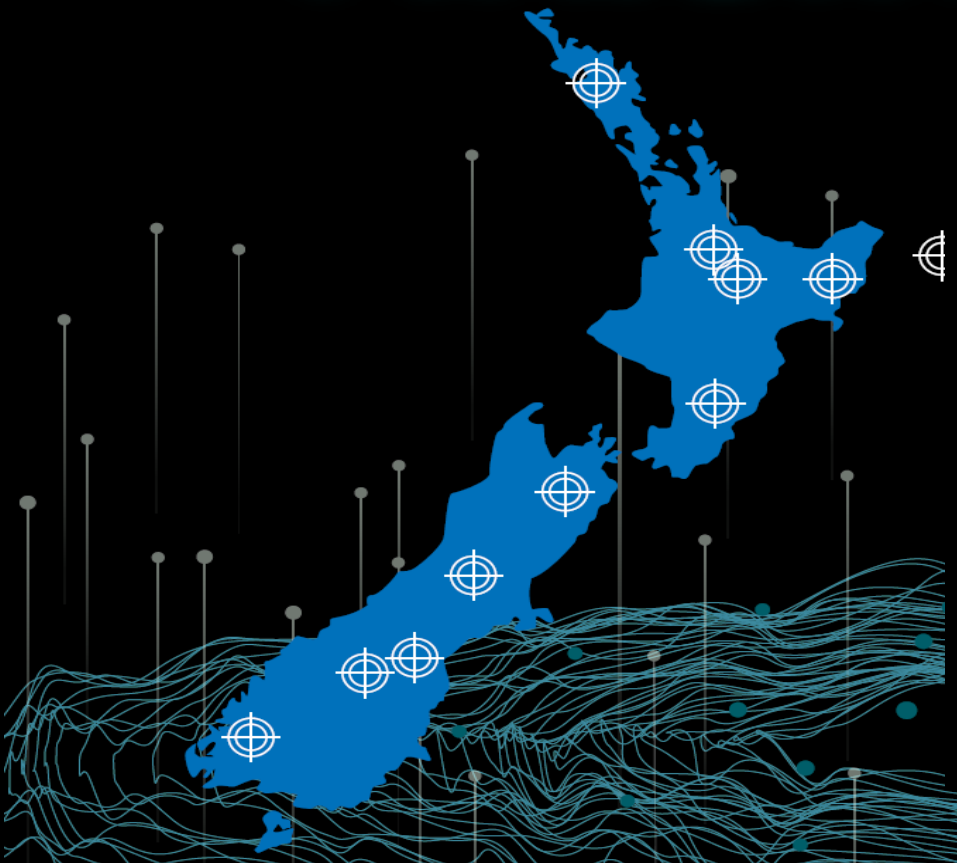
Microsoft

MICROSOFT SECURITY INTELLIGENCE REPORT:

NEW ZEALAND CYBER THREAT LANDSCAPE

Shifting Sands – Trends in Cybersecurity



Abbas Kudrati, Chief Cybersecurity Advisor
Microsoft Asia
Abbas.Kudrati@Microsoft.com

Current role:

- **Chief Cybersecurity Advisor** – Microsoft Asia
- **Industry Professor – Deakin University**
- **Professor of Practice in Cyber Security** – LaTrobe University
- **Executive Advisory Board Member – Cyber Security** – Deakin University, LaTrobe University and 6Clicks
- **Global Threat Advisory Board Member** – EC-Council ASPAC

Previous roles (last 6):

- KPMG Australia : **CISO**
- Public Transport Victoria : **CISO**
- National Bank of Kuwait : Dy **CISO**
- eGovernment Authority – Bahrain: **CISO**
- Ernst & Young – Bahrain : **Manager Cyber Advisory**
- KPMG Kuwait, Bahrain Qatar : **Sr, Consultant**

Awards and Accolades:

- **2019 "Top Cybersecurity Advisor for APJ" Microsoft**
- **2018 "Best Security Professional"** ISACA Oceanic CACS
- **2018 "CISO 100 Award"** by CISO Council, UAE
- **2017** SPLUNK **"Boss of the SOC "BOTS"** Winner for Melbourne region
- **2015** Australian **"CISO of the year"** finalist
- **2014** Middle East **"IT Governance Professional of year"**
- **2011** Middle East **"Security Strategist of year"**

