



Welcome to BlueHat Shanghai

Eric Doerr

General Manager, Microsoft Security Response Center

@edoerr

May 30, 2019

Chinese researchers were the most prolific and high-impact contributors to the Microsoft Bounty Program in 2019

Growth

2018 vs 2019



57%
**China-based
bounty
participants**

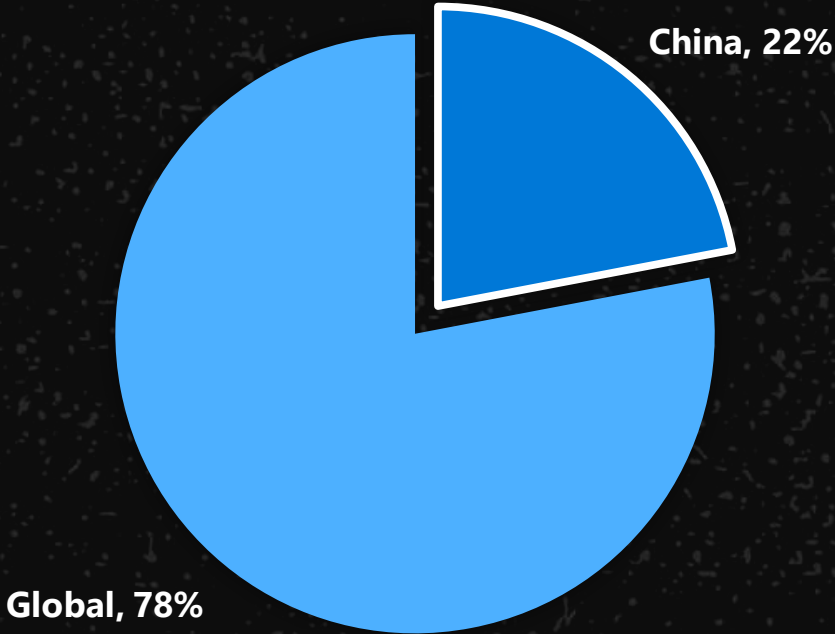


46%
**China-based
bounty
submissions**

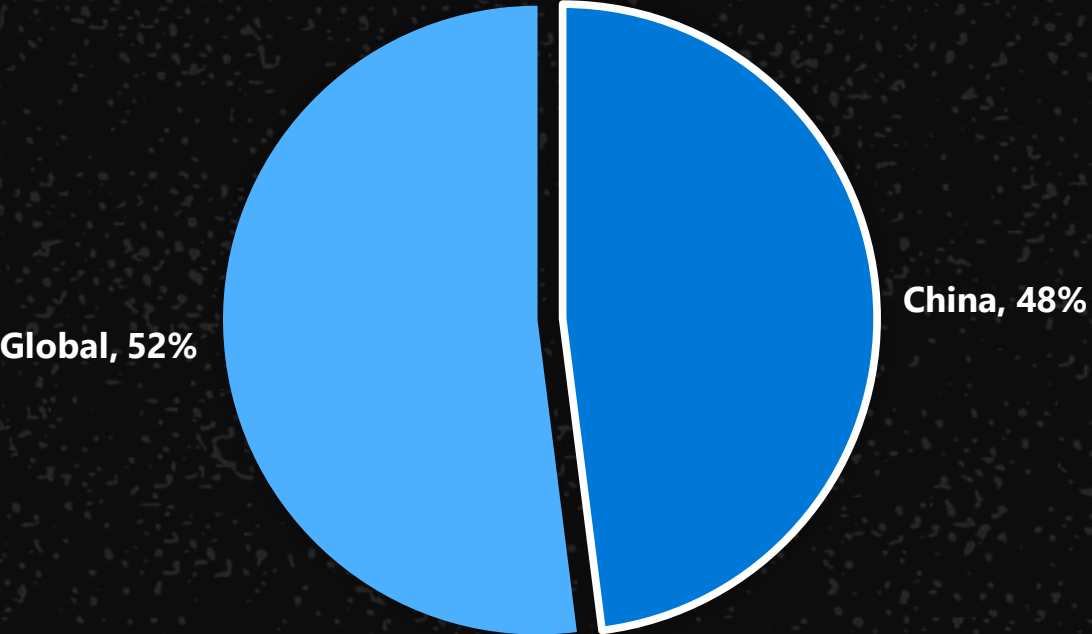
Impact

2018 vs 2019

BOUNTY-ELIGIBLE SUBMISSIONS



