Cybersecurity och molnet

Daniel Akenine | Microsoft

Kort om mig

- Teknik och säkerhetschef Microsoft
- Ordförande IASA – Sveriges IT arkitekter
- Ledamot i regeringens samordningsråd för säkerhet och integritet i smarta elnät.
- Ledamot i ISO's internationella expertgrupp för standarder inom cloud computing
- Ledamot i ledningsgruppen för Cloud Sweden samt EuroCloud.
- Undervisar på KTH

Vad blir konsekvensen av detta?

Antalet dagar i genomsnitt för ett intrång att upptäckas

Kostnad i genomsnitt för ett intrång

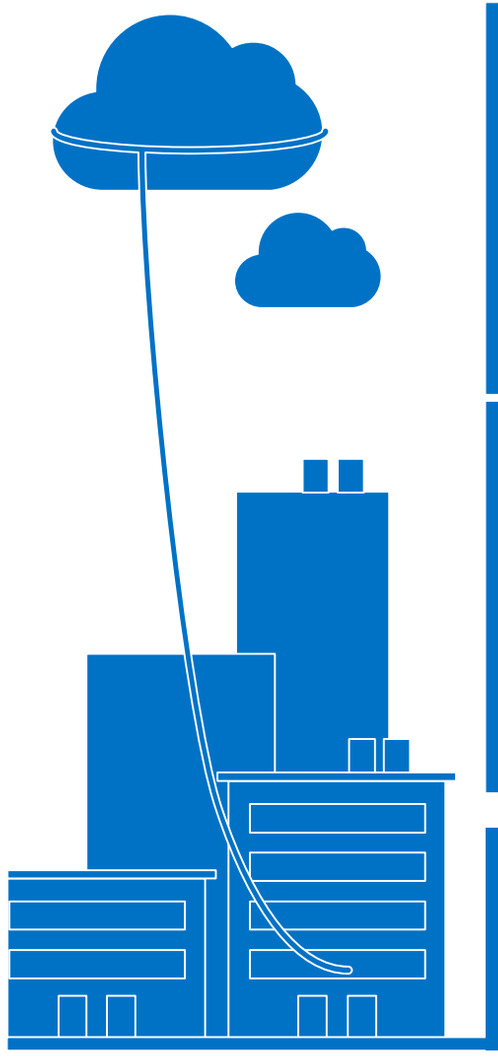
15 % ökning YoY

Säkerhet

fråga

Kostnad globalt kan vara så mycket som 20 000 miljarder SEK i förlorad produktivitet och tillväxt

Hur är Microsoft en del av detta?



