



欢迎参加 BlueHat Shanghai

Eric Doerr

微软安全响应中心总经理

@edoerr

May 30, 2019

**2019 年，中国的安全研究员是微软漏洞赏金
计划中成果最多，影响力最大的贡献者**

增长

2018 vs 2019



57%

来自中国的漏洞赏金计划参与者



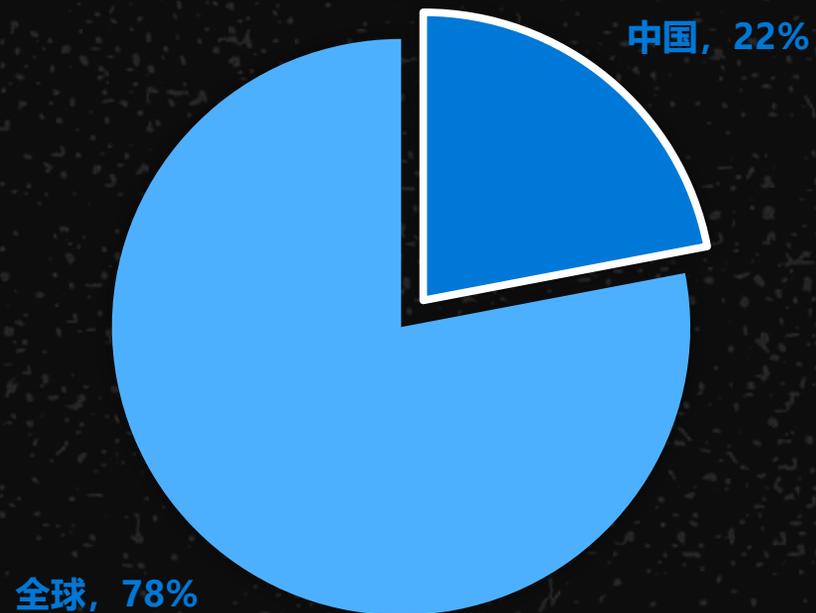
46%

来自中国的漏洞赏金计划提交成果

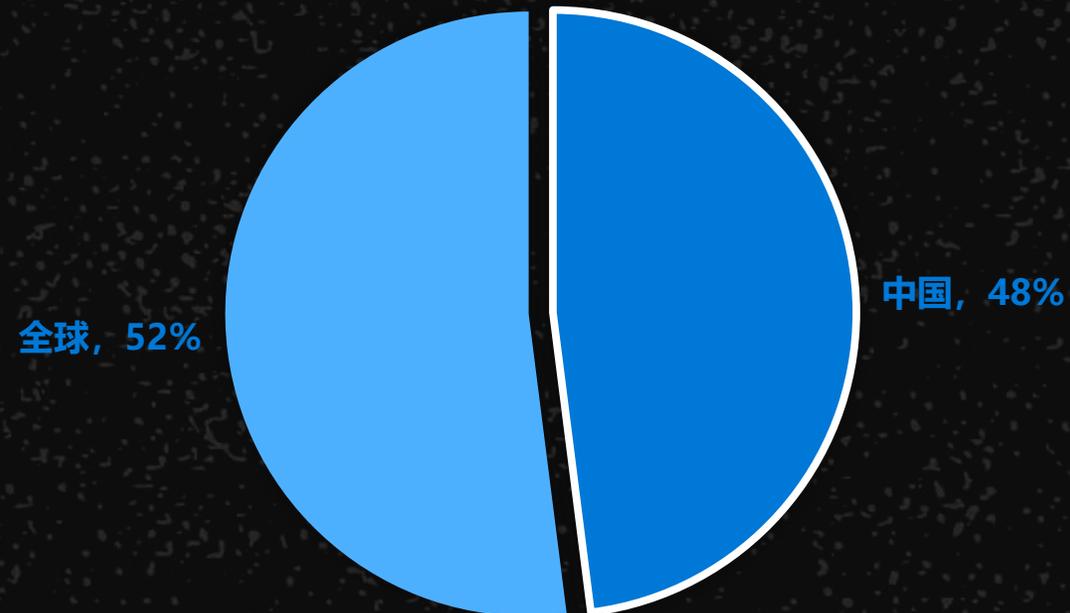
影响力

2018 vs 2019

符合漏洞赏金计划要求的提交



