



Irene Sardellitti
National Technology Officer

Security is shaping the world and impacting every organization



The hackers attempted to acquire data from a North American casino by using an Internet-connected fish tank, according to a report released Thursday by cybersecurity firm Darktrace.

The fish tank had sensors connected to a PC that regulated the temperature, food and cleanliness of the tank.

Servizio | Ad Hong Kong

Video fake del direttore finanziario: dipendenti spostano 25 milioni ma è una truffa

Un contenuto creato grazie all'intelligenza artificiale trae in inganno alcuni impiegati, così la multinazionale è stata truffata

di Biagio Simonetta

7 febbraio 2024

Servizio | La storia

Falso Ceo di Ferrari tenta di truffare dirigente con l'intelligenza artificiale

Un alto dirigente di Ferrari è stato vittima di un tentativo di truffa tramite deep fake e intelligenza artificiale, ma è riuscito a sventare il piano

di Biagio Simonetta

26 luglio 2024

Avviso. Presenza in rete di nuovi videomessaggi falsi con tecniche di deepfake

22 novembre 2024

Condividi



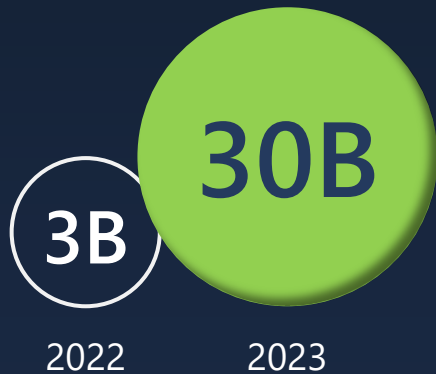
La Banca d'Italia avverte della presenza in rete di nuovi videomessaggi che, in maniera artificiosa, riproducono l'immagine e la voce del Governatore della Banca d'Italia.

Tali contenuti sono generati anche attraverso l'applicazione di tecniche, conosciute come deepfake, che fanno uso dell'intelligenza artificiale per veicolare e rendere maggiormente credibili messaggi non veritieri e presumibilmente finalizzati alla truffa.

