CIRCLE THE WAGONS! HOW ALL OF US DEFENDERS CAN WORK TOGETHER

Johnnie Konstantas  
Sr. Director, Enterprise Cybersecurity Group  
Microsoft  
@jkonstantas

Rob Lefferts  
Director, Enterprise and Security  
Microsoft

Sam George  
Director, Azure IoT  
Microsoft  
@samjgeorge
Easy marks are under attack

Adversaries still find low-hanging fruit quite tasty

Only 4% of SaaS apps support all HTTP headers session protection

Gamarue: 23 million infected IPs, 1,200 C2 points, 464 distinct botnets

96% of malware is automated polymorphic

Phishing volume: 200 million messages a month

https://www.microsoft.com/SIR
The digital estate
The market is fragmented and confusing.

150+ security controls
500+ vendors
Circle the wagons!
We can share resources

- Intelligence
- Platform
- Partners
Circle the wagons! We can share resources

Intelligence

Platform

Partners
Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals

- 400B emails analyzed
- 1.2B devices scanned each month
- 200+ global cloud consumer and commercial services
- 930M threats detected on devices every month
- 750M+ Azure user accounts
- 18B+ Bing web pages scanned
- 450B monthly authentications

Shared threat data from partners, researchers, and law enforcement worldwide

Botnet data from Microsoft Digital Crimes Unit

Windows

Outlook

Azure

OneDrive

Xbox Live

Bing

Microsoft accounts
Human intelligence
Partnerships to Defend Against a World of Increased Threats

By working together we can help protect our mutual customers
# Areas of Collaboration

<table>
<thead>
<tr>
<th>Identity and access management</th>
<th>Threat protection</th>
<th>Information protection</th>
<th>Security management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account authentication SSO across services and devices</td>
<td>Suspicious behavior and activity detection and response</td>
<td>Business data and app classification and control</td>
<td>Security risk assessment, controls and intelligence</td>
</tr>
</tbody>
</table>
## Areas of Collaboration

<table>
<thead>
<tr>
<th>Identity and access management</th>
<th>Threat protection</th>
<th>Information protection</th>
<th>Security management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure Active Directory</strong></td>
<td><strong>Microsoft Intune</strong></td>
<td><strong>Azure Information Protection</strong></td>
<td><strong>Azure Security Center</strong></td>
</tr>
<tr>
<td>Account authentication SSO across services and devices</td>
<td>Suspicious behavior and activity detection and response</td>
<td>Business data and app classification and control</td>
<td>Security risk assessment, controls and intelligence</td>
</tr>
</tbody>
</table>

**Windows Defender Advanced Threat Protection**

*Powered by the Intelligent Security Graph*
Microsoft Intelligent Security Association
Intelligence

Platform

Partners
Physical security
- Perimeter security
- Building security
- Server environment

Operational security
- Continuous testing
- Restricted access
- Thousands of security professionals

Customer controls
- Access control
- Encryption & key management
- Network & DDoS protection

Platform

Secure foundation
Fast identity online – the FIDO Alliance
The world’s largest ecosystem for standards-based, interoperable auth

<table>
<thead>
<tr>
<th>Security on-premises and web</th>
<th>Secure mobile user credentials</th>
<th>Secure authentication</th>
</tr>
</thead>
</table>

FIDO board members

- Microsoft
- Google
- Nok Nok Labs
- Oberthur Technologies
- Lenovo
- Aetna
- Bank of America
- PayPal
- infineon
- USAA
- Fingerprint
- Intel
- ARM
- yubico
- Visa
- BCcard
- RAON Secure
- Mastercard
- Samsung
- EGIS
- Synaptics
- RSA
- Qualcomm
- Gemalto
- docomo
- NXP
- ING
- CrucialTec
- VISA
- Daon
- Feitian
- Alibaba.com
- LINE
Conditional Access

- Privileged user?
- Credentials found in public?
- Accessing sensitive app?
- Unmanaged device?
- Device compromised?
- IP detected in Botnet?
- Impossible travel?

