Emmanuele Silanesu (Manny)

ASIA Security Lead, Microsoft Security Solutions

4M

UNFILLED CYBERSECURITY JOBS WORLDWIDE

2.7M

IN THE ASIA-PACIFIC REGION, THE LARGEST WORKFORCE GAP GLOBALLY

85M

ESTIMATED GLOBAL TALENT SHORTAGE BY 2030

“We’re teaching kids how to solve problems for **today**.
But what about the problems of **five years** from now?”

SIR KEN ROBINSON

Microsoft is addressing this challenge with a

$10.5B

INVESTMENT IN ASIA'S AI AND CLOUD INFRASTRUCTURE

Governments, corporations, & citizens are asking for 4 things

01

Be more secure

02

Stay compliant

03

Lower total cost of ownership

04

Ongoing proof of value

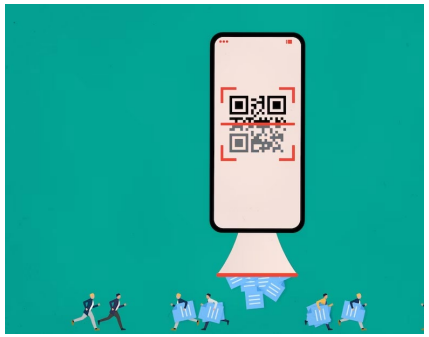
Security is shaping the world

Forbes

Criminals Hacked A Fish Tank To Steal Data From A Casino

The Washington Post

QR codes are a privacy problem — but not for the reasons you've heard



TechCrunch

CrowdStrike accepts award for 'most epic fail' after global IT outage

Anthony Ha

Updated Tue, August 13, 2024 at 3:24 AM GMT+10 · 1 min read

3

Just a few weeks after its software update triggered a global IT meltdown, CrowdStrike isn't shying away from the spotlight. In fact, the company's president Michael Sentonas even took the stage at the Pwnie Awards to accept the award for Most Epic Fail.

The awards took place at Def Con, right after the Black Hat conference where CrowdStrike had one of the biggest booths, giving out free T-shirts and action figures. A spokesperson told TechCrunch that the company's message to attendees was one of "gratitude and appreciation for the Black Hat community."