14M+
Microsoft Azure AD autentiseringar i veckan

57%
Av Fortune 500 använder Microsoft Azure

1 miljon
Microsoft Azure SQL databaser

29K+
Organisationer använder Windows Intune

93%
av Fortune 1000 använder Active Directory

67%
Av världens servrar kör på Windows Server

45%
Av världens databaser körs på SQL Server

66%
Av våra kunder använder System Center

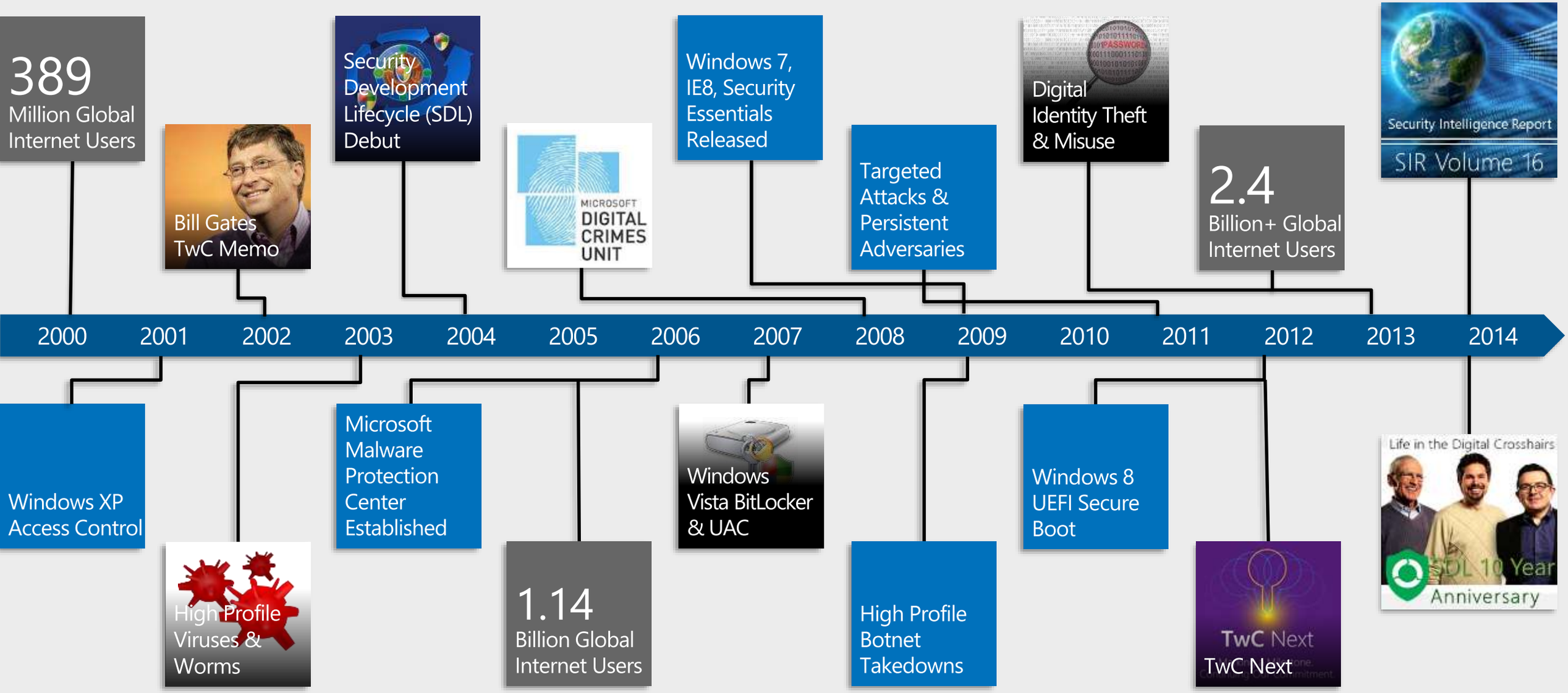
skype msn bing Office 365 Outlook XBOX LIVE Microsoft Dynamics CRM Online Microsoft Azure

Microsoft driftar en av de största molninfrastrukturerna i världen.

20 000 miljarder objekt lagrade i Azure

1 miljard Office användare, Office 365 är Microsoft snabbast växande produkt någonsin

En resa genom två årtionden av säkerhetshot



Låt oss fokusera på molnet och säkerhet en stund…

Vanliga frågor

SÄKERHET

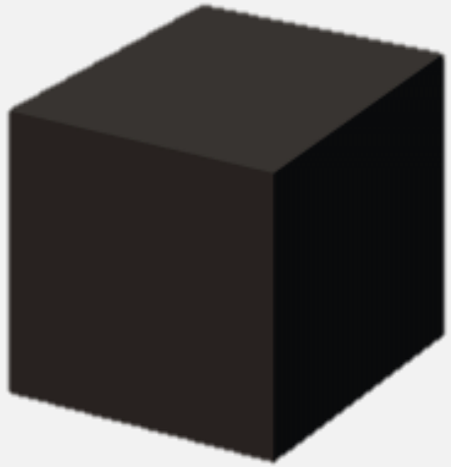
- Är molnet säkert?
- Är era molntjänster säkra?

PRIVACY

- Vad betyder integritet för Microsoft?
- Var finns mitt data ?

COMPLIANCE

- Vilka certifieringar och förmågor kan ni garantera?
- Hur stödjer Microsoft mitt behov kring regulatoriska krav ?
- Har jag rätt att utföra en audit av Microsofts datacenter?



1. Lova

2. Bevisa

Om att lova och bevisa i molnet

1. Följ säkerhetsstandarder (ISO 27001)
2. Revision och audit (SSAE 16)
3. Visa

Det var 1 minuts förklaringen…

Förtroende för teknik och IT.

Cybersecurity

Data Privacy

Compliance

Transparens

Microsoft och cybersecurity – 4 delar

1

Skapa säkra produkter och tjänster.

2

Håll våra kunders data säkra.

3

Hjälp kunder och partners att skydda sina tillgångar

4

Arbeta aktivt med att bekämpa cyberkriminalitet.

Skapa säkra produkter och tjänster.

Security Development Lifecycle (SDL)