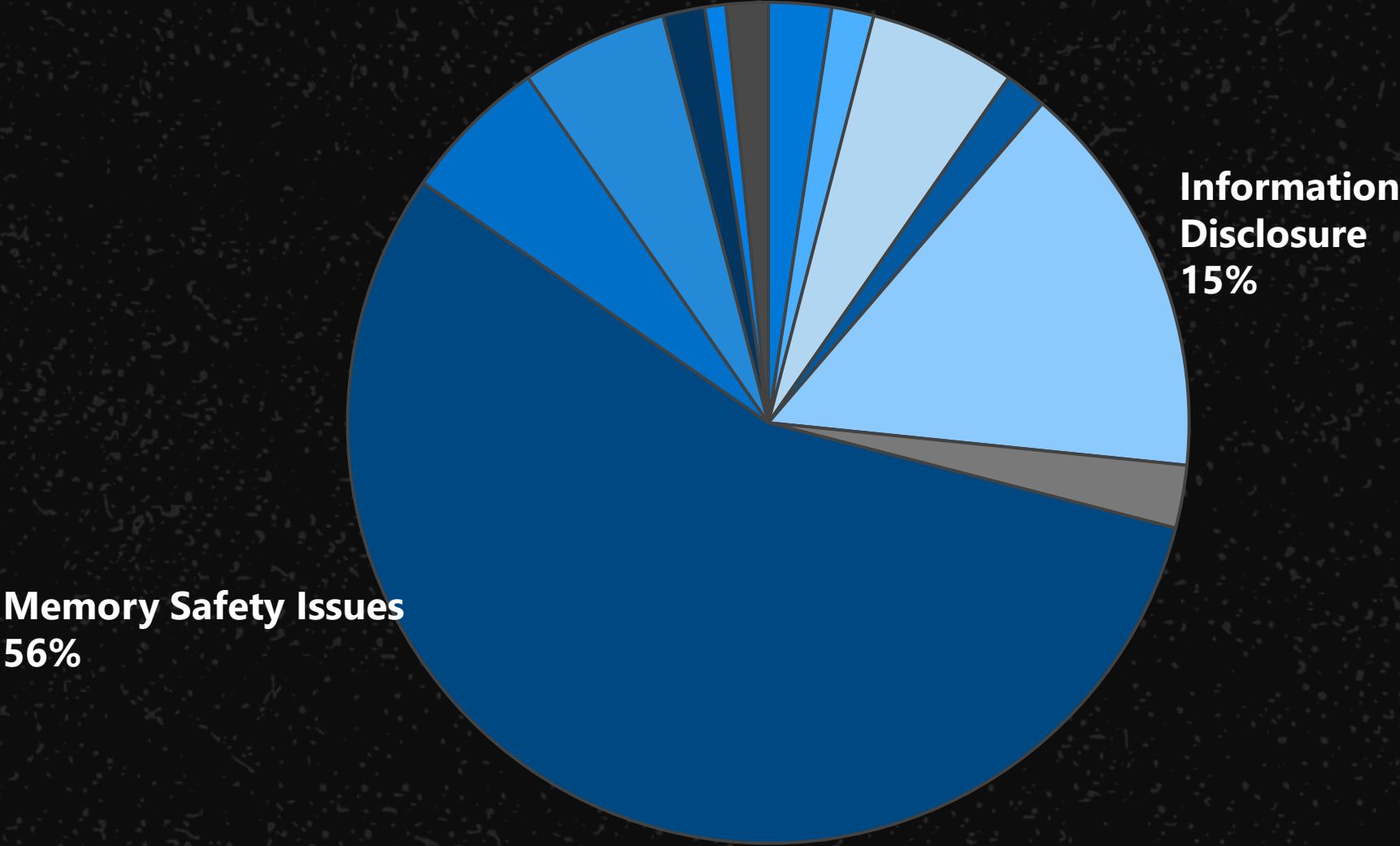
BOUNTY AWARDS



Focus

2019

Submissions by Vulnerability Type



Microsoft Bounty Programs

Microsoft Office
Insider

Microsoft
.NET Core and
ASP.Net Core

Microsoft Edge

Azure DevOps

Microsoft Cloud
Bounty

Windows Defender
Application Guard

Windows Insider
Preview

Microsoft
Identity

Mitigation Bypass
and Defense

Microsoft Hyper-V

Microsoft Bounty Programs

Microsoft Office
Insider

Microsoft
.NET Core and
ASP.Net Core

Microsoft Edge