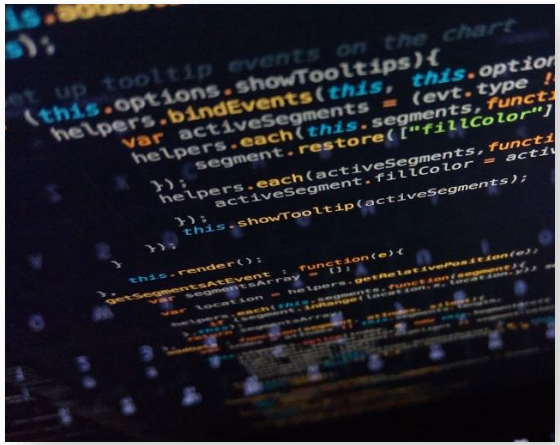
Certifications and Qualifications:

1. Certified Chief Information Security Officer **(C|CISO)**
2. Certified Information Security Manager **(CISM)**
3. Certified in Cloud Security Knowledge **(CCSK)**
4. Certified Information System Auditor **(CISA)**
5. **CSXP Certified Cybersecurity Practitioner** (CSX-P)
6. Certified in Governance of Information Technology
7. Certified Block Chain Expert **(CBE)**
8. Certified Ethical Hacker **(C|CEH)**
9. Certified Computer Forensic Hacking Investigator
10. TOGAF 8 Certified Enterprise Architect **(TOGAF CEA)**
11. **COBIT 5** Foundation Certified
12. **ISO 27001: 2005** Lead Auditor
13. **PRINCE 2** Practitioner and Foundation Certified
14. ITIL Foundation Certified **(ITIL)**
15. EC Council Disaster Recovery Professional **(E|DRP)**
16. SABSA Foundation Certified
17. **Microsoft Certified Azure Foundation**
18. **Microsoft Certified M365 Foundation**
19. Microsoft Certified Systems Engineer+ Security
20. **Cisco Certified Network Associate** (CCNA)
21. GNIIT Diploma in Systems Management
22. Bachelor of Commerce – Accounting and Auditing

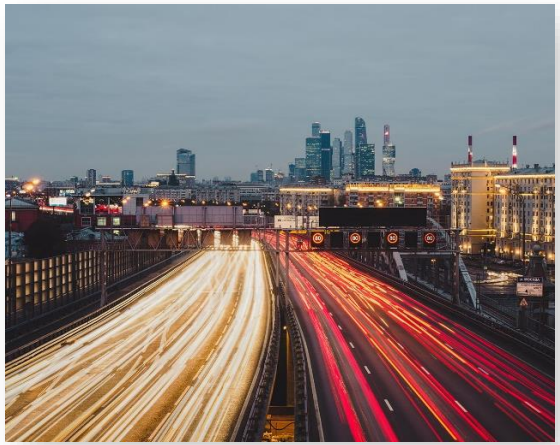
Cybersecurity Reality

The era of flux and transformation

Everyone is now in the technology business



Conventional security tools have not kept pace



Security professionals alone can't fill the gap

Regulatory requirements and costs are increasing

# of Cyberattacks in Asia Pacific

Trillions were lost to cyberattacks across Asia Pacific in 2017

Total economic loss across Asia Pacific

US$1.745 trillion ---> **7%** of Asia Pacific's GDP*

FROST & SULLIVAN: TOTAL ECONOMIC IMPACT OF CYBERATTACKS

US$30 million

Average economic loss for a large-sized company

DIRECT: US$3.4 million

Direct losses from cyberattacks are just the "tip of the iceberg"