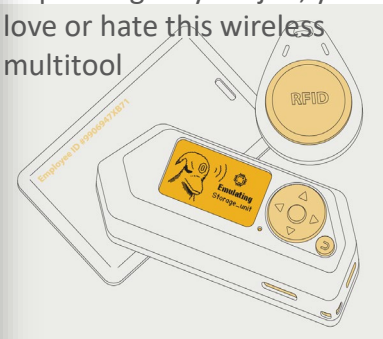
The New York Times

Microsoft Executives' Emails Hacked by Group Tied to Russian Intelligence

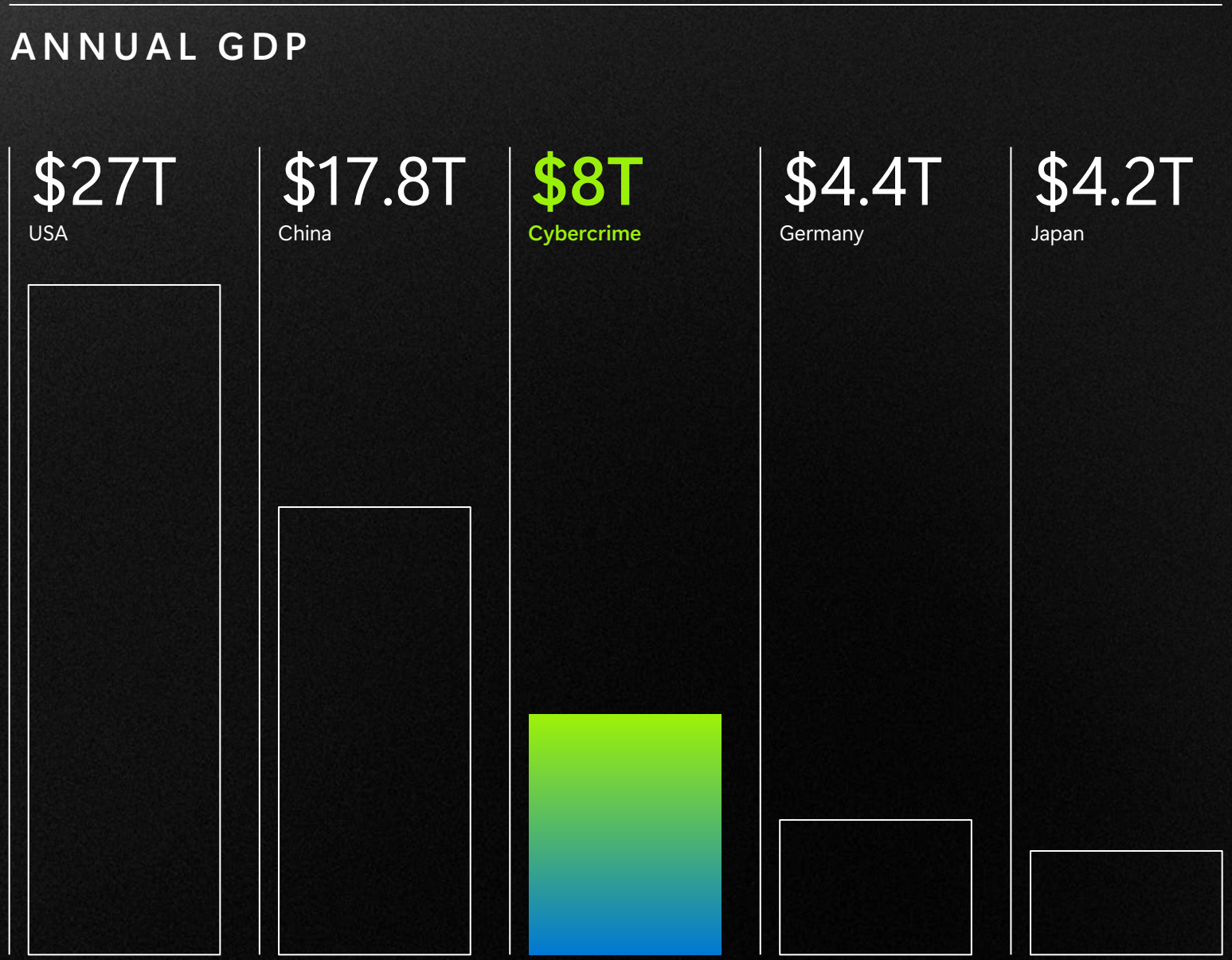
Spectrum

The Flipper Zero: A Hacker's Delight

Depending on your job, you'll love or hate this wireless multitool



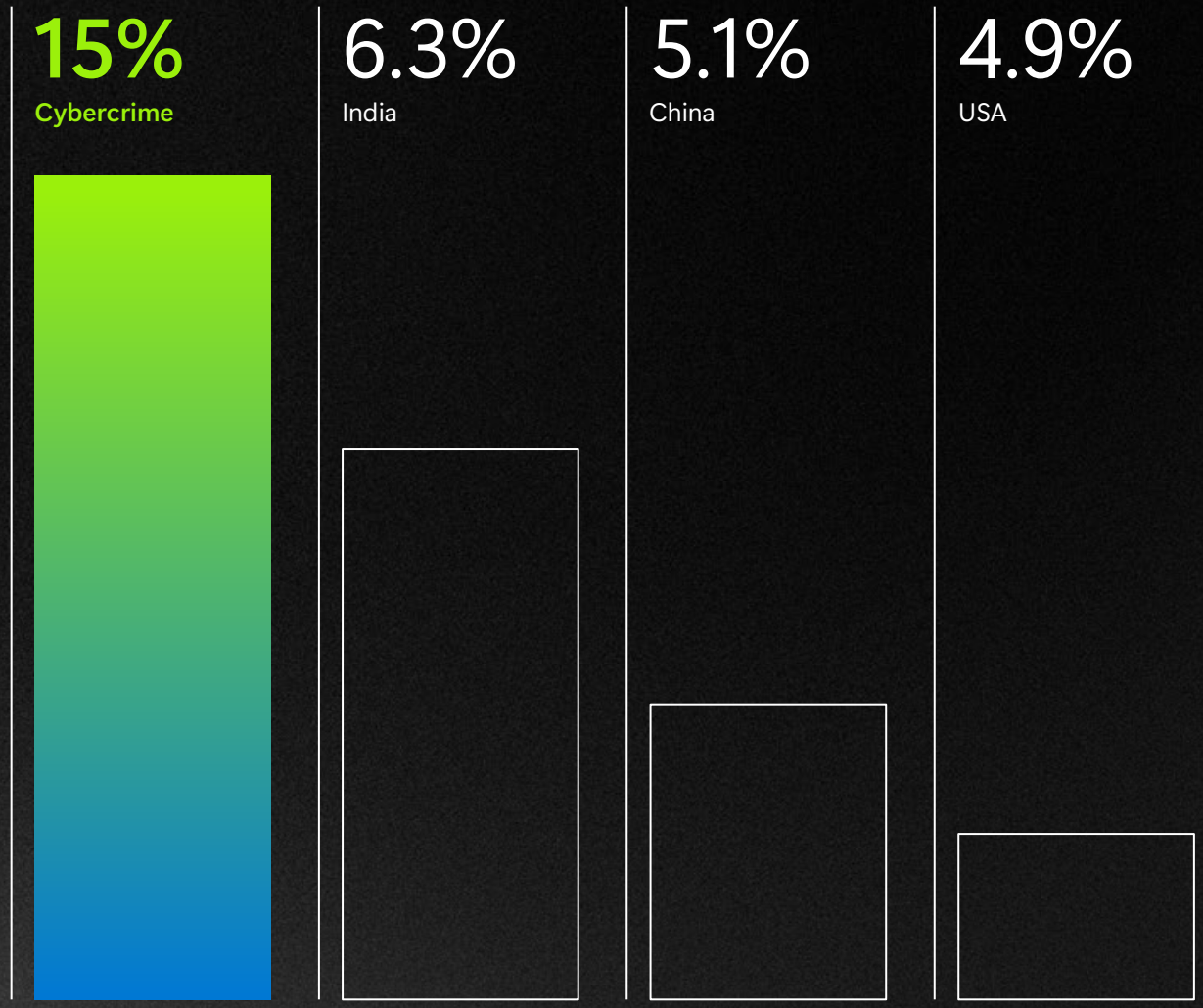
Cybercrime today equals the 3rd **largest** economy in the world



