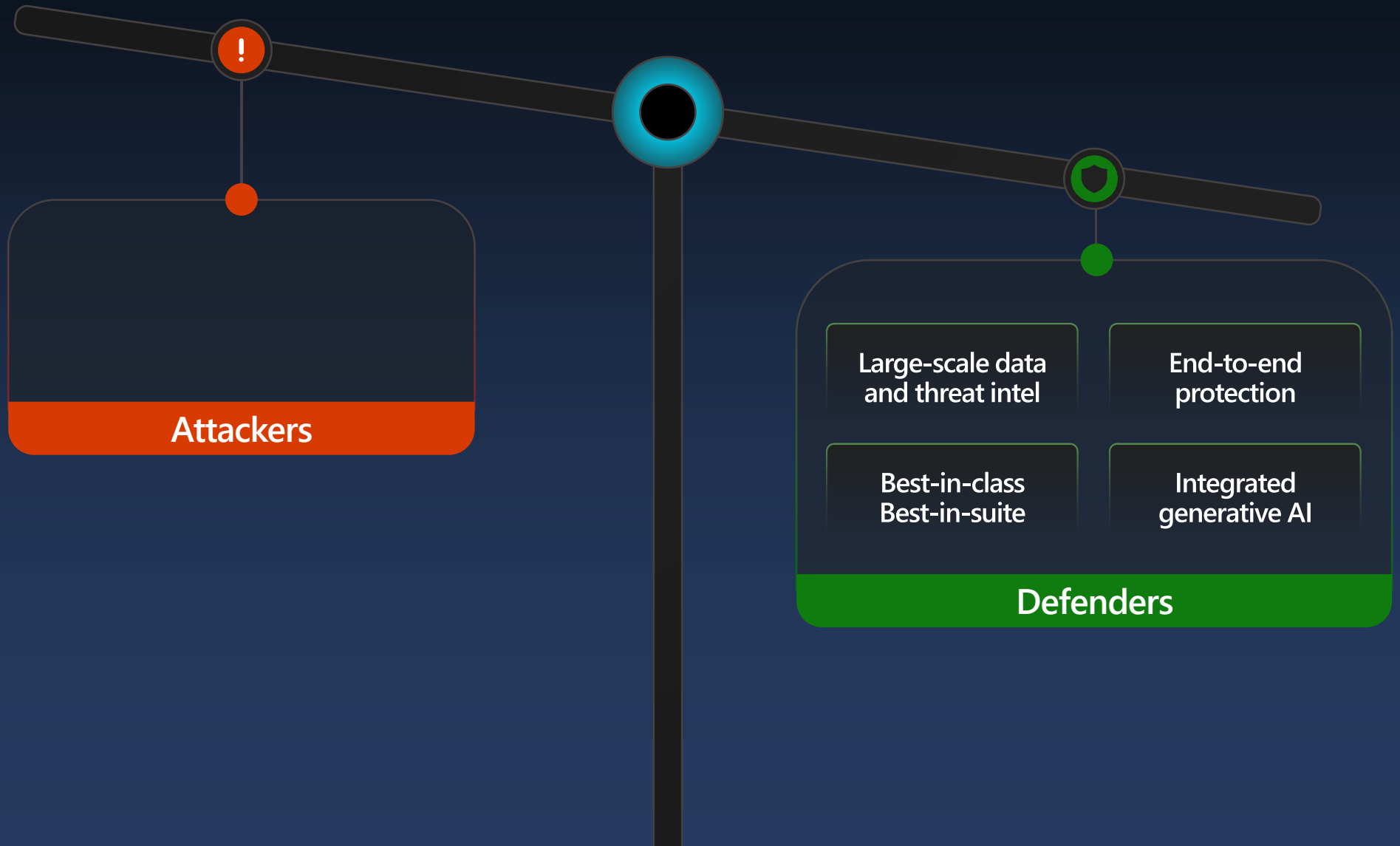
Generative AI



Powered by 78T signals


Copilot for Security
Ask anything about security

Microsoft tips the scale in favor of defenders



Microsoft – a Leader in three Gartner® Magic Quadrant™ reports

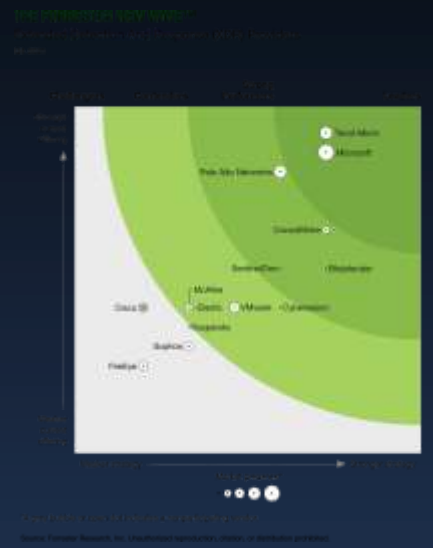
Gartner® Magic Quadrant™ for Access Management

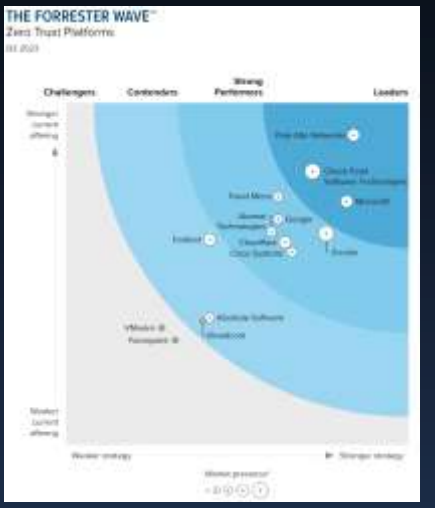
Gartner® Magic Quadrant™ for Endpoint Protection Platforms

Gartner® Magic Quadrant™ for Security Information and Event Management

Gartner Magic Quadrant for Access Management, Henrique Teixeira | Abhyuday Data | Nathan Harris | Robertson Pimentel, 16 November 2023.
Gartner Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook | Chris Silva, 31 December 2022.
Gartner Magic Quadrant for Security Information and Event Management, Pete Shoard | Andrew Davies | Mitchell Schneider, 10 October 2022.

Microsoft – a leader in nine Forrester Wave™ reports





The Forrester New Wave™: Extended Detection and Response (XDR), Q4 2021, Allie Mellen, October 2021.