**+75% of
submissions**

Azure DevOps

Microsoft Cloud
Bounty

Windows Defender
Application Guard

Windows Insider
Preview
**+40% of
submissions**

Microsoft
Identity

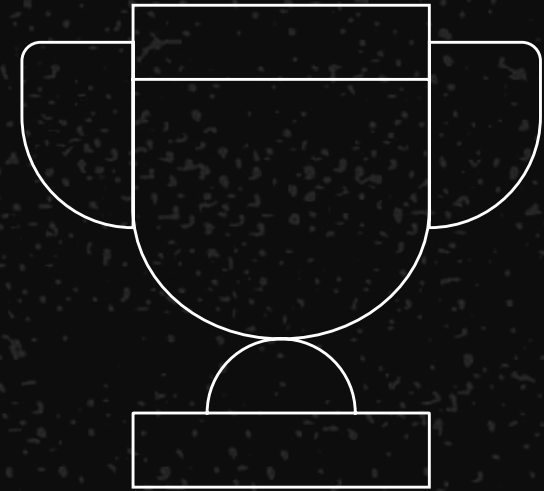
Mitigation Bypass
and Defense

Microsoft Hyper-V
**+50% of
submissions**



Our thanks

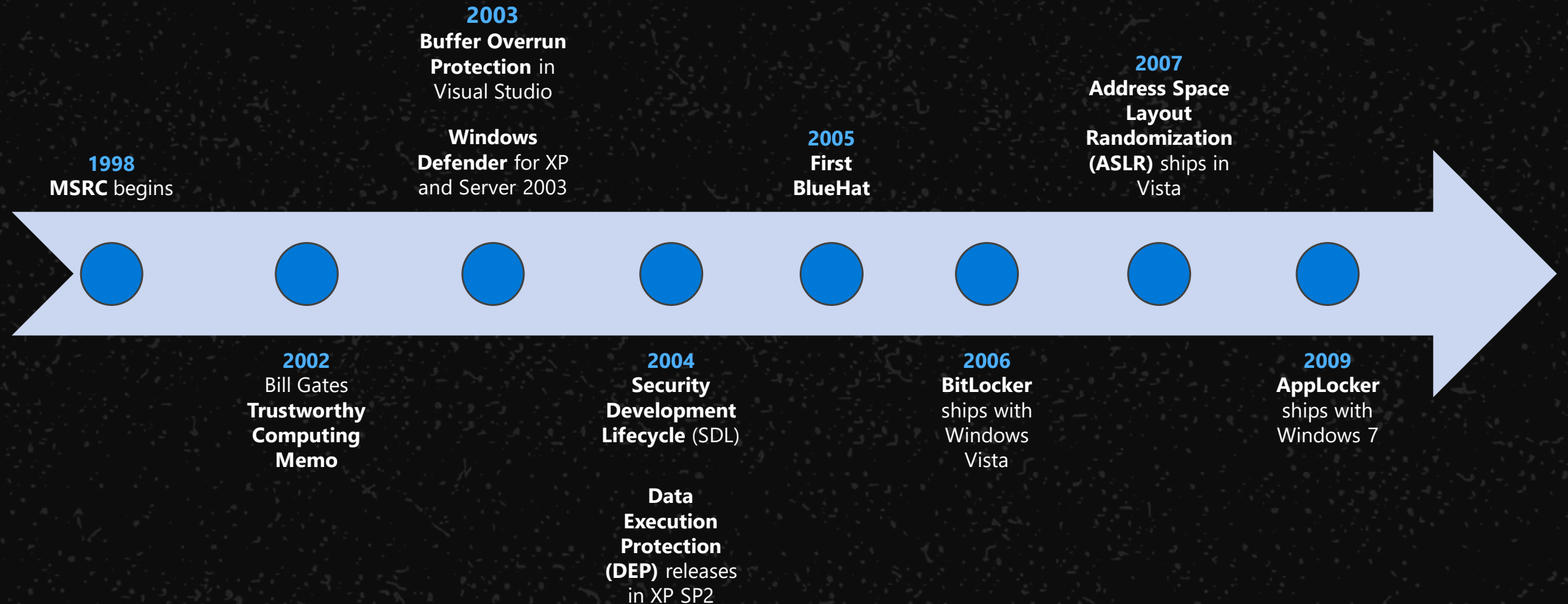
China-based researchers and partner companies have demonstrated their skill and helped us secure customers and the broader ecosystem in 2019.