Sources: Statistica

And it's growing quickly.

ANNUAL GDP GROWTH RATE



Sources: Statistica

AI is

01 Used to attack

02 Used to defend–and in the SOC

03 Used for productivity and speed

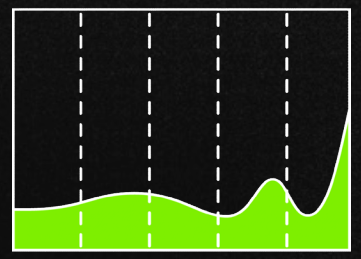
04 Used to secure AI streams

Committed to **cybersecurity**

SECURITY ABOVE ALL ELSE

The State of Cybercrime

2023 marked a **significant shift** in cybercriminal tactics



80-90%
Of ransomware attacks start from unmanaged devices

200%
Increase in human-operated ransomware

70%
Of human-operated ransomware targets had <500 employees

51%
Of cloud attacks due to weak or stolen credentials

Organizations today face an industrialized attacker economy

Stolen passwords	$0.97/1000 (avg) Bulk: $150 for 400M
Denial of service	$766.67/month
Ransomware kits	$66 upfront or 30% of the profit/affiliate model

Secure Future Initiative

2 OUTCOMES

01

A more resilient and transparent Microsoft

02

Advanced security tools

3 PRINCIPLES

01

Secure by design

Security comes first when designing any product or service

02

Secure by default

Security protections are enabled & enforced by default, require no extra effort, and are not optional

03

Secure operations

Security controls & monitoring will continuously be improved to meet current and future threats

