Microsoft

When things go wrong

Lesley Kipling
Lead Investigator *(former)*
Chief Security Advisor

To be prepared *against* surprise is to be trained.

To be prepared *for* surprise is to be educated.

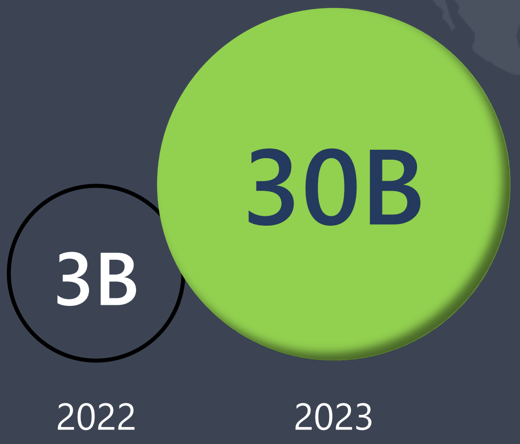
James Carse

Cybersecurity is an infinite game

We live in the most complex threat landscape in history

Speed, scale, and sophistication of attacks

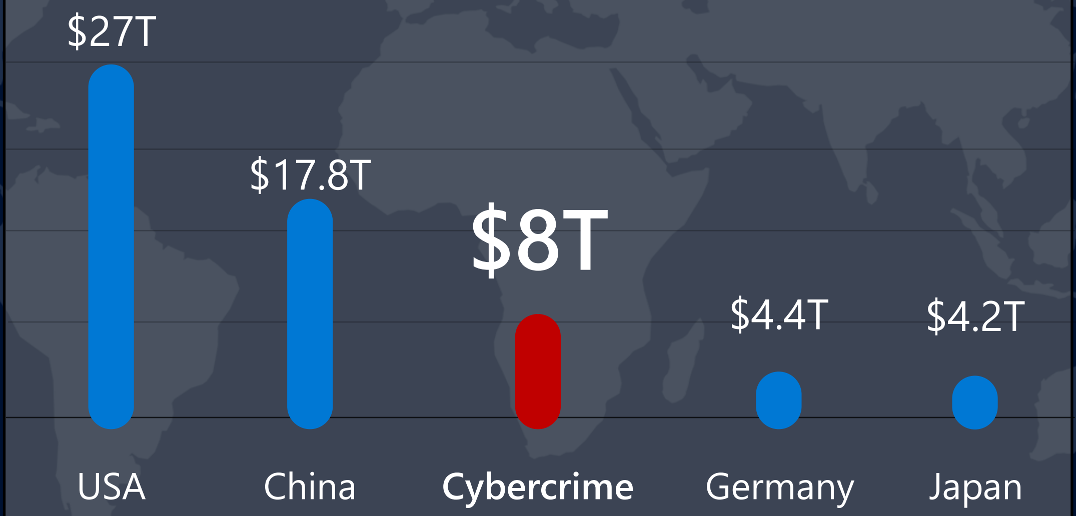
Password attacks per month



Source: Microsoft

Rapidly growing cyber economy

Annual GDP



Source: Statistica

Growing regulatory environment

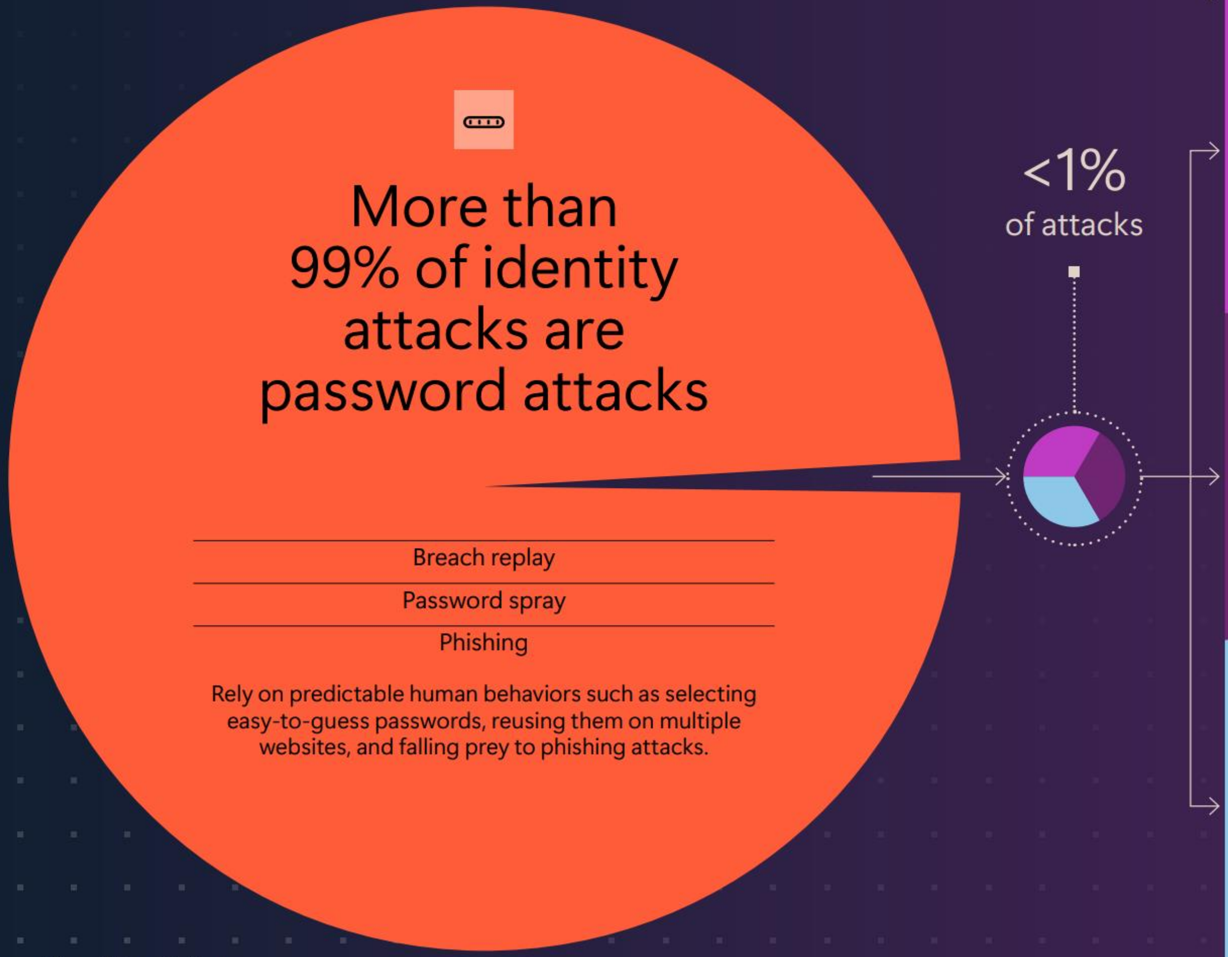
250

new regulatory updates tracked every day

Source: Microsoft

Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.



More than 99% of identity attacks are password attacks

Breach replay

Password spray

Phishing

Rely on predictable human behaviors such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.

<1% of attacks

Less than 1% combined

MFA attacks

- SIM swapping
- MFA fatigue
- AitM

End-run MFA protection by intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve, and capturing first and second factor credentials using fake replicas of legitimate websites.

