How many of you can answer “Yes” to these questions?

Do you **know** who is accessing your data?

Can you **grant access** to your data based on risk in real time?

Can you **protect** your data on devices, in the cloud, and in transit?

Can you quickly **find** and **react** to a breach?

Do your users **love** their work experience?
Security and Emerging Threats

Mark Ghazai, Director of Cyber Security and Cloud
Akhlesh Sharma, Sr. Premier Field Engineer
Microsoft State and Local Government
Microsoft mission

Empower every person and every organization on the planet to achieve more
We are focused on your journey to be a digital business

DIGITAL TRANSFORMATION

Systems of Intelligence

Engage employees and citizens
Empower your employees
Optimize your operations
Transform your services
OUR COMMITMENT TO TRUST

TRANSPARENCY

PRIVACY

COMPLIANCE

SECURITY
160 MILLION customer records compromised
99+ DAYS between infiltration and detection
$3 MILLION of cost/business impact per breach
YOUR IT ENVIRONMENT
YOUR IT ENVIRONMENT
Microsoft’s Commitment to Cybersecurity

Microsoft’s Cloud Weathers 1.5 Million Hack Attempts Each Day

By Pedro Hernandez | June 06, 2017

Microsoft’s 3,500 security engineers and its AI-enabled Intelligent Security Graph system helps the company thwart over a million attempts to breach its cloud infrastructure each day.

Microsoft’s cloud is constantly under attack. While it’s no surprise that the Redmond, Wash. technology giant makes a tempting target for cyber-attackers, but the scale of the attacks weathered by the company may raise some eyebrows.

On a typical day, 1.5 million attempts are made to breach Microsoft’s cloud systems, the company revealed today on its website. Keeping attackers at bay are over 3,500 security engineers and Microsoft’s Intelligent Security Graph, an AI-enabled system that uses machine learning to analyze hundreds of billions of authentications and other security information generated by the company’s IT systems.

Each second, Microsoft feeds hundreds of gigabytes of telemetry into the Intelligent Security Graph, the company claims. And every month, Microsoft scans an estimated 400 billion emails that flow through Office 365 and Outlook for phishing scams and malware.

All told, Microsoft invests $1 billion each year in cloud security. These statistics aside, the company continues to roll out new features and product enhancements to eliminate security gaps for customers.
THE MICROSOFT INTELLIGENT SECURITY GRAPH

200+ global cloud consumer and commercial services

+1B Windows devices updated

18+ billion web pages scanned

450B monthly authentications

400B e-mails analyzed

Unparalleled cybersecurity visibility and insight
EXPERIENCE

- 1M+ Corporate Machines protected by enterprise IT security
- Multi-platform cloud-first hybrid enterprise
- Decades of experience as a global enterprise
- Runs on multi-tenant Azure environment, same as you

CONTEXT

- Trillions of URLs indexed
- Hundreds of Billions of authentications, monthly emails analyzed
- Billions of daily web pages scans, Windows devices reporting
- Hundreds of Millions of reputation look ups
- Millions of daily suspicious files detonations

VISIBILITY

- Malware largest anti-virus and antimalware service
- Clients Windows Updates, Error Reports
- Email Outlook.com, Office 365
- Web content Bing, Azure AD
- Cloud platform Azure IaaS and PaaS, Azure Security Center

EXPERTISE

- Development Security established Security Development Lifecycle (SDL) - ISO/IEC 27034-1
- Operational Security for Hyper-scale cloud services
- Combating Cybercrime in the cloud & partnering with law enforcement to disrupt malware
- Incident Investigation and recovery for customers

CONTEXT

- Trillions of URLs indexed
- Hundreds of Billions of authentications, monthly emails analyzed
- Billions of daily web pages scans, Windows devices reporting
- Hundreds of Millions of reputation look ups
- Millions of daily suspicious files detonations
Microsoft employs a layered approach to security:

- Digital Crimes Unit (DCU)
- Cyber Defense Operations Center (CDOC)
- Cyber Security Services Engineering
- Microsoft Services Security Architects
- Premier Incident Response & Recovery
- Information Security & Risk Management
- Microsoft Product Engineering
  - (Microsoft Azure, Office 365, Windows)
- Microsoft Security Response Center
- Microsoft Threat Intelligence Center (MSTIC)
OUR SECURITY POSTURE