A little history...

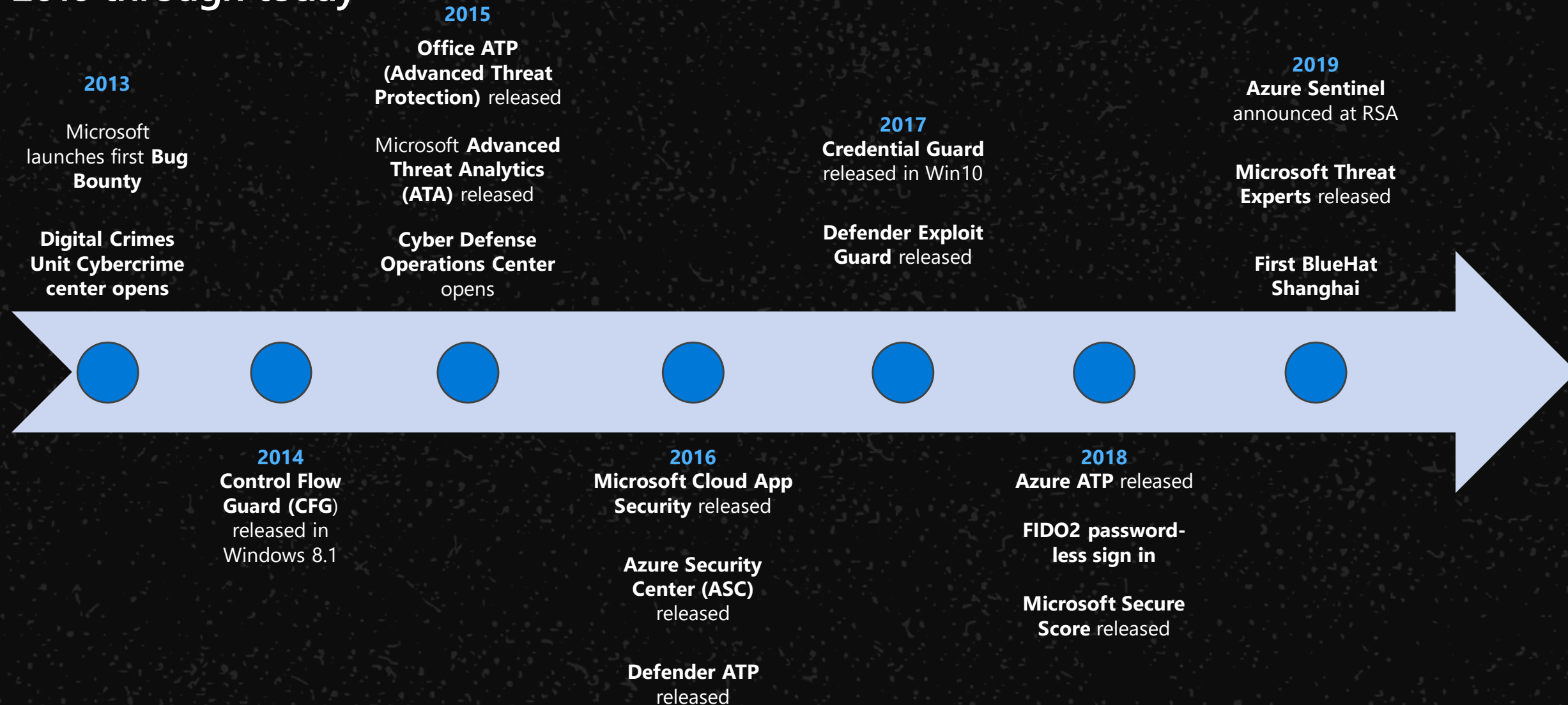
Long history of security investment

90's through 2010



Long history of security investment

2010 through today



CVE-2019-0708 example

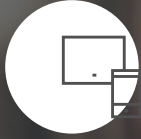
Security focus paid off with newer versions of Windows