Säkerhet vid planering, design, utveckling och installation

Operationell säkerhet

Säkerhet vid planering, design, utveckling och installation

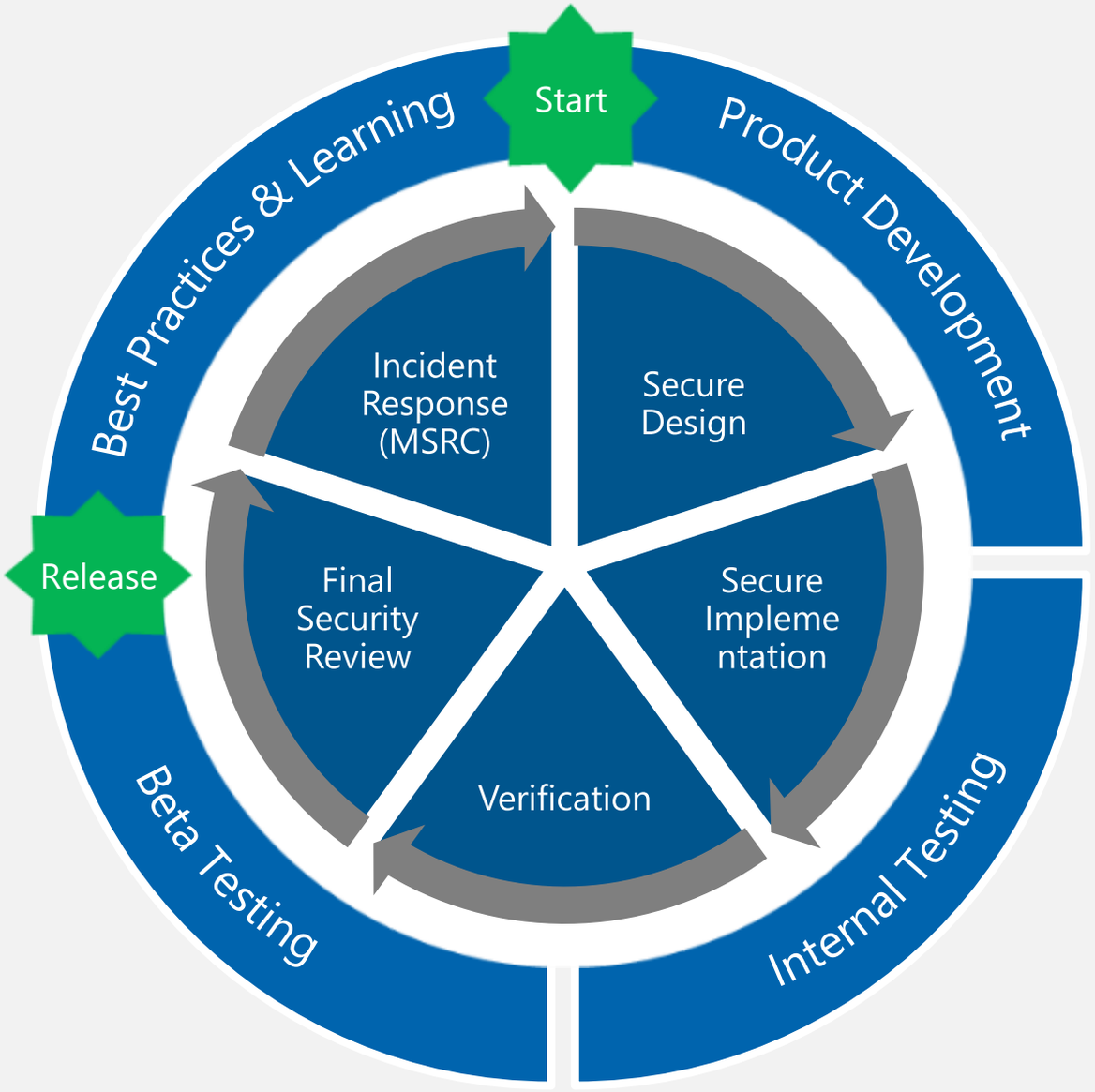
Förmoda intrång

Stränga åtgärder för att hindra, upptäcka, isolera och svara på hot

Incidentrespons

Global 24x7, incidentrespons för att minska effekterna vid en attack

Microsoft Security Development Lifecycle



Mål

Skydda Microsofts kunder genom att:

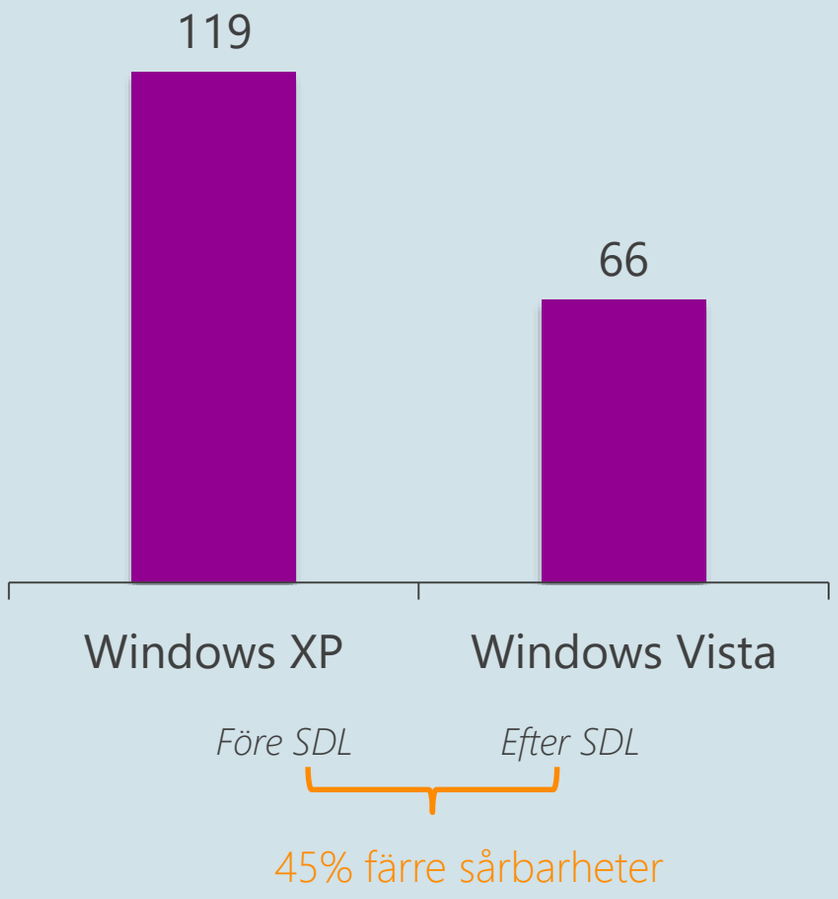
- Reducera **antalet** sårbarheter
- Reducera **konsekvenserna**

Principer

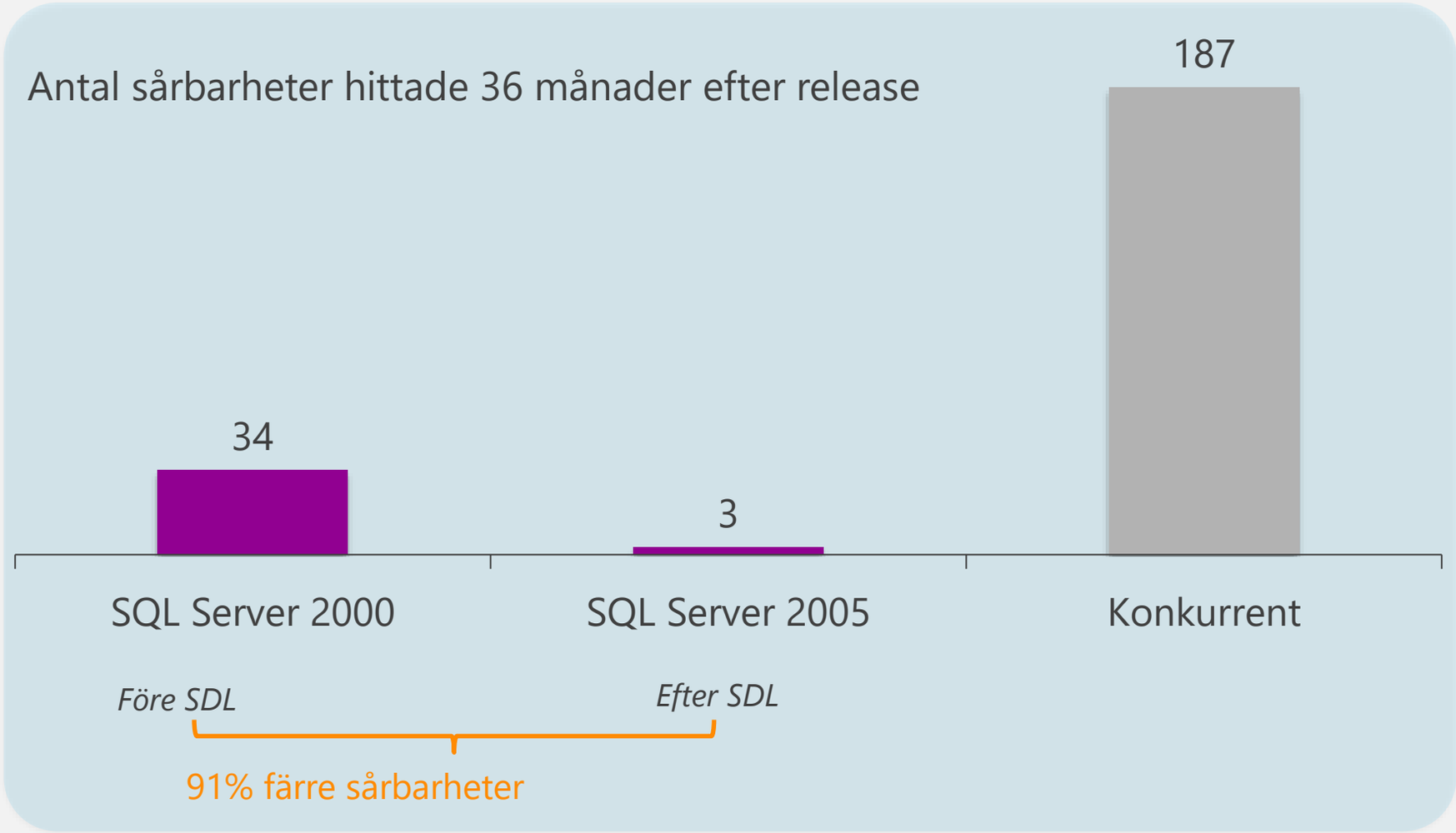
- Eliminera säkerhetsproblem tidigt
- “Secure by design”