**Risk**
- High
- Medium
- Low

**IF**
- Users
- Devices
- Location
- Apps

**THEN**
- Allow access
- Require MFA
- Force password reset
- Deny access
- Limit access
**Built in security**

Platform

- Identity & access management
- Threat protection
- IoT security
Threat protection
Cloud-driven and automated

1. Reduce attack surface
2. Detect attacks faster and block them
3. Respond automatically to breaches where appropriate
Reduce attack surface

Assess your security state continuously

Enable security controls, and receive recommendation for further improvements

Remediate vulnerabilities and drive compliance
Detect and block attacks

Gain **visibility** and reduce blind spots

Detect attacks and **zero-day** exploits

Investigate your cloud ecosystem, the device, and your identities

Cloud-driven advanced behavioral analytics and machine learning
Respond automatically to breaches

Investigate and remediate threats
We do the investigation and remediation faster than anyone, and we do it at scale.

Driven by artificial intelligence
Applies industry best practices and intelligent decision-making algorithms to determine whether a threat is real and what action to take.

Cyber analyst logic at scale
Automatically investigates alerts to determine the appropriate course of action. Multiple parallel investigations to resolve the full extent of a breach.

Choose how to close the loop
Remediates threats automatically without human intervention to stop further damage or infection. Your choice: fully automated or semi-automated.

Going from alert to remediation in minutes at scale
Built in security

Platform

Identity & access management

Threat protection

IoT security
How do you know that the compressor in your fridge needs to be replaced?
How do you know that the compressor in your fridge needs to be replaced?

**TODAY**
Melted ice cream and spoiled milk

**TOMORROW**
Message that a technician with replacement compressor will arrive tonight
How do you know that the compressor in your fridge needs to be replaced?

**TODAY**
Melted ice cream and spoiled milk

**TOMORROW**
Message that a technician with replacement compressor will arrive tonight

**THE DIFFERENCE IS CLOUD CONNECTIVITY**
Highly secured connected devices require 7 properties

- **Hardware Root of Trust**: Is your device’s identity and software integrity secured by hardware?
- **Defense in Depth**: Does your device remain protected if a security mechanism is defeated?
- **Small Trusted Computing Base**: Is your device’s TCB protected from bugs in other code?
- **Dynamic Compartments**: Can your device’s security protections improve after deployment?
- **Certificate-Based Authentication**: Does your device use certificates instead of passwords for authentication?
- **Failure Reporting**: Does your device report back about failures and anomalies?
- **Renewable Security**: Does your device’s software update automatically?

**Support Requirements**:
- 🔄 = Silicon support required
- 🕵️‍♂️ = OS support required
- ⛅️ = Cloud Service support required

[link](http://aka.ms/7properties)
Azure Sphere

an end-to-end solution for creating highly-secured, connected MCU devices

**SECURED MCUs**
A new 4x4-class of MCUs with built-in Microsoft security technology provide connectivity and a dependable hardware root of trust.

**SECURED OPERATING SYSTEM**
A highly-secured 4x4 IoT OS from Microsoft combines the best of Microsoft and OSS technologies to create a trustworthy platform for new IoT experiences.

**CLOUD SERVICE SECURING EACH DEVICE**
The 4x4 Security Service guards every 4x4 device; it brokers trust for device-to-device and device-to-cloud communication, detecting emerging threats, and renewing security.
Device to Cloud Security

Security Program for Azure IoT

Device protection
- Trusted Platform Module (TPM)
- Windows Device Health Attestation*
- Secure Boot
- BitLocker
- DICE

Threat resistance
- Windows as a Service
- Device Guard
- Windows Firewall
- Windows Defender*

Data protection in-motion
- X.509/TLS-Based Handshake and Encryption

Cloud security
- Encryption at Rest
- Azure Active Directory
- Key Vault
- Policy-Based Access Control
- IP-based blocking
- Secure Device Registration
- Standards-based best practices

Response
- Device Management
- Device Recovery
- Device-specific repudiation

*Only available on Windows IoT Enterprise

Device to Cloud Security

Microsoft

RSA Conference 2018
Security Program for Azure IoT

Trusted security auditors trained on Azure IoT

Discover issues, get recommended remediations

Keep your IoT Solution secure

Not all partners may be listed; check internetofyourthings.com for latest status.
Apply what you have learned today

- **Next week:**
  - Understand what low hanging fruit your organization is offering to adversaries

- **In the next three months:**
  - Find three ways you can increase security through cloud adoption

- **In the next six months:**
  - Assess your IoT supply chain against the 7 principles
THANK YOU!