Proactive **threat hunting**

Identification and removal of bad actors

$20B In revenue

120 Countries

78T Signals synthesized daily

1M Customers

100K+ Domains removed

10K+ Security & threat intelligence experts

4K ID attacks blocked/sec

135M Managed devices

300+ Threat actors tracked

15K+ Security ecosystem partners

$20B Of investment

Governments, corporations, & citizens are asking for 4 things

01

Be more secure

02

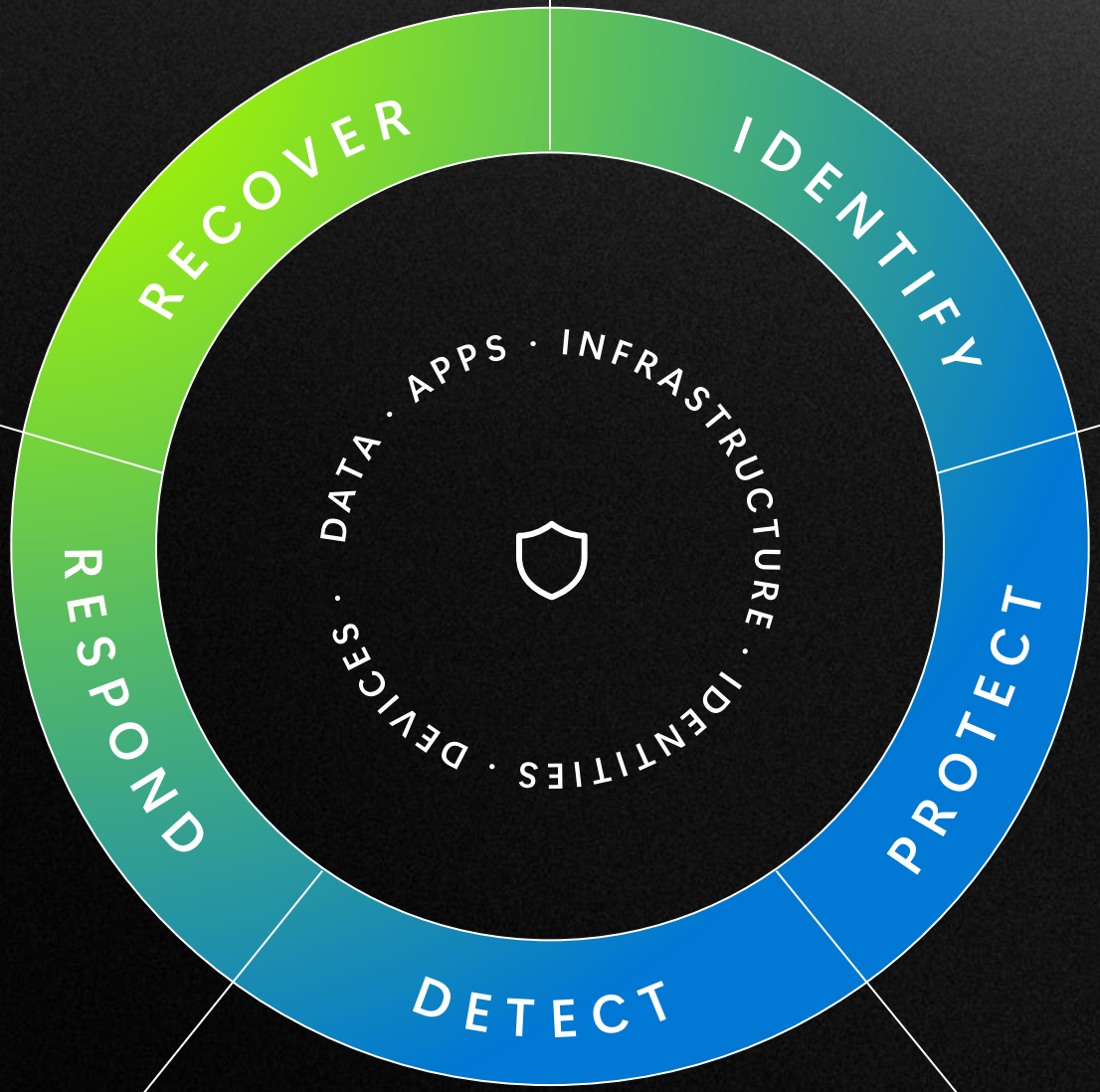
Stay compliant

03

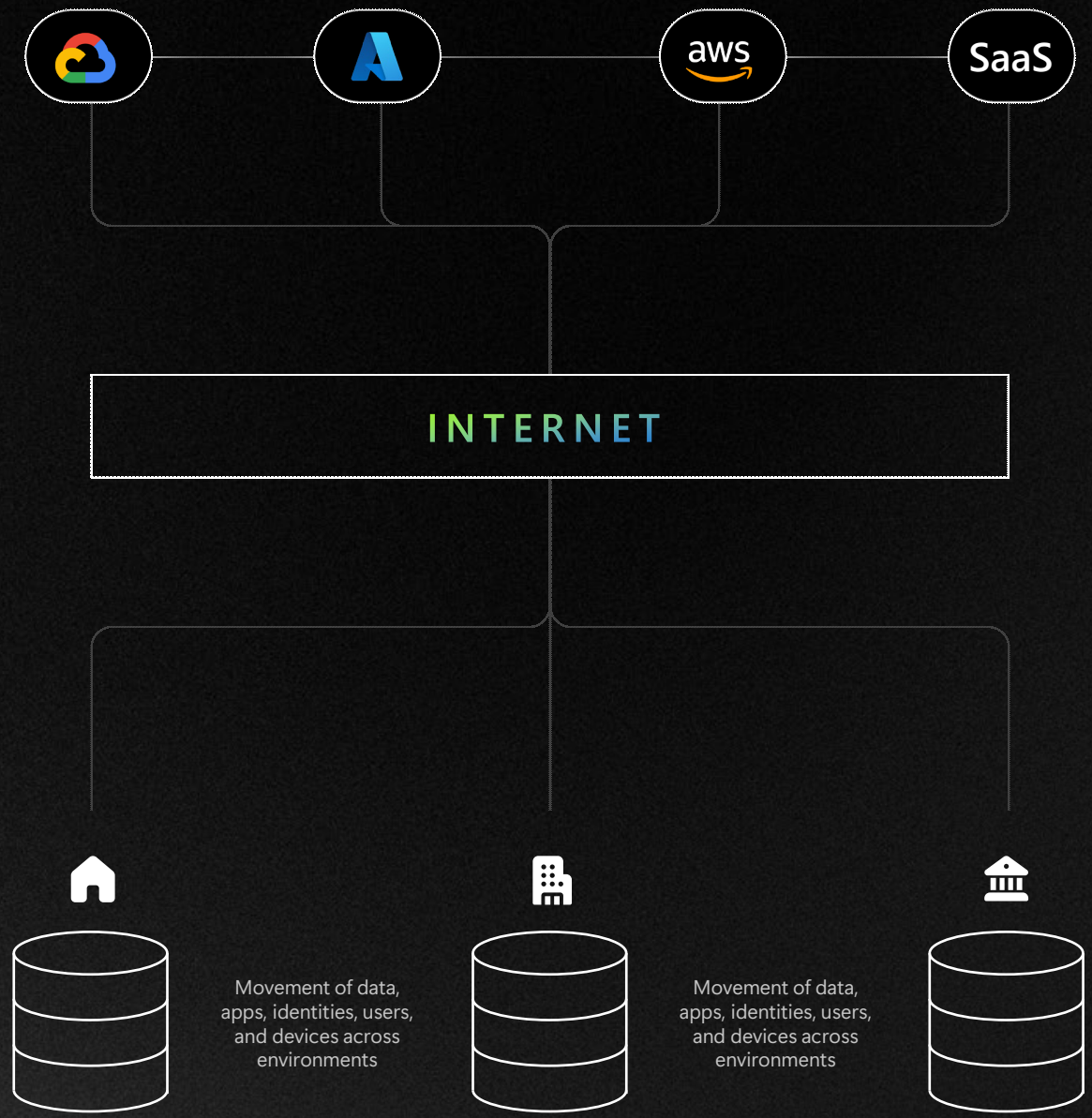
Lower total cost of ownership

04

Ongoing proof of value


RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
DATA · APPS · INFRASTRUCTURE · IDENTITIES · DEVICES ·

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



Current state

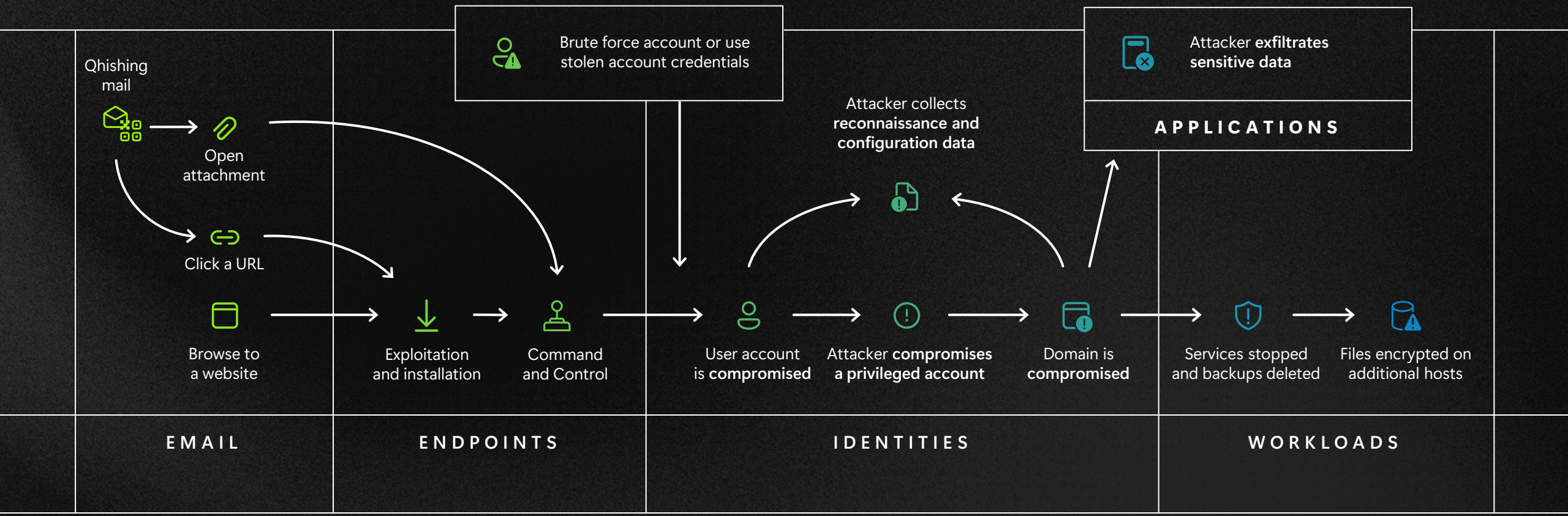
How companies and governments solve it today