Microsoft SDL och Windows

Antal sårbarheter hittade ett år efter release



Microsoft SDL och SQL Server



Operationell säkerhet (OSA)

Bevisad, skalbar metod

Kompletterar industristandarder

Internetbaserade hot

Kontinuerligt uppdaterad

Bygger på Microsoft erfarenheter av att drifta stora molntjänster.

http://aka.ms/OSA

Förmoda intrång

Förmoda intrång

Kriminella administratörer

APT (Advanced persistent Threats)

Icke-auktoriserade data förfrågningar

Hitta nya hot och förstå eventuella gap mot sitt eget system

Kör kontinuerliga säkerhetsprogram för att minska tiden till upptäckt och återskapande

Reducera exponering mot interna attacker

0-standing administrator rights – ingen enskild person har stående administrativa rättigheter

Microsoft Security Response Center (MSRC)

Best-in Class Security Response

Distribute timely and authoritative security guidance and updates to customers, industry partners, and the security community

- Help manage security risks and threats through 24x7 monitoring
- Conduct rapid incident analysis, resolution and worldwide mobilization
- 10+ years of industry leading security bulletin update process
- Enable best practices for the software, services and devices industry for collective defense

Strong Industry Collaboration

Collaborates with security community and industry partners to improve the broader security ecosystem

- **Microsoft Active Protection Program (MAPP):** enabling a global network of defenders with early access to vulnerability and update information
- **Security Update Validation Program:** enabling testing of security updates for application compatibility, stability and reliability in simulated environments
- **Bounty Programs:** rewards for researchers who find mitigation bypass techniques and accompanying defensive ideas

Advance Innovation and Quality

Commitment to excellence, innovation and quality to help evolve the security landscape

- **Enhanced Mitigation Experience Toolkit (EMET):** anticipates and blocks most common actions and techniques adversaries might use in compromising a computer
- **Microsoft Exploitability Index (EI):** provides information on the likelihood that a vulnerability will be exploited within the first 30 days of an update's release
- **Blue Hat Security Briefings:** facilitates exchange of ideas between Microsoft and outside security professionals

Microsoft och cybersecurity – 4 delar

1

Skapa säkra produkter och tjänster

2

Håll våra kunders data säkra.

3

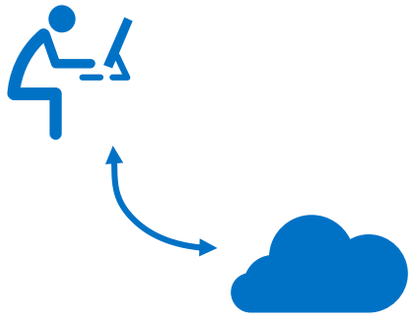
Hjälp kunder och partners att skydda sina tillgångar

4

Arbeta aktivt med att bekämpa cyberkriminalitet.

Datakryptering

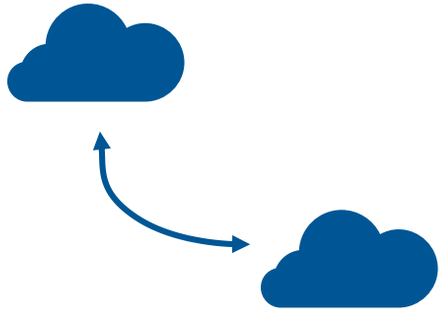
1



Data mellan en användare och tjänsten

Skyddar användare från avlyssning och skyddar mot datamanipulation

2



Data mellan datacenters

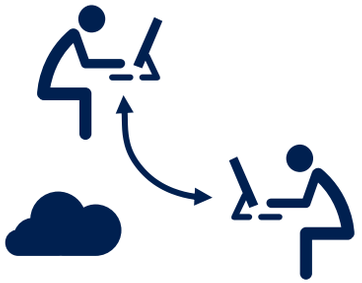
Skyddar mot massövervakning

3

Data i vila

Skyddar mot stöld av fysisk media

4



End-to-end kryptering av kommunikation mellan användare

Skyddar från avlyssning mellan användare

Microsoft och cybersecurity – 4 delar

1

Skapa säkra produkter och tjänster.

2

Håll våra kunders data säkra.