We live in the most complex threat landscape in history

Speed, scale, and
sophistication of attacks

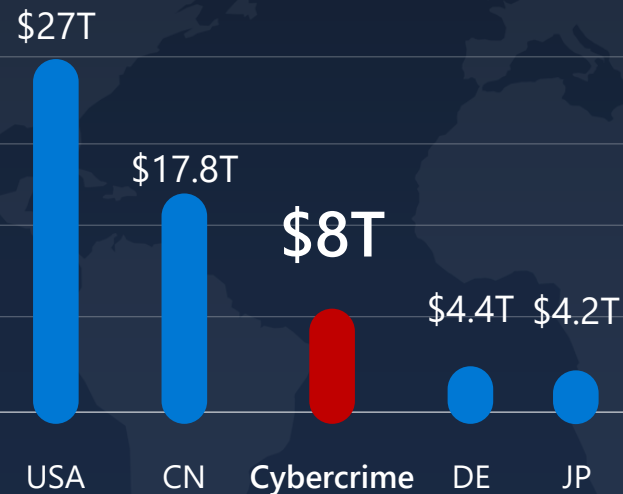
Password attacks
per month



Source: Microsoft

Rapidly growing
cyber economy

Annual GDP



Source: Statista

Growing regulatory
environment



250
new regulatory
updates tracked
every day

Source: Microsoft

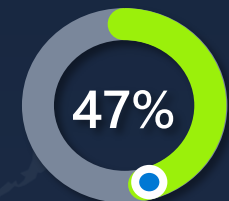
Open cybersecurity jobs

1 in 3



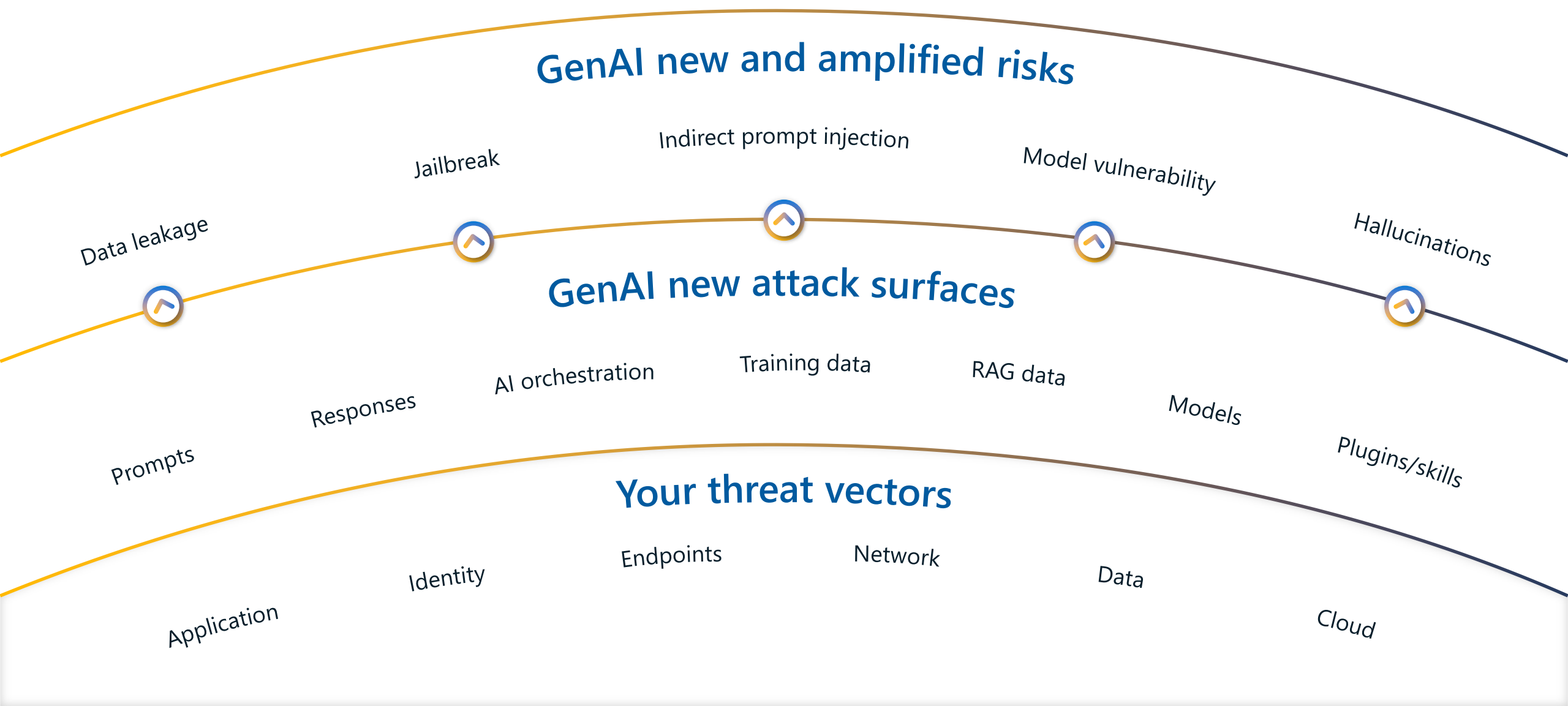
Source: Cyberseek

Increase in phishing
attacks, driven by attack
use of AI



Source: Zscaler

GenAI attack surfaces introduce new and amplified risks



Security teams need better outcomes

Microsoft teams need the same



Be more secure



Stay compliant



Lower total cost of
ownership

...in the age of generative AI

For Microsoft, security is job 1

“

...prioritizing security above all else is critical to our company's future”

Satya Nadella

Chairman and CEO



2 Outcomes



A More Resilient and Transparent
Microsoft



Advanced Security Tools

3

Principles of Microsoft's Secure Future Initiative

Secure by Design

Security comes first when designing
any product or service

Secure by Default

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

Secure Operations

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

The Secure Future Initiative (SFI) builds on three core principles which ensure that our products are secure from inception through deployment and ongoing use

SFI: Culture and governance

Culture

- **Performance management:** Security is now a factor in performance evaluation at every level.
- **Learning and development:** To improve security skilling, we
 - Introduced Microsoft Security Academy, which will be customized for specific roles and functions.
 - Required training, including Security Foundations and Standards of Business Conduct trainings.