Legacy Technology Companies

Next-Gen Technology Companies

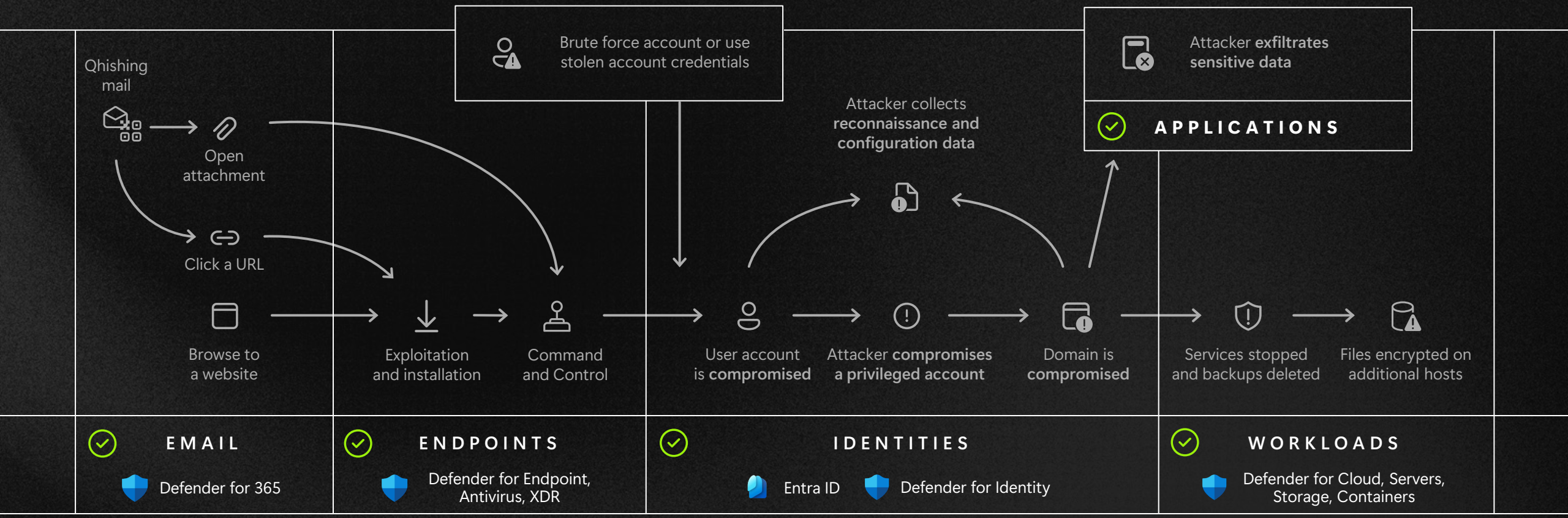
Simple mistakes open doors

TYPICAL HUMAN-OPERATED RANSOMWARE CAMPAIGN



Protection across the entire kill chain

WITH MICROSOFT SIEM AND XDR



UNCOVER THE ATTACK END TO END AND TAKE ACTION TO EVICT THE ATTACKER

Microsoft

Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

Security Operations / SOC

Microsoft Security Experts
Defender Experts | Detection and Response Team (DART)

Managed Security Operations
Using Microsoft Security

Microsoft Defender XDR
Unified Threat Detection and Response across IT, OT, and IoT Assets
Incident Response | Automation | Threat Hunting | Threat Intelligence

Microsoft Sentinel
Cloud Native SIEM, SOAR, and UEBA

Microsoft Security Copilot (Preview)

Cloud	Endpoint	Office 365	Identity	SaaS	Data	OT/IoT	Other
Azure, AWS, GCP, On Prem & more	Workstations, Server/VM, Containers, etc.	Email, Teams, and more	Cloud & On-Premises	Cloud Apps	SQL, DLP, & more	devices	Tools, Logs, & Data

Software as a Service (SaaS)

Microsoft Defender for Cloud Apps
- App Discovery & Risk Scoring (Shadow IT)
- Threat Detection & Response
- Policy Audit & Enforcement
- Session monitoring & control
- Information Protection & Data Loss Prevention (DLP)

Microsoft Entra Internet Access

Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

Endpoints & Devices

Unified Endpoint Management (UEM)
Intune | Configuration Manager

Microsoft Defender for Endpoint
Unified Endpoint Security
Endpoint Detection & Response (EDR)
Web Content Filtering
Threat & Vuln Management
Endpoint Data Loss Protection (DLP)
...