3

Hjälp kunder och partners att skydda sina tillgångar

4

Arbeta aktivt med att bekämpa cyberkriminalitet.

Key Threats

- Melissa (1999), Love Letter (2000)
- Mainly leveraging social engineering

Key Threats

- Code Red and Nimda (2001), Blaster (2003), Slammer (2003)
- 9/11
- Mainly exploiting buffer overflows
- Script kiddies
- Time from patch to exploit: Several days to weeks

Key Threats

- Zotob (2005)
- Attacks «moving up the stack» (Summer of Office 0-day)
- Rootkits
- Exploitation of Buffer Overflows
- Script Kiddies
- Raise of Phishing
- User running as Admin

Key Threats

- Organized Crime
- Botnets
- Identity Theft
- Conficker (2008)
- Time from patch to exploit: days

Key Threats

- Organized Crime, potential state actors
- Sophisticated Targeted Attacks
- Operation Aurora (2009)
- Stuxnet (2010)

Key Threats

- Passwords under attack
- Digital identity theft and misuse
- Signatures based AV unable to keep up
- Digital signature tampering
- Browser plug-in exploits
- Data loss on BYOD devices

2001

Windows XP

- Logon (Ctrl+Alt+Del)
- Access Control
- User Profiles
- Security Policy
- Encrypting File System (File Based)
- Smartcard and PKI Support
- Windows Update

2004

Windows XP SP2

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Security Development Lifecycle (SDL)
- Auto Update on by Default
- Firewall on by Default
- Windows Security Center
- WPA Support

2007

Windows Vista

- Bitlocker
- Patchguard
- Improved ASLR and DEP
- Full SDL
- User Account Control
- Internet Explorer Smart Screen Filter
- Digital Right Management
- Firewall improvements
- Signed Device Driver Requirements
- TPM Support
- Windows Integrity Levels
- Secure “by default” configuration (Windows features and IE)

2009

Windows 7

- Improved ASLR and DEP
- Full SDL
- Improved IPSec stack
- Managed Service Accounts
- Improved User Account Control
- Enhanced Auditing
- Internet Explorer Smart Screen Filter
- AppLocker
- BitLocker to Go
- Windows Biometric Service
- Windows Action Center
- Windows Defender

2012

Windows 8

- UEFI (Secure Boot)
- Firmware Based TPM
- Trusted Boot (w/ELAM)
- Measured Boot and Remote Attestation Support
- Significant Improvements to ASLR and DEP
- AppContainer
- TPM Key Protection
- Windows Store
- Internet Explorer 10 (Plugin-less and Enhanced Protected Modes)
- Application Reputation moved into Core OS
- BitLocker: Encrypted Hard Drive and Used Disk Space Only Encryption Support
- Virtual Smartcard
- Picture Password, PIN
- Dynamic Access Control
- Built-in Anti-Virus