PROTECT
across all endpoints, from sensors to the datacenter

DETECT
using targeted signals, behavioral monitoring, and machine learning

RESPOND
closing the gap between discovery and action
Typical Credential Theft Attack
Compromises administrative control

1. Beachhead (Phishing Attack, etc.)
2. Lateral Movement
   a. Steal Credentials
   b. Compromise more hosts & credentials
3. Privilege Escalation
   a. Compromise unpatched servers
   b. Get Domain Admin credentials
4. Execute Attacker Mission
   a. Steal data, destroy systems, etc.
   b. Persist Presence
A secure modern enterprise is resilient to threats
Aligned to business objectives and current threat environment

**Identity**
Embraces identity as primary security perimeter and protects identity systems, admins, and credentials as top priorities

**Apps and Data**
Aligns security investments with business priorities including identifying and securing communications, data, and applications

**Infrastructure**
Operates on modern platform and uses cloud intelligence to detect and remediate both vulnerabilities and attacks

**Devices**
Accesses assets from trusted devices with hardware security assurances, great user experience, and advanced threat detection

**Secure Platform (secure by design)**
Microsoft Holistic Cybersecurity Approach

Product
- AD, Azure AD, MIM, EMS, O365 EOP, O365 ATP
- Azure Security Center, OMS, etc.
- System Center, Defender ATP, Win10, etc

Support
- Microsoft Premier Support
- Reactive (Security Support, IR/TR)
- Proactive (Security Assessments, MSRA, PADS, POP-SLAM, Workshops, etc)
- Cyber DSE

Services
- Cyber Security Architect (CSA)
- Identity solutions (DIAD, ADSH, MIM, ePAM, Azure AD)
- ATA Implementation Services (ATAIS)
- CTM Suite (ESAE, PAW) & Cyber ITSM
Protect and Enable

Cybersecurity Priorities

- Securing Privileged Access (On-Prem AD & Cloud)
- People/Process (ITSM)
- Application (SDL) & Info Protection (RMS)
- Identity Hygiene
- IoT
- Patch
Getting started
Building the Security Foundation

Phase 1: Build the Security Foundation
Start the journey by getting in front of current attacks
• Critical Mitigations – Critical attack protections
• Attack Detection – Hunt for hidden persistent adversaries and implement critical attack detection
• Roadmap and planning – Share Microsoft insight on current attacks and strategies, build a tailored roadmap to defend your organization’s business value and mission

Phase 2: Secure the Pillars
Continue building a secure modern enterprise by adopting leading edge technology and architectures:
• Privileged Access Security - Industrial Grade protections for critical identities and assets
• Shadow IT visibility – Discover, protect, and monitor your critical data in the cloud
• Device and Datacenter Security - Hardware rooted protections for devices, servers, and credentials
• Threat Detection - Deep analyst expertise and unique technical and human insights into threats
• Cloud Security Risk Mitigation - Chart a secure path as a cloud-enabled enterprise

Secure Platform (secure by design)
ASSUME BREACH
Securing Privileged Access
Typical Attack Timeline & Observations

- **First Host Compromised**
- **Domain Admin Compromised**
- **Attacker Undetected (Data Exfiltration)**
- **Attack Discovered**

24-48 Hours

More than 99 days (varies by industry)

**Attack Sophistication**
- Attack operators exploit any weakness
- Target information on any device or service

**Target AD & Identities**
- Active Directory controls access to business assets
- Attackers commonly target AD and IT Admins

**Attacks not detected**
- Current detection tools miss most attacks
- You may be under attack (or compromised)

**Response and Recovery**
- Response requires advanced expertise and tools
- Expensive and challenging to successfully recover
1. Restrict Privilege Escalation
   a. Privileged Access Workstations
   b. Assess AD Security