Post-authentication attacks

- Token theft
- Consent phishing

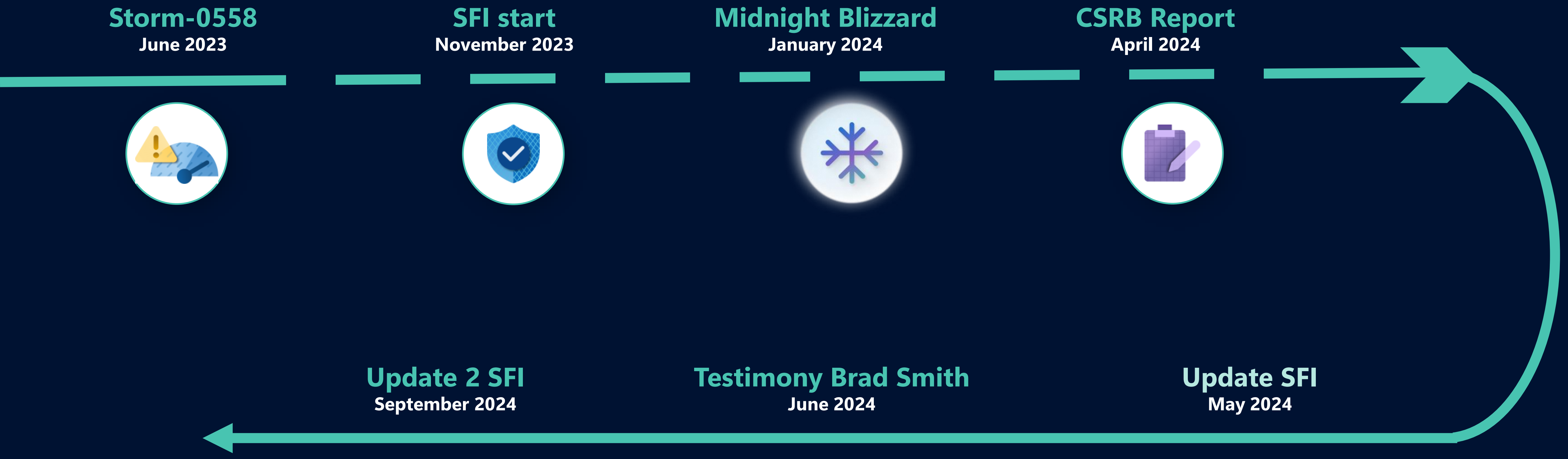
Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated user into granting permissions to malicious apps.

Infrastructure compromise

Often silently executed by professional groups or nation-state-backed threat actors with sophisticated operations, making them very hard to detect. Threat actors may compromise an on-premises federation server and copy its private signing key to forge tokens, compromise a privileged cloud user and add new federation contracts, or compromise a non-human workload identity and create new credentials with elevated privileges.

Source: Microsoft Threat Intelligence

THE SECURE FUTURE INITIATIVE TIMELINE



Storm-0558
June 2023

SFI start
November 2023

Midnight Blizzard
January 2024

CSRB Report
April 2024

Update SFI
May 2024

1st update on SFI progress. Satya Nadella: "Prioritizing security above all else“.

Testimony Brad Smith
June 2024

MSFT accepts responsibility and underscores additional steps MSFT is taking to ensure cyber security is company-wide effort.

Update 2 SFI
September 2024

25-page SFI progress report publicly published.

If you’re faced with the tradeoff between security and another priority, your answer is clear: **Do security**.