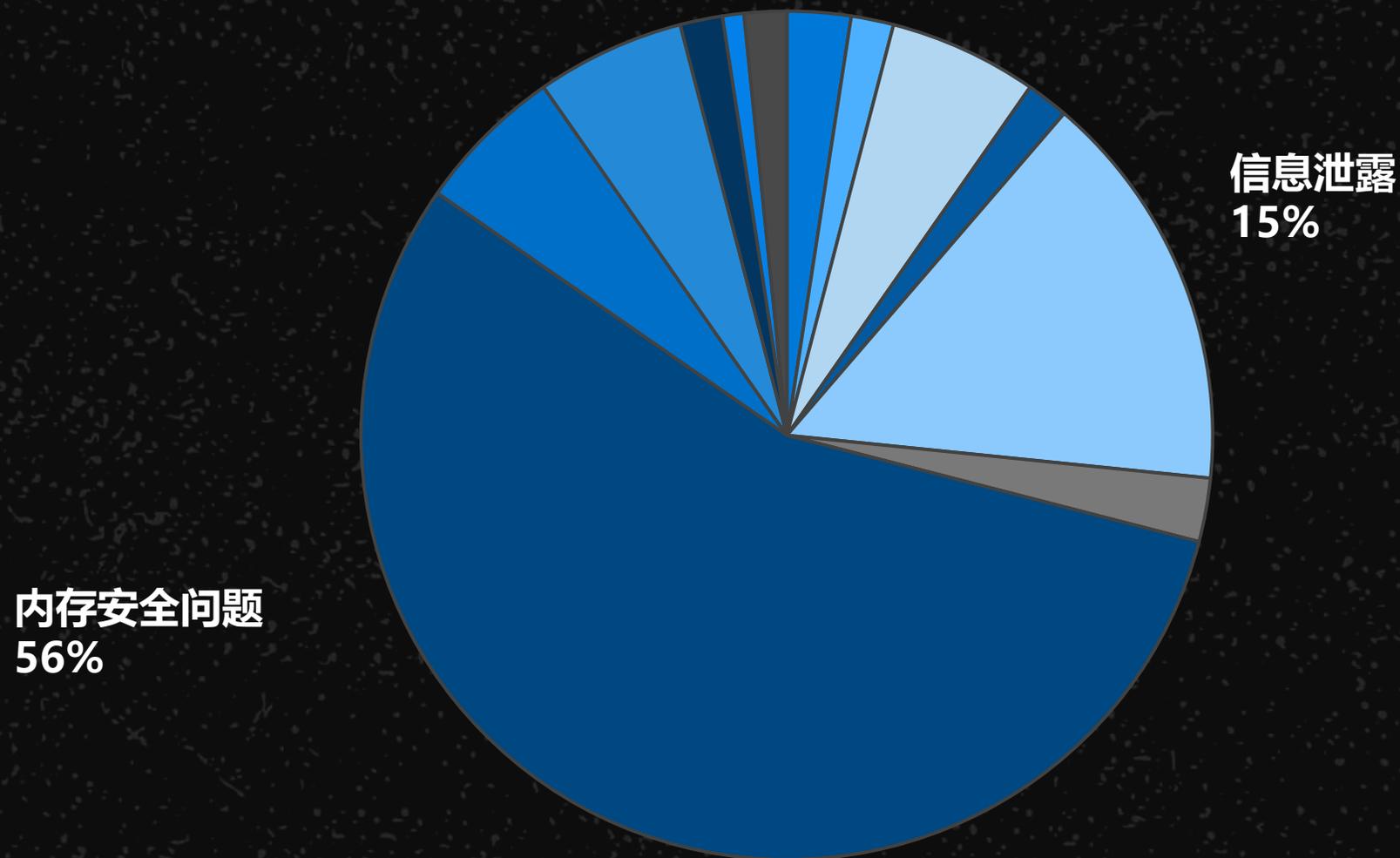
漏洞赏金计划奖金



侧重点

2019

所提交漏洞类型的划分



微软漏洞赏金计划

Microsoft Office
Insider

Microsoft
.NET Core 和
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

微软漏洞赏金计划

Microsoft Office
Insider

Microsoft
.NET Core 和
ASP.Net Core

Microsoft Edge
提交数增加 75%

Azure DevOps

Microsoft Cloud