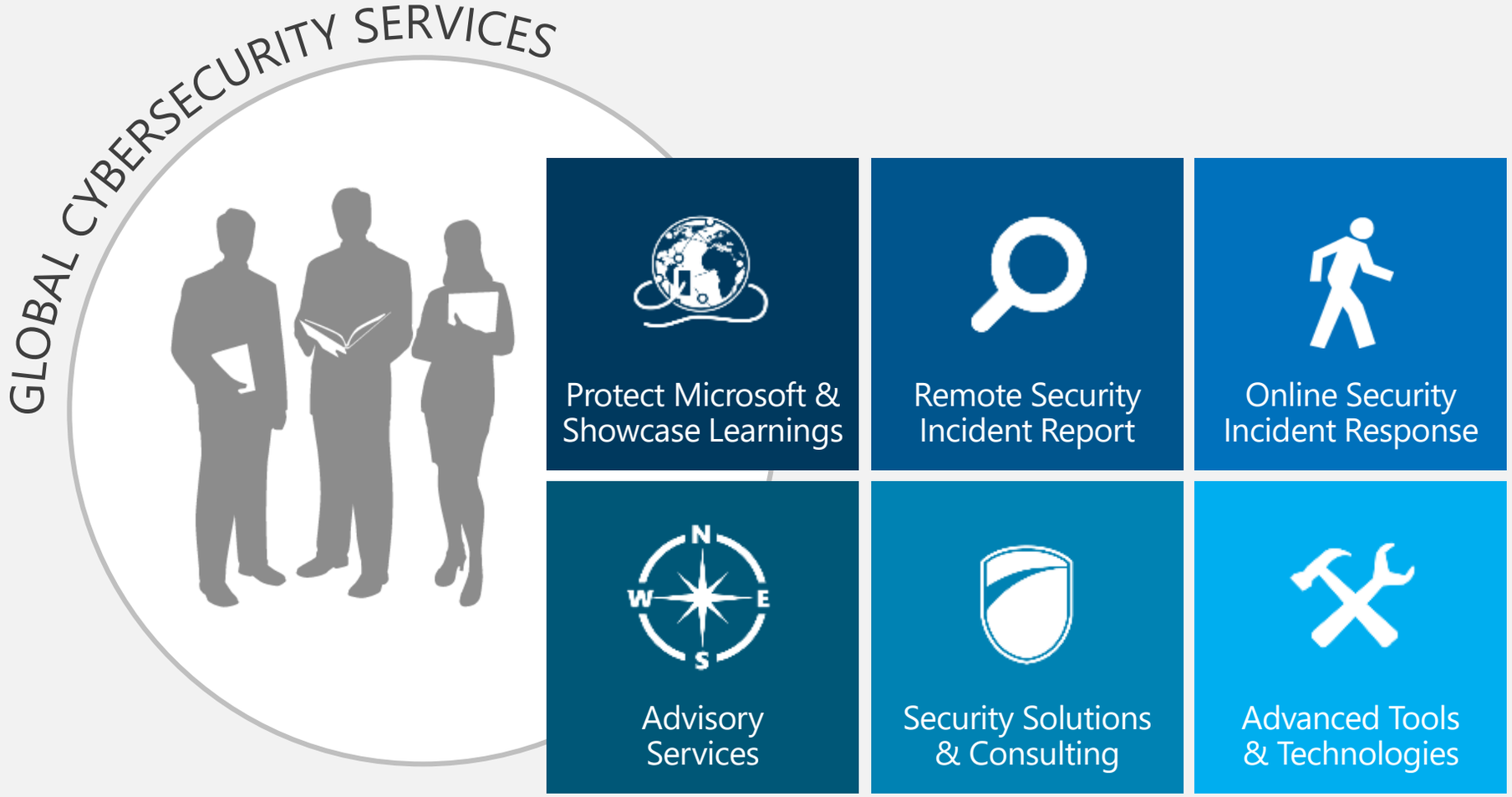
2013

Windows 8.1

- Touch Fingerprint Sensors
- Improved Biometrics
- TPM Key Attestation
- Certificate Reputation
- Improved Virtual Smartcards
- Provable PC Health
- Improved Windows Defender
- Improved Internet Explorer
- Device Encryption (All Editions)
- Remote Business Data Removable

MCS Cybersecurity tjänster

IT-arkitekter, konsulter & ingenjörer



Microsoft och cybersecurity – 4 delar

1

Skapa säkra produkter och tjänster.

2

Håll våra kunders data säkra.

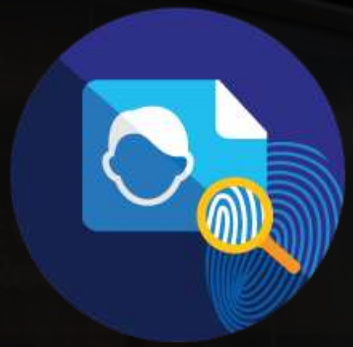
3

Hjälp kunder och partners att skydda sina tillgångar

4

Arbeta aktivt med att bekämpa cyberkriminalitet

Digital Crimes Unit



Skydda utsatta grupper

Bekämpa malware och botnets

Big data

Utredningar

Juridiska processer





Skydda utsatta grupper





Microsoft supportsamtal

Hur det fungerar

- Bedragare ringer och låtsas vara teknisk support från Microsoft
- Personen ger tillgång till PC och installerar malware.

I USA blir personer lurade på c:a 10 miljarder varje år.