Satya Nadella

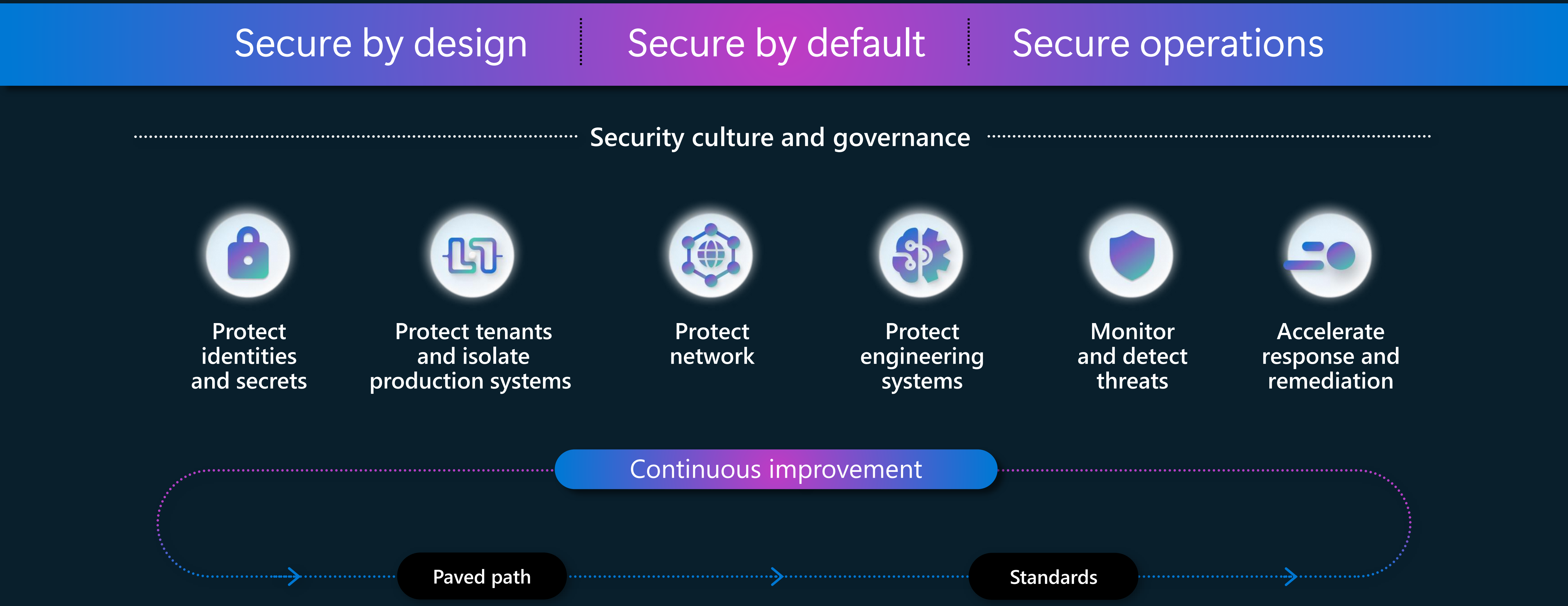
Microsoft Secure Future Initiative

A multi-year commitment to advance the way we design, build, test and operate our technology to ensure we deliver solutions that meet the highest possible standard of security in the new era of AI

The largest cybersecurity engineering project in history.

https://www.microsoft.com/en-gb/microsoft-cloud/resources/secure-future-initiative

Secure Future Initiative (SFI)



Secure by design

Secure by default

Secure operations

Security culture and governance

Protect identities and secrets

Protect tenants and isolate production systems

Protect network

Protect engineering systems

Monitor and detect threats

Accelerate response and remediation

Continuous improvement

Paved path

Standards

And we are making progress

98% credentials rotated

5.7 million aged tenants removed

1M accounts have MFA by default

730K SFI non-compliant apps eliminated

270K employees and vendors have enhanced MFA with additional security layers

Proactive Threat Hunting: Identification and Removal of Bad Actors

1M customers

120 countries

Continuous innovation

$20B of investment

100,000+ domains removed

10,000+ security and threat intelligence experts

15,000+ Partners in our security ecosystem

4,000 Identity attacks blocked per second

300+ threat actors tracked

135 million Manages devices

78 trillion signals synthesized daily

The Reality

We live in the gap between our aspired security policies and our lived security hygiene