Bounty

Windows
Defender
Application Guard

Windows Insider
Preview
提交数增加 40%

Microsoft
Identity

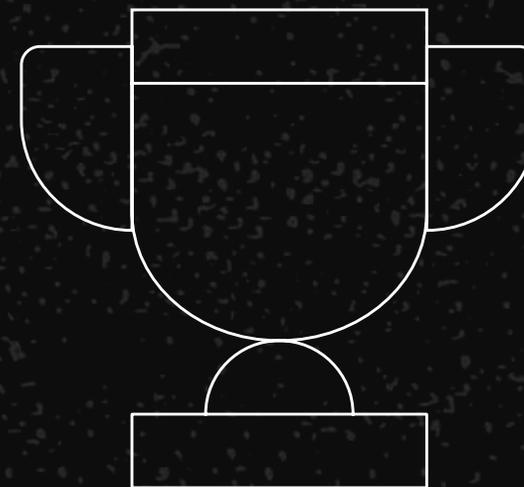
Mitigation Bypass
and Defense

Microsoft Hyper-V
提交数增加 50%



致谢

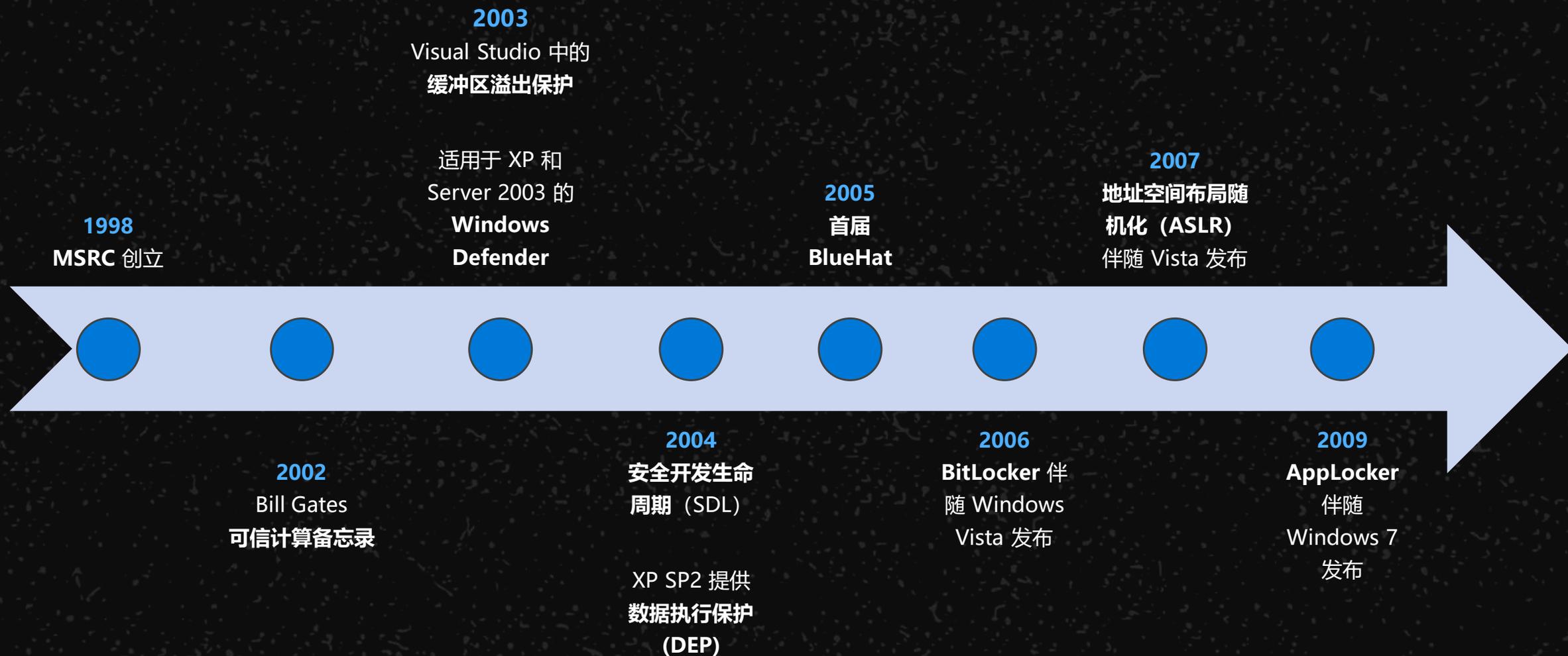
来自中国的安全研究人员和合作公司已经证明了自己的技术实力，帮助我们一起在 2019 保护广大的用户和整个安全生态圈。