2. Restrict Lateral Movement
   a. Random Local Password

3. Attack Detection
   a. Attack Detection
   b. Hunt for Adversaries

4. Organizational Preparation
   a. Strategic Roadmap
   b. Technical Education

Organizational Preparation
Education
Strategy & Integration

Tier 0
Domain & Enterprise Admins

Tier 1
Server Admins

Tier 2
Workstation & Device Admins

Attack Detection
Advanced Threat Analytics (ATA)
Hunt for Adversaries

Restrict Lateral Movement
Restrict Privilege Escalation
Modernize Roles and Delegation Model

Tier-0
Control

Tier-1
Data and Services

Tier-2
Access
Administration Forest for Administrators

Tier-0: Control

Tier-1: Data and Services

Tier-2: Access

Privileged Access

IPsec
Example: Physical PAW, Productivity VM

Jump Server is optional
Internet Connectivity Design: Option 1

- Prohibiting internet use
Privilege Vaulting

1. Request Access (10:00)
2. Auto-Approve (10:00)

PAM Server

Admin Group (or Custom Action)

Managed Servers
Domain Admin
Schema Admin
Top Secret Project

Customizable Workflows
- Notifications
- Approva
- Actions

Admin Account

11:00
1:00
2:00
3:00

9:00
10:00
11:00
12:00
1:00
2:00
3:00
Microsoft Advanced Threat Analytics

An on-premises platform to identify advanced security attacks *before* they cause damage

Comparison:

- **Credit card** companies monitor cardholders’ behavior.
- If there is any abnormal activity, they will notify the cardholder to verify charge.

Microsoft Advanced Threat Analytics brings this concept to IT and users of a particular organization.
Advanced Threat Analytics (ATA)

**Account enumeration**
- Net Session enumeration
- DNS enumeration
- Abnormal resource access

**Net Session enumeration**

**DNS enumeration**

**Abnormal resource access**

**Abnormal working hours**

**Brute force using NTLM, Kerberos or LDAP**

**Sensitive accounts exposed in plain text authentication**

**Service accounts exposed in plain text authentication**

**Honey Token account suspicious activities**

**Unusual protocol implementation**

**Malicious Data Protection Private Information (DPAPI) Request**

**Pass-the-Ticket**

**Pass-the-Hash**

**Overpass-the-Hash**

**Abnormal authentication requests**

**Abnormal resource access**

**Compromised Credential**

**Privilege Escalation**

**Skeleton key malware**

**Golden ticket**

**Remote execution**

**Malicious replication requests**

**Reconnaissance**

**Lateral Movement**

**Domain Dominance**

**MS14-068 exploit (Forged PAC)**

**MS11-013 exploit (Silver PAC)**
### Securing Privileged Access – Estimated Timeline

<table>
<thead>
<tr>
<th>2-4 Weeks</th>
<th>1-3 Months</th>
<th>6+ Months</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Assessment/Training</td>
<td>Secure Enterprise Foundation – Identity Administration &amp; Privileged Access</td>
<td>Secure Identity / Device Pillars</td>
</tr>
</tbody>
</table>

**2-4 Weeks**
- Initial Assessment/Training
- MSRA: Comprehensive Risk Assessment
- POP – SLAM: Secure Lateral Account Movement Review / Plan
- POP-ATA: Advanced Threat Analytics Review/Plan
- POP-ADD: AD Delegation Review / Plan
- POP-SUM: Patch Management Review / Plan
- WorkshopPLUS: Windows Client Security Review/Plan
- Designated Security Engineer (DSE): Operational Integration, Training, Readiness

**1-3 Months**
- Secure Enterprise Foundation – Identity Administration & Privileged Access
- ETP: Enterprise Threat Protection
- PAW: Privileged Account Workstation
- AD Hardening/Remediation:
  - Tiered Administration
  - Just Enough Admin
  - AD Hardening and Account Rationalization
- Azure AD / MFA: Azure AD Implementation Services
- PAM: Privileged Access Mgmt

**6+ Months**
- Secure Identity / Device Pillars
- Shielded Virtual Machines Proof of Concept
- Windows 10 Security Foundation (Defender/ATP)
- Red Forest - ESAE (Enhanced Security Administration Environment)
- MS Services Solutions

**Cyber Security Architect (CSA)**
- Architectural Oversight and Technical Leadership

**Red Forest - ESAE**
- Shielded Virtual Machines Proof of Concept
- Windows 10 Security Foundation (Defender/ATP)