AI maintained

We need a/n knowledge graph of the estate

Autonomous

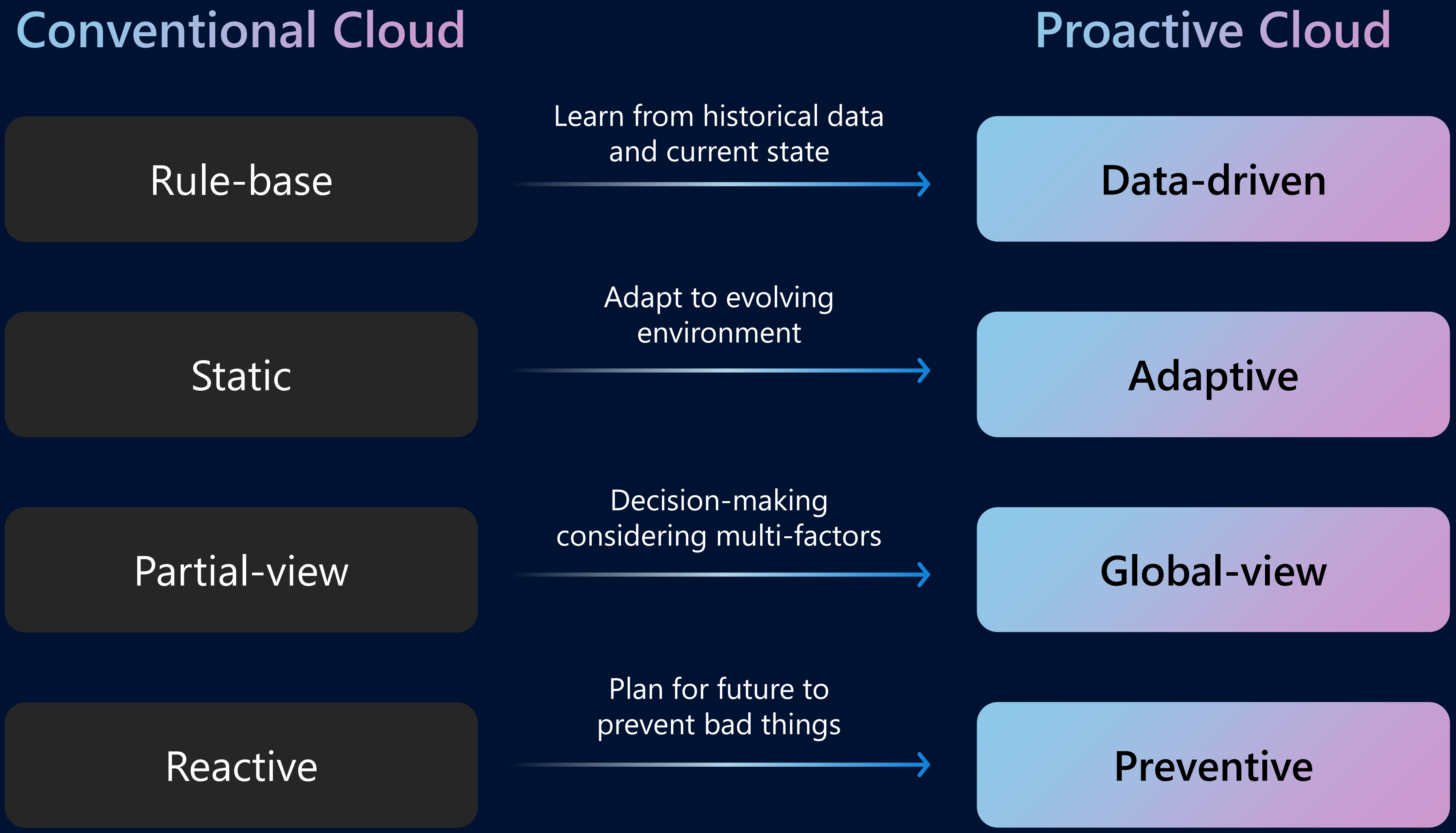
We need risk-aware personalized security hygiene …at scale

Autonomous

We need real-time
coordinated defense
...at scale

The future of cybersecurity requires a fundamental shift of mindset

Paradigm shift



Conventional Cloud

Proactive Cloud

Rule-base → Data-driven: Learn from historical data and current state

Static → Adaptive: Adapt to evolving environment

Partial-view → Global-view: Decision-making considering multi-factors

Reactive → Preventive: Plan for future to prevent bad things

collective defence

Strength in numbers

Thank you!