The screenshot shows the Microsoft MSRC website. At the top, there is a navigation bar with the Microsoft logo, 'MSRC', and links for 'Report an issue', 'Customer guidance', 'Engage', 'Who we are', and 'Blogs'. Below this, the page title is 'CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability' under the 'Security Vulnerability' category. It is published on 05/14/2019 and references MITRE CVE-2019-0708. A news article snippet is overlaid on the page, titled '14 Microsoft Patches 'Wormable' Flaw in Windows XP, 7 and Windows 2003' dated MAY 19. The article text states: 'Microsoft today is taking the unusual step of releasing security updates for unsupported but still widely-used Windows operating systems like XP and Windows 2003, citing the discovery of a "wormable" flaw that the company says could be used to fuel a fast-moving malware threat like the WannaCry ransomware attacks of 2017.' Below the article is a world map with North and South America highlighted in red. A callout box over the map says 'Prevent a worm by updating Remote Desktop Services (CVE-2019-0708)'. At the bottom of the callout, it says 'MSRC Team May 14, 2019' and includes social sharing buttons for Facebook (1.6K shares), Twitter (0), LinkedIn (0), and a comment icon (0). The article text continues: 'Today Microsoft released fixes for a critical Remote Code Execution vulnerability, CVE-2019-0708, in Remote Desktop Services – formerly known as Terminal Services – that affects some older versions of Windows. The Remote Desktop Protocol (RDP) itself is not vulnerable. This vulnerability is pre-authentication and requires no user interaction. In other words, the vulnerability is 'wormable'.'

- Vulnerability: Pre-auth UAF (Use After Free) in RDP Server
- Win8, Server 2012, Win10 not affected
- Released patches for "out of support" XP, Win7 and Server 2003

Microsoft Future

Going Digital



1 million/hour
new devices
coming online
by 2020

12 years
average age of S&P
500 corporations
by 2020
50% of S&P 500
replaced by 2026