Governance

- **Cybersecurity Governance Council:** Responsible for overall cyber risk and compliance.
- **Execution framework:** Addresses risk at scale through SFI engineering actions with repeatable and durable patterns.
-

SFI: Microsoft progress to date



Protect identities and secrets

Video-based user verification enabled for 95% of employees

Enforcing phishing-resistant multifactor authentication (MFA), and adopting managed identities.



Protect tenants and isolate production systems

Eliminated 730,000 unused applications and 5.75 million tenants

Completed full lifecycle management for productivity and production tenants



Protect networks

99.3% of network assets inventoried

Increased isolation of virtual networks with backend connectivity from the Microsoft network to reduce



Protect engineering systems

85% of production build pipelines use centrally governed pipeline templates

Implemented standards of strong authentication protocols that do not rely on weak mechanisms such as plaintext credentials



Monitor and detect threats

Over 99% of network device audit logs centrally stored and analyzed

Established standardized log libraries and a two-year minimum retention policy



Accelerate response and remediation

90% of high severity cloud vulnerabilities addressed within our reduced time to mitigate

Transparently sharing vulnerability mitigations and improving security incident communications. Created new Customer Security Management Office (CSMO)

How we are building a digital defense

Investing

\$20B in cybersecurity research and development over five years

Tracking