一些历史回顾.....

围绕安全投入的漫长历史

90 年代至 2010 年



围绕安全投入的漫长历史

2010 年至今

2013

微软发起
首个漏洞
赏金计划

数字安全
中心成立

2015

Office ATP
(高级威胁防
护) 发布

微软高级威胁
分析 (ATA)
发布

网络防御运营
中心成立

2017

Credenti
al Guard
伴随 Win
10 发布

Defender
Exploit
Guard 发
布

2019

Azure
Sentinel 在
RSA 发布

Microsoft
Threat
Experts 发布

首届 BlueHat
Shanghai

2014

控制流防
护 (CFG)
伴随
Window
s 8.1 发
布

2016

微软云应用安
全服务 发布

Azure 安全
中心 (ASC)
发布

Defender
ATP 发布

2018

Azure ATP
发布

FIDO2 免密
码登录

Microsoft
Secure
Score 发布

CVE-2019-0708 范例

对安全的关注和投入在新版 Windows 中获得了回报

Microsoft | MSRC Report an issue Customer guidance Engage Who we are Blogs All Micrc

Security Update Guide > Details

CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability

Security Vulnerability

Published: 05/14/2019
MITRE CVE-2019-0708

14 Microsoft Patches 'Wormable' Flaw in Windows XP, 7 and Windows 2003

MAY 19

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.

Prevent a worm by updating Remote Desktop Services (CVE-2019-0708)

MSRC Team May 14, 2019

Rate this article ★★★★★

Share 1.6K 0 0 0

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’.

漏洞：远程显示协议中的身份验证前 UAF (Use After Free)