INDIRECT: US$9.7 million

Opportunity costs, eg, loss of

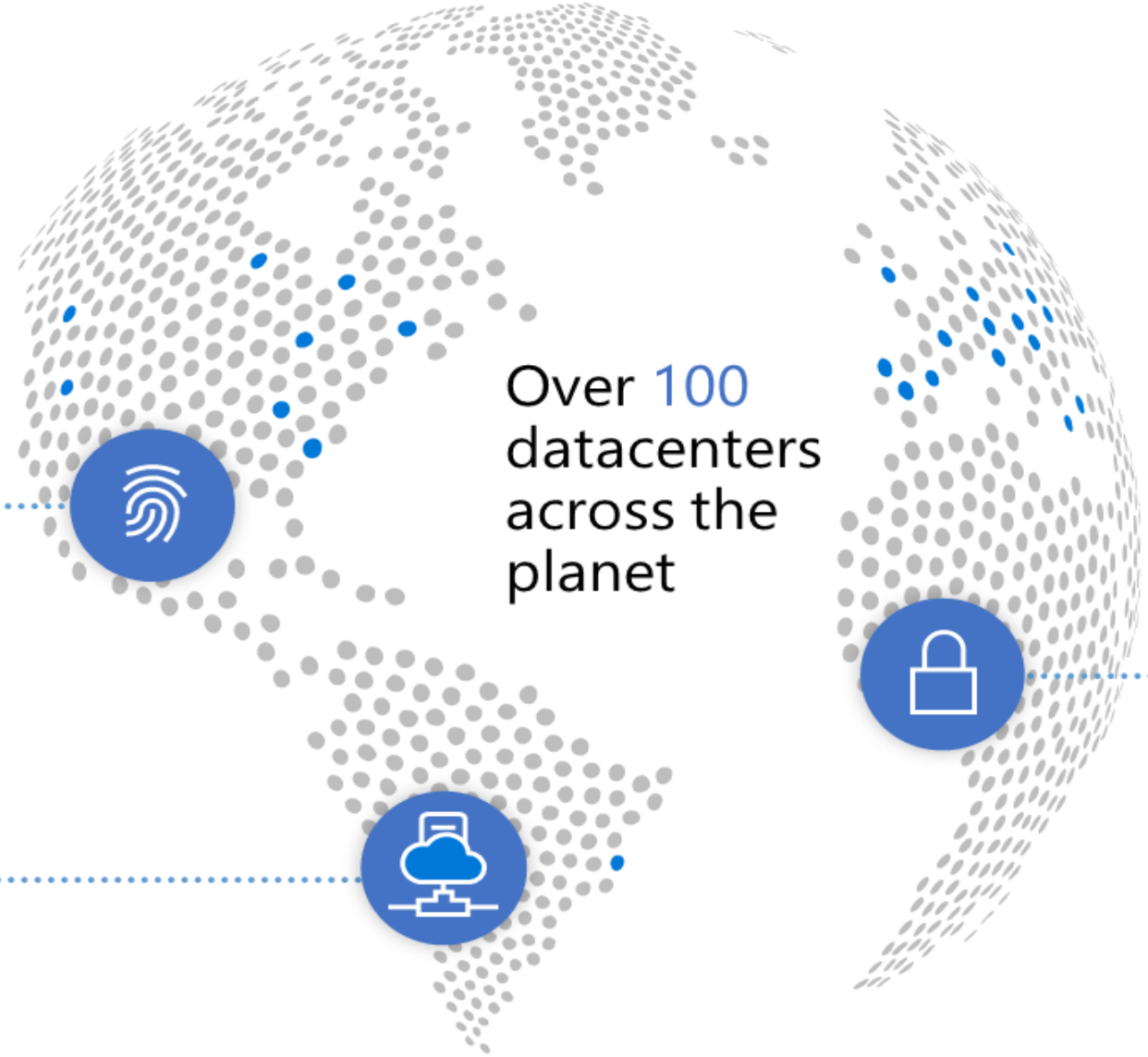
Get more insights about the Microsoft Asia and Frost & Sullivan Security Study 2018 findings here **https://news.microsoft.com/apac/features/cybersecurity-in-asia**.

"Just like the size of an iceberg, the economic loss for organizations suffering cybersecurity attacks can be often underestimated."