1500+ unique nation-states, cybercriminals, and other threat actors

Analyzing

78T threat signals every day

Partnering

15K Partners in our security ecosystem

Protecting

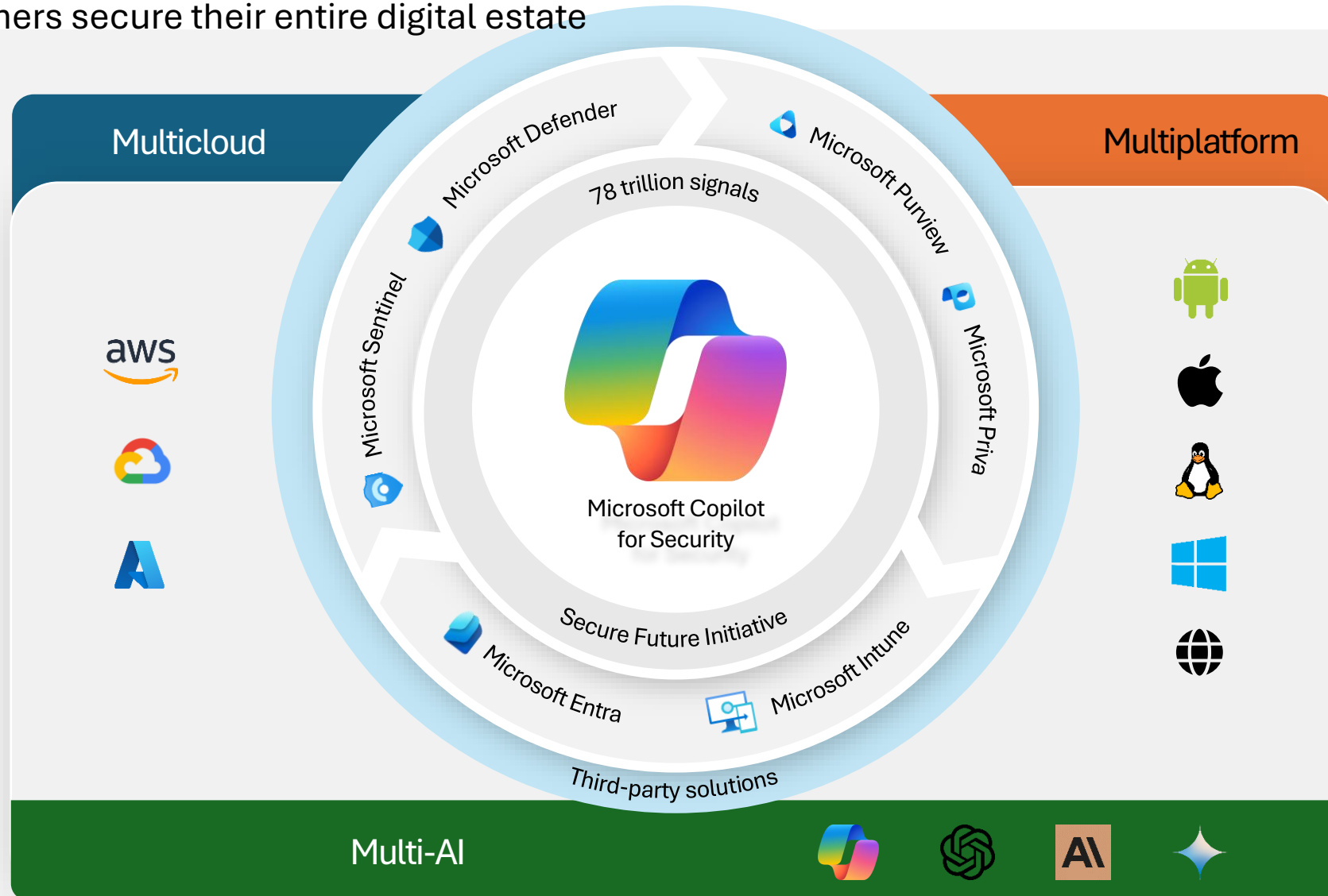
1M+ organizations in 120 countries

Removed

100K domains used by cybercriminals

AI-first end-to-end security for the age of AI

to help customers secure their entire digital estate



AI-first end-to-end security for the age of AI



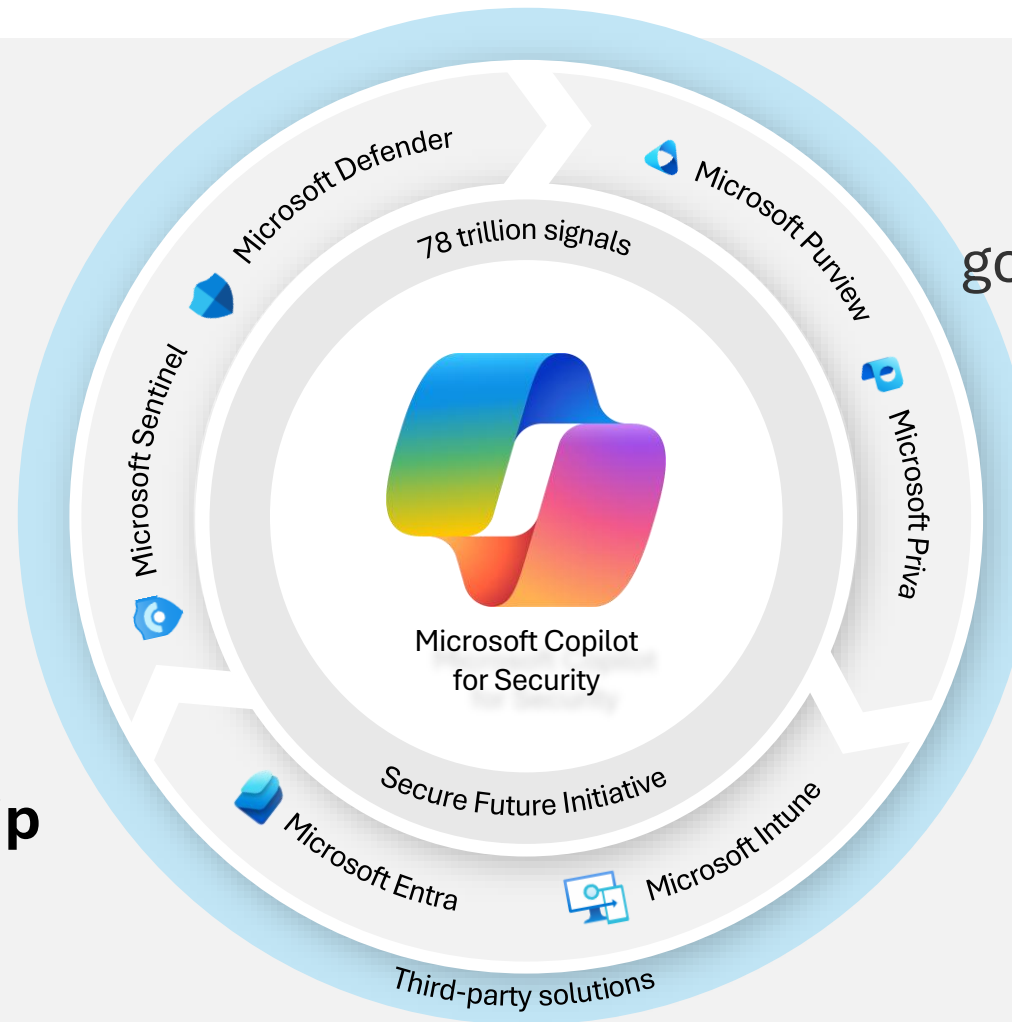
Security



Compliance



**Lower your total
cost of ownership**









Multi-AI

Purview providing governance and data security;
Defender and Sentinel providing threat protection and posture management
Intune managing endpoint and enforcing policies;
Entra providing identity and access management

Microsoft cloud investments in Europe

Dedication to Europe spans more than 40 years.

Over the past 16 months, we have invested more than \$20 billion in AI and cloud infrastructure across the EU expanding local options and meet growing demand.

Microsoft expands local options	Microsoft EU Data Boundary	Microsoft 365 Advanced Data Residency	Microsoft Cloud for Sovereignty	Microsoft European Cloud Principles
 17 + 17+ DATACENTER REGIONS WITH DATA RESIDENCY IN EUROPE 	 CUSTOMER DATA, PSEUDONYMIZED PERSONAL DATA STORED AND PROCESSED AND PROFESSIONAL SERVICES DATA STORED IN THE EU BOUNDARY.	 CONTROLS OVER MICROSOFT 365 CUSTOMER DATA LOCATION.	 SPECIFIC PUBLIC SECTOR AND REGULATED CUSTOMERS BUILD AND DIGITALLY TRANSFORM AZURE WORKLOADS IN THE MICROSOFT CLOUD.	 ENHANCED TRANSPARENCY FOR THE PUBLIC.