The Forrester Wave™: Endpoint Detection and Response Providers, Q2 2022, Allie Mellen, April 2022.
The Forrester Wave™: Enterprise Email Security, Q3 2023 Jess Burn, Joseph Blankenship, June 2023.
The Forrester Wave™: Security Analytics Platforms, Q4 2022, Allie Mellen, Joseph Blankenship, December 2022.
The Forrester Wave™: Infrastructure-As-A-Service Platform Native Security, Q2 2023, Andras Cser, May 2023.
The Forrester Wave™: Data Security Platforms, Q1 2023 Heidi Shey, March 2023.
The Forrester Wave™: Zero Trust Platform Providers, Q3 2023 Carlos Rivera, Heath Mullins, September 2023.
The Forrester Wave™: Endpoint Security, Q4 2023 Paddy Harrington, October 2023.
The Forrester Wave™: Unified Endpoint Management, Q4 2023 Andrew Hewitt, November 2023.

Microsoft Security

Welcome to the new era of security.

Thank you

In Person

Modern SecOps using Microsoft Sentinel and Copilot for Security

When: Monday, June 03, 2024, 9:00 AM – 4:50 PM

Where: Microsoft Office, The Circle 02, Zürich-Airport

[Microsoft Events - Modern SecOps using Microsoft Sentinel and Copilot for Security]