Insights on a global scale – 8 trillion signals a day

Each physical datacenter protected with world-class, multi-layered protection

Global cloud infrastructure with custom hardware and network protection

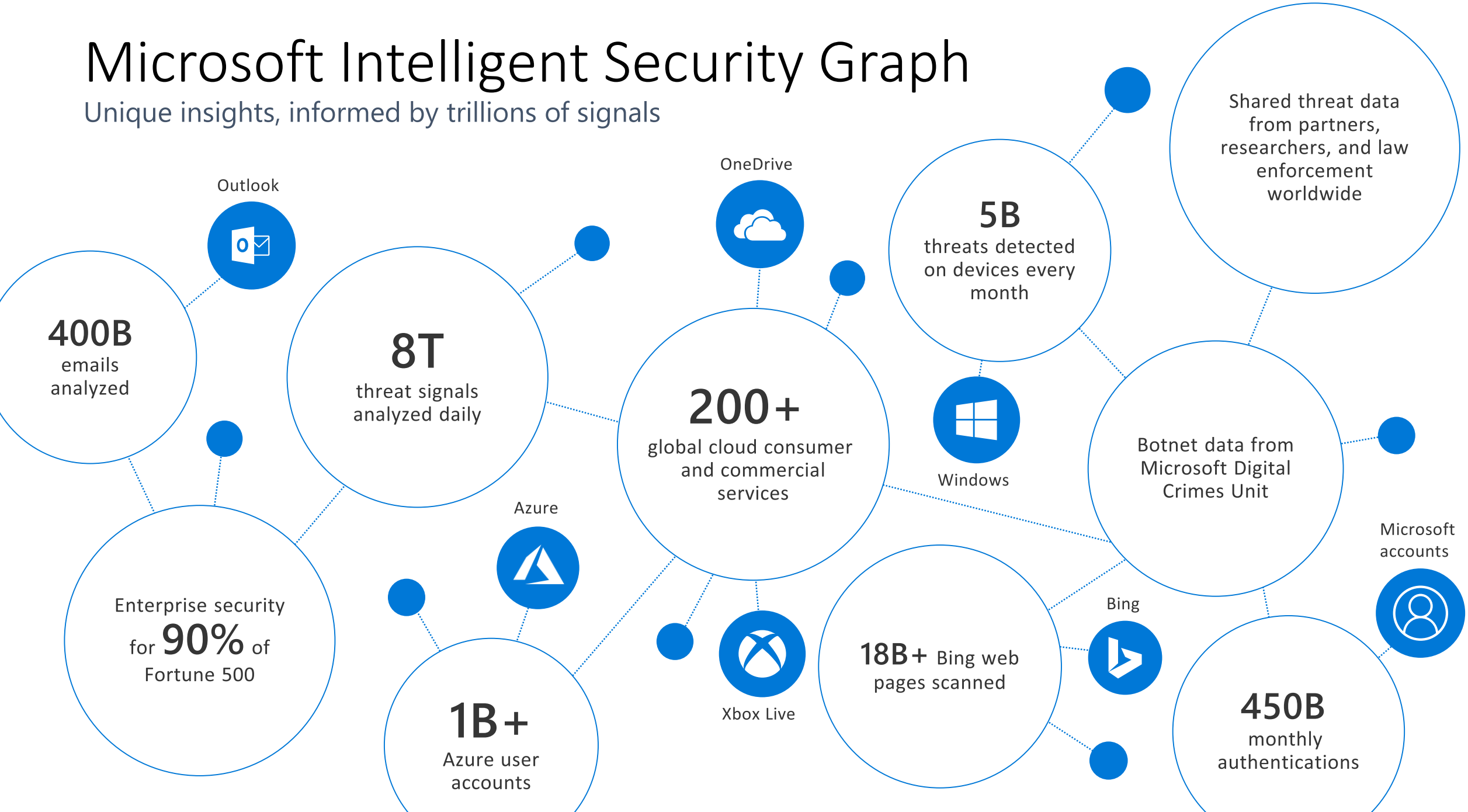


Secured with cutting-edge operational security

- Restricted access
- 24x7 monitoring
- Global security experts

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Top four cyber threats

MALWARE

Malware poses risks in the form of impaired usability, data loss, intellectual property theft, monetary loss and even emotional distress.

60%

Lower than the **Global** average

71%

Lower than the **Asia Pacific** average

Malware

- Severe impact: Malware poses risks in the form of impaired usability, data loss, intellectual property theft, and monetary loss.
- Decline in malware infection: Global malware encounter rate has **decreased by 34%** but malware encounter in Asia Pacific was still **37% higher** than the global rate.
- Developing markets: Poor cybersecurity hygiene and low user security awareness in these markets can lead to higher malware infection.
- Developed markets: Mature and comprehensive cybersecurity infrastructures, practices and education programs in these markets have led to lower malware encounter rates

Asia Pacific encounter rate

▲37%

Higher than the **Global** average

Markets with highest encounter rates

1. Indonesia
2. Philippines
3. Vietnam

Markets with lowest encounter rates

1. Japan
2. Australia
3. New Zealand

Microsoft

CRYPTOCURRENCY MINING

Attackers seeking illicit profits have increasingly turned to malware that lets them use victim's computer to help them mine cryptocurrency coins.