Every
Organization
is becoming a software
company to stay
relevant

60% computing
in the cloud by
2025



The Microsoft Cloud

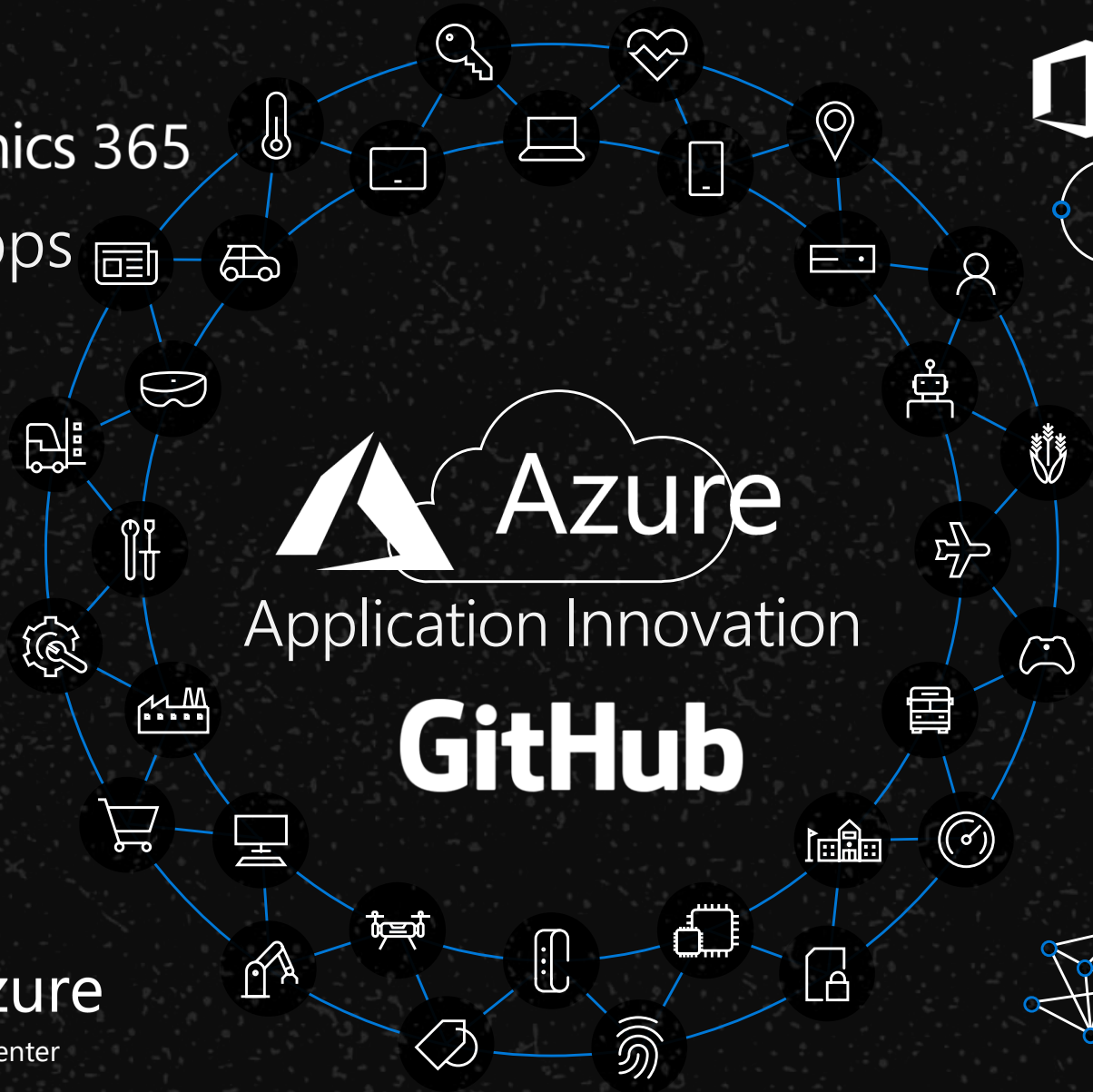
Microsoft Dynamics 365
Business Apps

Office 365
Productivity

Windows Defender
Advanced Threat Protection
Security & Management

Azure
Advanced Threat Protection

Azure
Security Center



Power BI

Data

Cognitive Services

Machine Learning

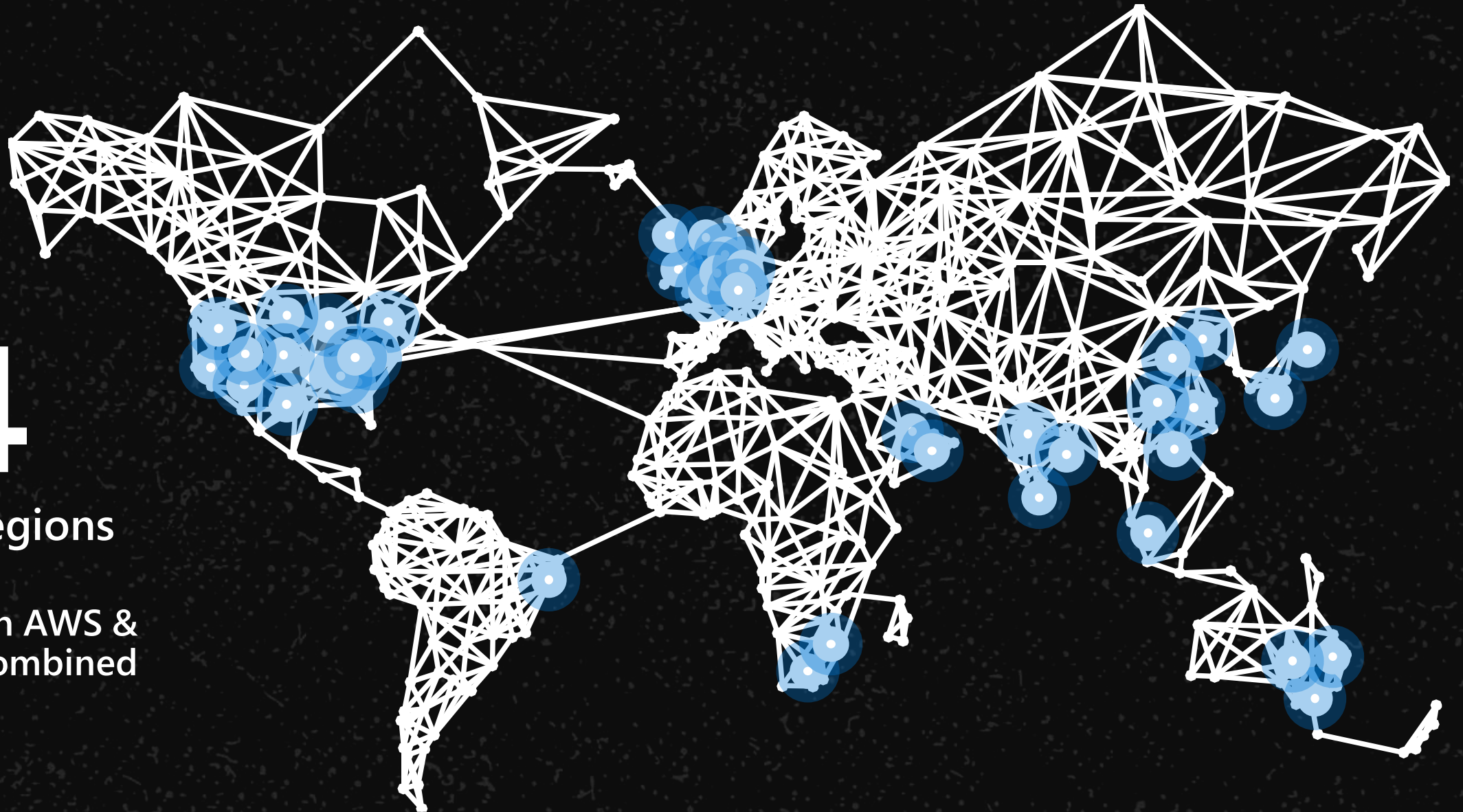
AI & Machine Learning

Azure: Planetary Scale

54

Azure regions

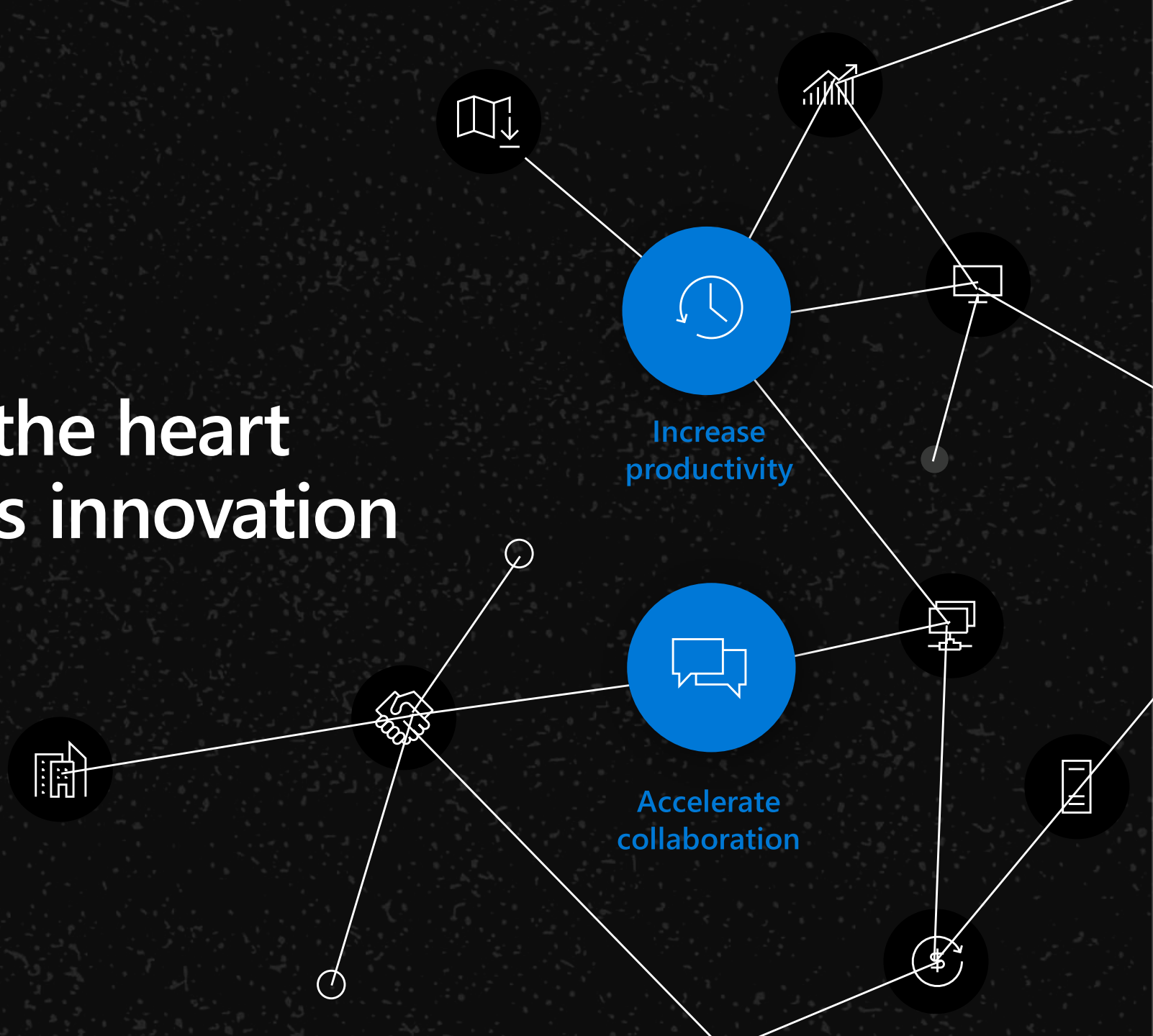
More than AWS &
Google combined



>95% of Fortune 500 use Azure

Developers are at the heart
of every company's innovation