Bekämpa malware

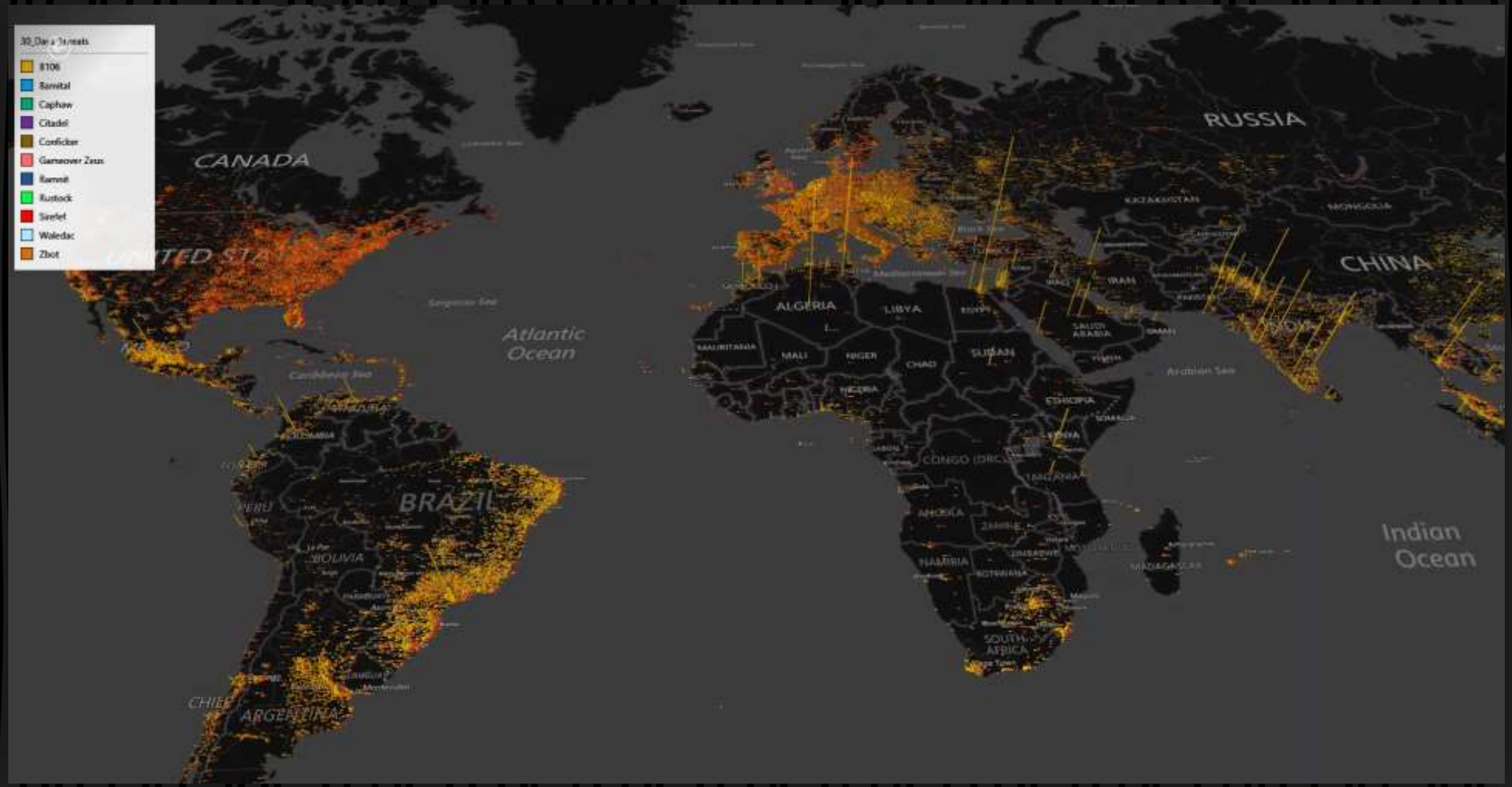




Cyber Threat Intelligence Program

60 miljoner IP addresser

400 miljoner pings/dag



Sammanfattning

Det är din data!

Inbyggd säkerhet

Privacy by Design

Compliance

Transparent Service Operation

Bekämpa Cybercrime

Säkerhet är stort men nästan allt vi diskuterat idag finns samlat på ett ställe…

Microsoft Azure Säkerhetscenter

Det tillförlitliga molnet

- Säkerhet och sekretess är inbäddade i hela utvecklingsprocessen av Azure
- Säkerhet: Vi arbetar för att skydda dina data
- Sekretess: Du äger och styr din kundinformation
- Transparens: Du vet hur dina data är lagrade, hur åtkomsten till dem ser ut och hur vi hjälper till att skydda dem
- Efterlevnad: Vi följer globala standarder

Senast uppdaterad: april 2015

Overview | Security | Privacy | Transparency | Compliance

Vi på Microsoft är väl medvetna om att du som vår företagskund för att dra nytta av fördelarna med molnet måste vilja anförtro en av dina viktigaste tillgångar – dina data – till en molnleverantör du verkligen litar på. Om du investerar i en molntjänst måste du kunna lita på att dina kunddata är i tryggt förvar, att integriteten är skyddad och att du har kvar ägarskapet av och kontroll över informationen och att den bara kommer att användas på det sätt du förväntar dig.

Microsoft strävar efter att vinna ditt förtroende för Microsoft Azure. Vår långa erfarenhet av att köra onlinetjänster har inneburit omfattande investeringar i grundläggande teknik som bygger in säkerhet och sekretess i utvecklingsprocessen. Vi har med tiden utvecklat branschledande säkerhetsmetoder och

Mer resurser

TwC cloud trust	Security intelligence report	Security development lifecycle	Trustworthy computing	Security blog
www.microsoft.com/trustedcloud	www.microsoft.com/sir	www.microsoft.com/sdl	www.microsoft.com/twc	blogs.technet.com/security

TACK!

daniel.akenine@microsoft.com