Win8、Server 2012、Win10 不受影响

为“结束支持”的 XP、Win7 和 Server 2003 发布了补丁

微软的未来

变得数字化



1 百万/小时
到 2020 年，新设备的上线速度

到 2020 年时，标准普尔 500 公司的平均年龄会达到
12 岁

50% 的标普 500 公司将在 2026 年被取代

为了不落后于时代，
每个组织都必须成为软件公司

60% 计算能力
到 2025 年将通过云平台提供



微软云

 Microsoft Dynamics 365
业务应用

 Office 365
生产力

 Power BI

 数据

 认知服务

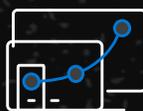
 机器学习

 人工智能和机器学习

 Azure
应用程序创新

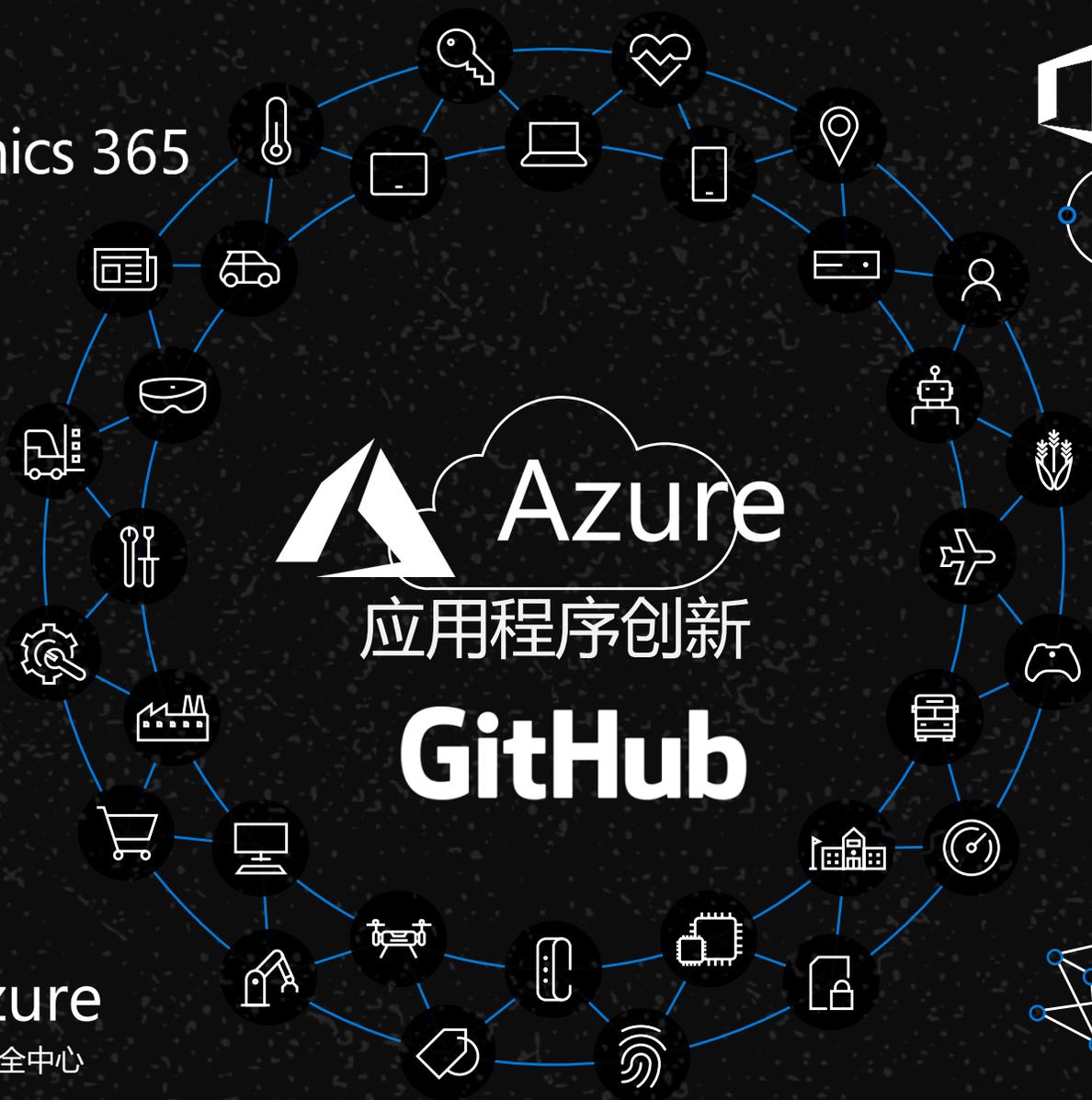
 GitHub

 Windows Defender
Advanced Threat Protection

 安全和管理

 Azure
高级威胁防护

 Azure
安全中心

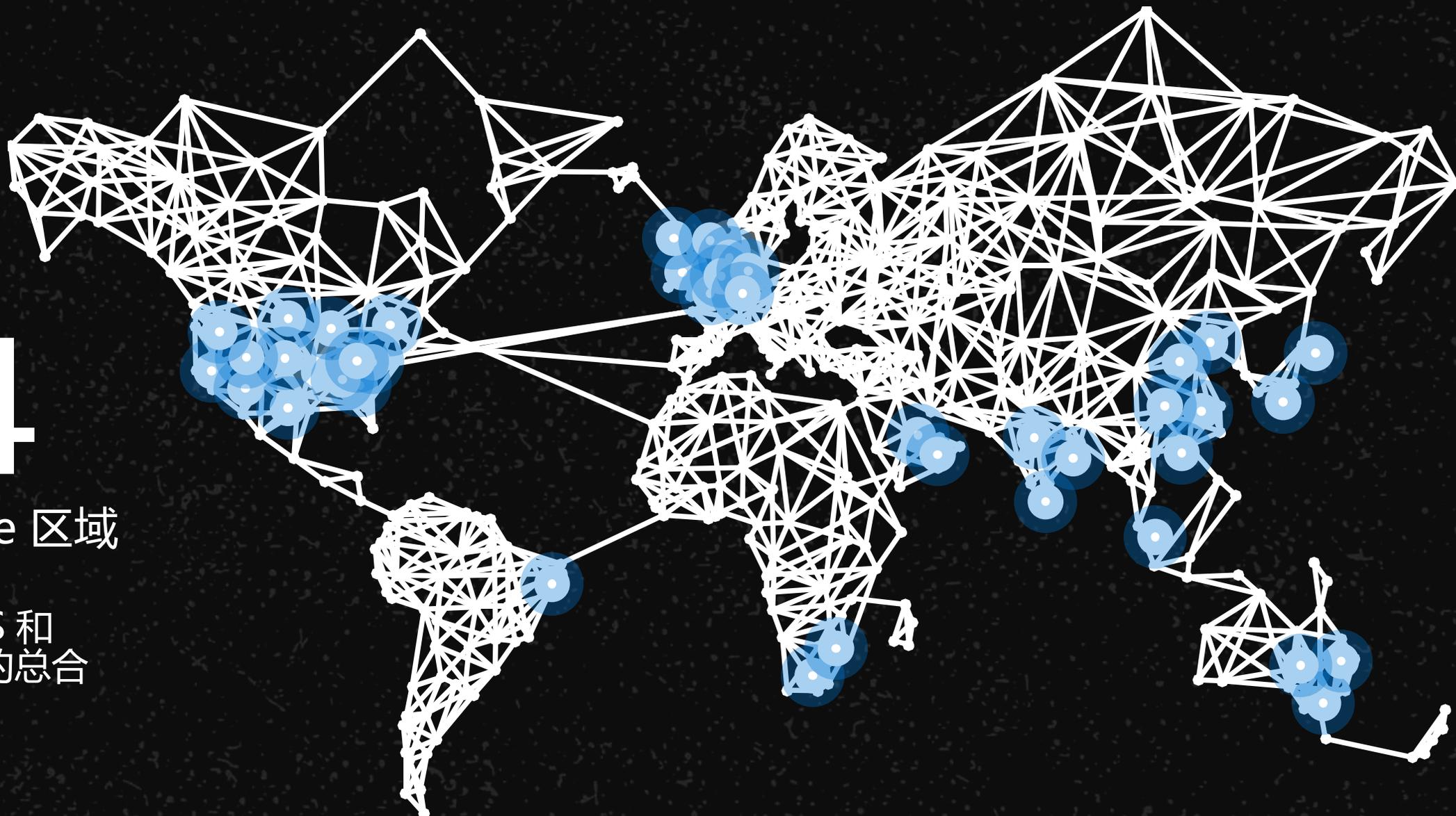


Azure: 全球规模

54

个 Azure 区域

超过 AWS 和
Google 的总合



超过95% 的世界500强公司使用 Azure

开发者是每个公司业务创新的核心





全球第一的开发者平台

最多贡献者 2018 年 11 亿人

最多开发者 3600 万人

增速最快 2018 年新增开发者 800 万人

最多代码库 9600 万个

最活跃 每天 2 亿 Pull 请求, 8 亿 API 请求

最多学生 110 万人

最多组织 220 万个

最安全 2018 年 500 万个弱点警报

Azure AI

由微软突破性的研发成果推动前进

MSR 雷德蒙德

MSR 蒙特利尔
MSR 纽约
MSR 新英格兰

MSR 剑桥

MSR 印度

MSR 北京
MSR 上海



首次将 FPGA 部署到数
据中心

配合 Intel Stratix
10 实现 39.5
Teraflops



近似于人类的语音识别
能力

Switchboard 测试
94.9%



近似于人类的机器翻译
能力

MT Research 系统
69.9%



近似于人类的对话问
答能力

Stanford CoQA 测试
89.4%



近似于人类的对象检
测能力

RESNET 视觉测试
96%

Bounty

Microsoft Office
Insider

Microsoft
.NET Core 和
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 -> 我们的方向

Microsoft Office Insider	Microsoft .NET Core 和 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	

以及更多的.....

Azure

Dynamics

DevOps / GitHub

AI & ML

无论现在亦或将来，在这段旅途
上我们需要与所有的这些合作伙
伴一起前行。

谢谢

Thank You