The #1 Developer platform on the planet

Most contributions 1.1B in 2018

Most developers 36M

Highest growth 8M new devs in 2018

Most Repos 96M

Most activity 200M PRs, 800M API requests daily

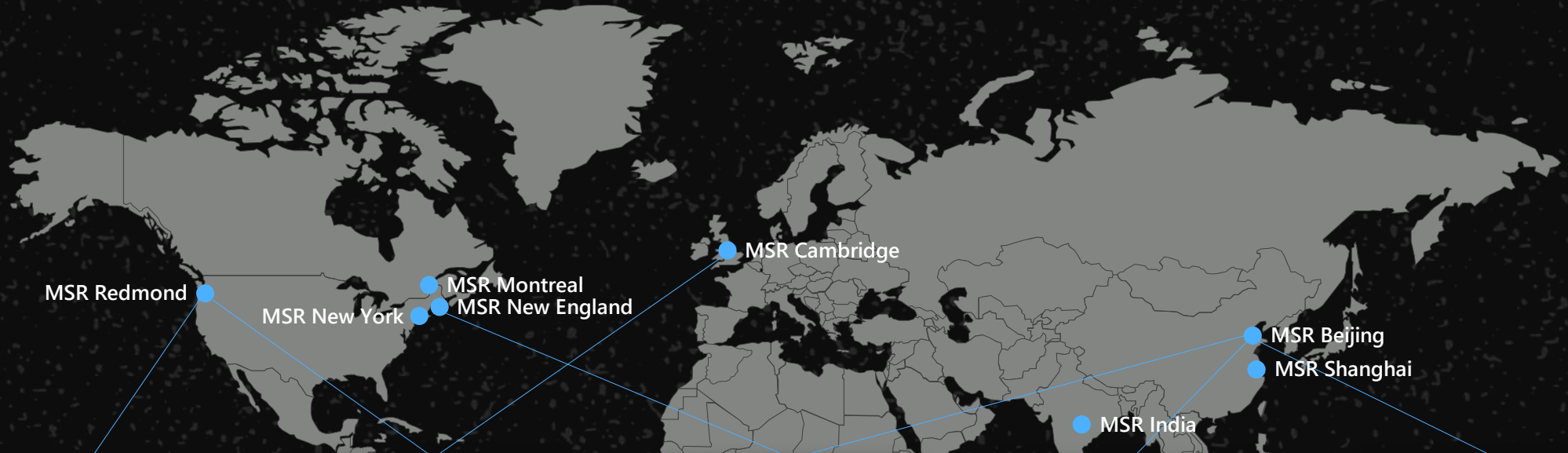
Most students 1.1M

Most organizations 2.2M

Most secure 5M vulnerability alerts in 2018


Azure AI

Fueled by Microsoft breakthrough research



First FPGA deployed in a datacenter

39.5 Teraflops with Intel Stratix 10




Speech recognition human parity

94.9% on Switchboard test




Machine translation human parity

69.9% with MT Research system



Conversational Q&A human parity

89.4% on Stanford CoQA test



Object detection human parity

96% on RESNET vision test

Bounty

Microsoft Office
Insider

Microsoft
.NET Core and
ASP.Net Core

Microsoft Edge

Azure DevOps

Microsoft Cloud
Bounty

Windows Defender
Application Guard

Windows Insider
Preview

Microsoft
Identity

Mitigation Bypass
and Defense

Microsoft Hyper-V

Bounty -> Where we are going

Microsoft Office Insider	Microsoft .NET Core and ASP.Net Core	Microsoft Edge	Azure DevOps
Microsoft Cloud Bounty	Windows Defender Application Guard	Windows Insider Preview	Microsoft Identity
	Mitigation Bypass and Defense	Microsoft Hyper-V	

Azure

Dynamics

DevOps / GitHub

AI & ML

And a whole lot more...

This journey would not be possible without our partnership, now and in the future.

谢谢

Thank You