Hybrid Infrastructure – IaaS, PaaS, On-Premises

Defender for Cloud – Cross-Platform Cloud Security Posture Management (CSPM)

Secure Score
Compliance Dashboard
...

On Premises Datacenter(s) | *3rd party IaaS & PaaS* | Microsoft Azure

Extranet
NGFW
Edge DLP
IPS/IDS/NDR
Microsoft Entra Private Access & App Proxy
Beyond User VPN
Intranet
Azure Arc
Azure Stack
Express Route
Private Link
Azure Marketplace

Azure Firewall & Firewall Manager
Azure WAF
DDoS Protection
Azure Key Vault
Azure Bastion
Azure Lighthouse
Azure Backup
Security & Other Services

Information Protection

Microsoft Purview
Information protection and governance across data lifecycle
Discover | Classify | Protect | Monitor

Classification Labels
File Scanner
(on-premises and cloud)

Data Governance
Advanced eDiscovery

Compliance Manager

Microsoft Entra

Passwordless & MFA
Hello for Business
Authenticator App
FIDO2 Keys

Entra ID Protection
Leaked cred protection
Behavioral analytics

ID Governance
Microsoft Entra PIM
External Identities

Defender for Identity

Active Directory

Securing Privileged Access – aka.ms/SPA

Entra Permission Management – Discover and Mitigate Cloud Infrastructure Permission Creep

Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users

Security Posture Management – Monitor and mitigate technical security risks using Secure Score, Compliance Score, CSPM: Defender for Cloud, Microsoft Defender External Attack Surface Management (EASM) and Vulnerability Management

Windows 11 & 10 Security
Network protection | App control
Credential protection | Exploit protection
Full Disk Encryption | Behavior monitoring
Attack surface reduction | Next-generation protection
...

IoT and Operational Technology (OT)

Azure Sphere

Microsoft Defender for IoT (and OT)
ICS, SCADA, OT
Internet of Things (IoT)
Industrial IoT (IIoT)
Asset & Vulnerability management
Threat Detection & Response

Defender for Cloud – Cross-Platform, Multi-Cloud XDR
Detection and response capabilities for infrastructure and development across IaaS, PaaS, and on-premises