Efforts reflect our ongoing focus on supporting Europe's innovation, growth, and technology needs as the region moves into an increasingly digital future.

Italy North



1

Geography

1

Region

3

Zones



Data Residency and Sovereignty



Minimal latency of under 2 ms



Fully Microsoft managed and operated

EU data boundary

Commitment

The EU Data Boundary is a promise by Microsoft Online Services to provide customers in the EU and EFTA with greater control and transparency over where their data is stored and processed.

Objective

Align with European digital values and needs.

Initiative rollout



Phase 1 (January 2023):
Focused on customer data.

Phase 2 (January 2024):
Extended coverage to pseudonymized personal data.

Phase 3 (February 2025):
Professional Services Data (technical support data) is now also securely stored within the EU and EFTA regions.

Data Sovereignty and local regulation



Sovereign Control Portfolio

Protect workloads from outside access using advanced sovereignty and **encryption controls** such as **confidential computing** and **Azure Managed HSMs**.

Sovereign Guardrails & Guidance

Get access **to codified architectures, policy, workload templates**, and tooling to assist in creating compliant architectures and answer sovereign questions.

Compliance & Transparency

Ensure local compliance with **policy packs** for your region and increased **transparency** over—and into—your environment's operations.

Public Cloud Capabilities within the EUDB

Get the **innovation, scale, and security of the public cloud**, with capabilities significantly beyond private or on-prem datacenters.