Defender for APIs *(preview)*

People Security

Attack Simulator | Insider Risk Management | Communication Compliance

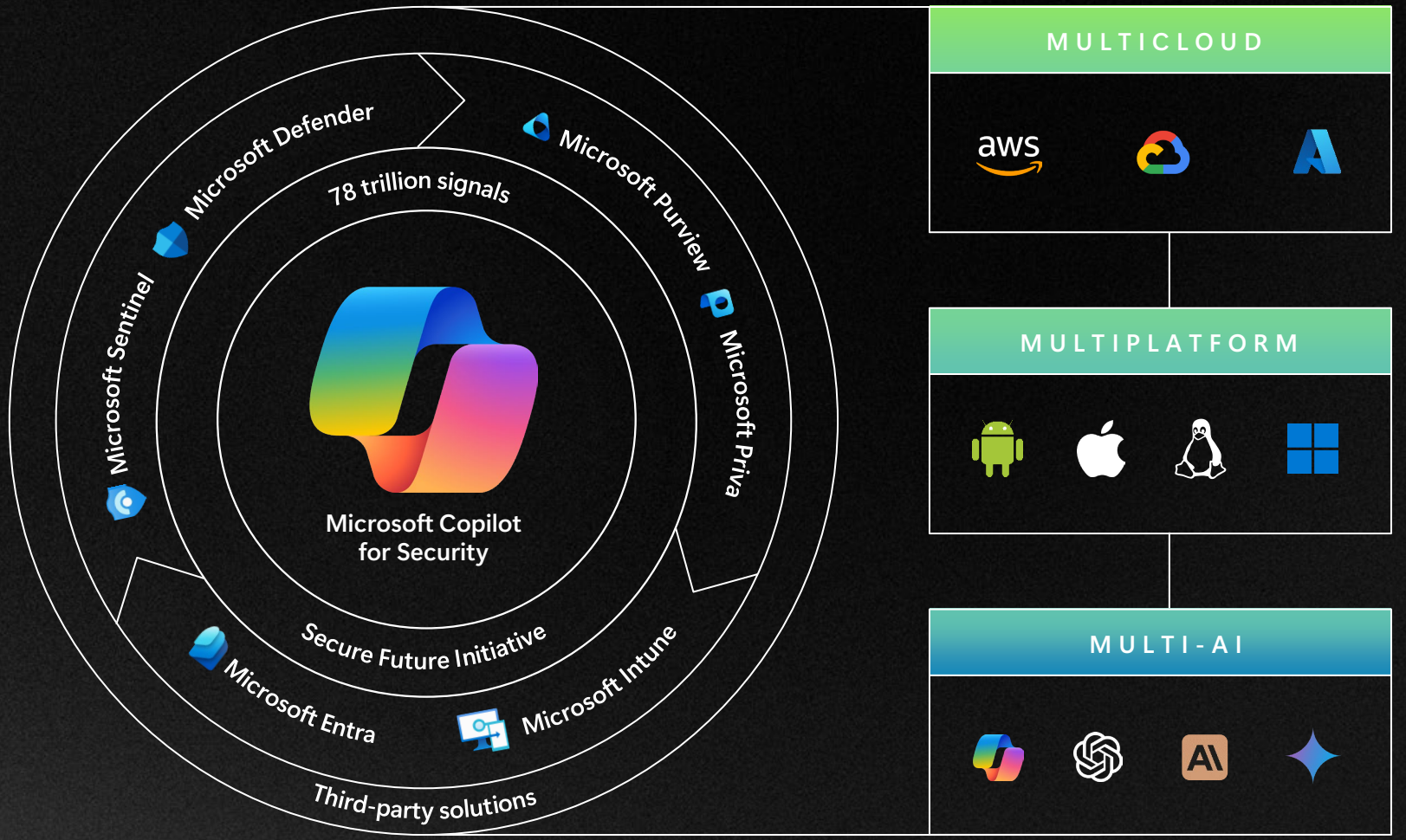
GitHub Advanced Security & Azure DevOps Security
Secure development and software supply chain

Threat Intelligence – 65+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

Force multiplier for security



Governments, corporations, & citizens are asking for 4 things

0 1	0 2	0 3	0 4
Be more secure	Stay compliant	Lower total cost of ownership	Ongoing proof of value

© Copyright Microsoft Corporation. All rights reserved.

Stay compliant

Secure and govern your organization's data across your entire digital estate.

Accelerate the secure adoption of AI with ready-to-go data security and governance tools purpose-built for generative AI.

90+

Global certifications and attestations, including GDPR, ISO 27001, and SOC 1/2/3

400+

GenAI app risk assessments ready for use by your team

320+

Ready-to-use and customizable regulatory assessment templates to meet multicloud compliance requirements

Supports AI compliance with the EU AI Act, NIST AI Risk Management Framework, ISO 42001, ISO 23894, code-of-conduct policies, and more

99.9%

Uptime commitment for Microsoft 365 ensures continuous compliance management

Discover, protect, and govern the use of generative AI for Copilot, ChatGPT, Claude, Gemini, private LLMs, and more

Governments, corporations, & citizens are asking for 4 things

0 1	0 2	0 3	0 4
Be more secure	Stay compliant	Lower total cost of ownership	Ongoing proof of value

© Copyright Microsoft Corporation. All rights reserved.

Lower total cost of ownership

Simplify your security operations with seamlessly integrated end-to-end protection that consolidates fragmented tools, offering more cost savings and higher productivity.

60%

Cost savings

231%

Return on investment*

50

Products categories replaced

26%

Time saved by security novices when using Copilot for Security

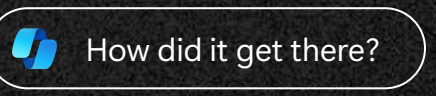
22%

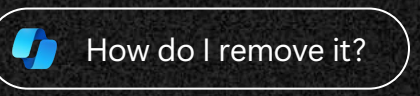
Time saved by experienced security professionals when using Copilot for Security

*Source: Forrester

Governments, corporations, & citizens are asking for 4 things

0 1	0 2	0 3	0 4
Be more secure	Stay compliant	Lower total cost of ownership	Ongoing proof of value





Conceptual demo. Features not yet available

Governments, corporations, & citizens are asking for 4 things

01

Be more secure

02

Stay compliant

03

Lower total cost of ownership

04

Ongoing proof of value