Service Trust Portal

Comprehensive resource for regulatory support for **security**, regulatory **compliance**, and **privacy information related to the Microsoft cloud**

KEY FEATURES










- Compliance Manager
- Audit and Compliance Report
- Risk management tool

Service Trust Portal






Informazioni su come Microsoft i servizi cloud proteggono i dati e su come gestire la sicurezza e la conformità dei dati cloud per l'organizzazione.





Certificazioni, normative e standard

 ISO/IEC International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)	 SOC Report soc (System and Organization Controls) 1, 2 e 3	 GDPR Regolamento generale sulla protezione dei dati	 FedRAMP Programma federale di gestione dei rischi e delle autorizzazioni	 Pci Payment Card Industry (PCI) Data Security Standards (DSS)
 CSA Star Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR)	 IRAP Australia Australia Information Security Registered Assessors Program (IRAP)	 MTCS Singapore Multi-Tier Cloud Security (MTCS) Singapore Standard	 Spagna ENS Spagna Esquema Nacional de Seguridad (ENS)	

Report, white paper e artefatti

 BCP e ripristino di emergenza Continuità aziendale e ripristino di emergenza	 Test di penetrazione e valutazioni della sicurezza Attestazione di test di penetrazione e valutazioni di sicurezza condotte da terze parti	 Privacy e protezione dei dati Risorse per la privacy e la protezione dei dati	 Domande frequenti e white paper White paper e risposte alle domande frequenti	 Risorse di intelligenza artificiale Risorse che descrivono l'approccio alla conformità, alla sicurezza e alla privacy nelle soluzioni di intelligenza artificiale, ad esempio Copilot e 'Azure' Open AI
--	--	---	---	---

Settore e risorse regionali

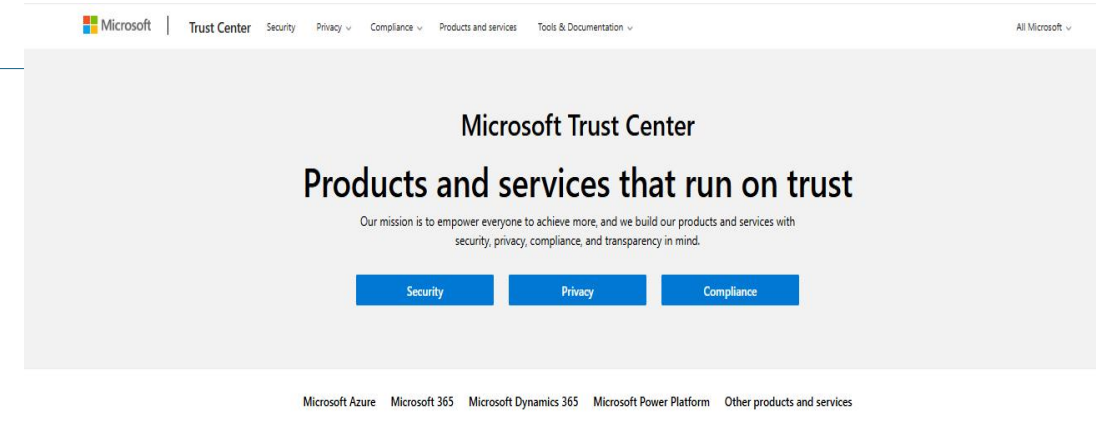
 Servizi finanziari Risorse che elaborano le linee guida per la conformità alle normative per FSI (per paese)	 Sanità e scienze della vita Funzionalità offerte da Microsoft per il settore sanitario	 Media e intrattenimento Risorse del settore multimediale e dell'intrattenimento	 Stati Uniti governo Risorse esclusivamente per i clienti del governo degli Stati Uniti	 Risorse a livello di area Documenti che descrivono la conformità dei MicrosoftServizi online con varie politiche e normative regionali
--	--	---	--	--

Microsoft Trust Center

Central hub for security and compliance. A go-to resource offering transparent insights into Microsoft's practices on **security, privacy and regulatory compliance**.

KEY FEATURES

- Data Privacy and Transparency
- Certification & Compliance documentation
- Regulatory Trust and Confidence



Our mission is to make the world
safer for **everyone**