58%

Lower than the **Global** average

64%

Lower than the **Asia Pacific** average

Cryptocurrency mining malware

- Profit-driven: With the rise in cryptocurrency value, cybercriminals have turned to malware that lets them use infected computers to mine cryptocurrency coins.
- Opportunistic: Cryptocurrency mining malware encounter rate corresponds with the rise or fall in the value of cryptocurrency.
- Low barrier to entry: Cybercriminals are leveraging the wide availability of mining software and repacking them into malware.
- Stealthy: As these types of malware works in the background, victims may not know they are infected unless it degrades the computer's performance sufficiently.

Asia Pacific encounter rate

▲17%

Higher than the **Global** average

Markets with highest encounter rates

1. India
2. Sri Lanka
3. Indonesia

Markets with lowest encounter rates

1. China
2. Japan
3. Australia

Microsoft

RANSOMWARE

While individuals and organizations are becoming more intelligent in dealing with ransomware, it continues to be a significant threat in New Zealand.

60%

Lower than the **Global** average

71%

Lower than the **Asia Pacific** average

Ransomware

- Decline in frequency: Ransomware encounters have decreased by 73% globally.
- Greater awareness: Organizations and individuals have become more aware of and more intelligent in dealing with ransomware.
- Still a threat in the region: Asia Pacific encounter rate was 40% more than the global average.
- Severe consequences: Severity of ransomware attacks have not declined and it is still capable of disrupting organizations' operations and crippling critical services.

Asia Pacific encounter rate

▲40%

Higher than the **Global** average

Markets with highest encounter rates

1. Indonesia
2. Vietnam
3. India

Markets with lowest encounter rates

1. Japan
2. Australia
3. New Zealand

Microsoft

DRIVE-BY DOWNLOAD

Attackers are exploiting vulnerabilities in webpages to direct users to compromised sites that can secretly infect users even when they do not attempt to download anything.

100%

Lower than the **Global** average

100%

Lower than the **Asia Pacific** average

Drive-by Downloads (DbD)

- Unsuspecting victims: Attackers are exploiting vulnerabilities in webpages to direct users to comprised sites that can secretly infect users even when they do not attempt to download anything.
- Exploiting loopholes: Malicious code are used to exploit vulnerabilities in web browsers, browser add-ons, applications, and the operating system.
- Malware delivery: More advanced drive-by download campaigns can install ransomware or cryptocurrency mining malware on the victim's devices.

Asia Pacific Drive-by Download pages

▲ 22%

Higher than the **Global** average

Markets with highest DbD pages

1. Taiwan
2. Malaysia
3. Indonesia

Markets with lowest DbD pages

1. New Zealand
2. Japan
3. South Korea

Microsoft

CYBERSECURITY BEST PRACTICES

FOR ORGANIZATIONS

1. **Prevention:** Preventive controls increase the cost of attacks for cybercriminals and prevent cheap, effective cyberattack techniques.

   - **Cloud Backup:** Use cloud storage services to automatically backup important data.
   - **Access Control:** Implement network segmentation and exert caution when granting application permissions.
   - **Cybersecurity Education:** Educate employees on safe cyber practices and maintain robust IT policies.

2. **Detection & Response:** Leverage cloud technology to limit attackers' access to data and help security operations better respond to attacks.

FOR INDIVIDUALS

1. **Cyber Hygiene:** Use anti-virus solution and keep software and operating systems updated.

2. **Genuine Software:** Avoid using pirated software and only use software from trusted sources.
3. **Password Management:** Use a strong password for each account and change them regularly.

4. **Backup Personal Files:** Backup photos and other important personal data on a trusted cloud storage platform.
5. **Stay Vigilant:** Activities where personal information will be transmitted should only be done on the users' own devices, on a trusted network.

Learn more

Download the full Microsoft Security Intelligence Report, Volume 24 for more insights

www.microsoft.com/sir

Check out the Microsoft Security Blog for insights on the latest cybersecurity topics

www.microsoft.com/security/blog

Microsoft

Cybersecurity Trend in **2020**

Microsoft

2020 Security Trends

01

Adversaries will increasingly use AI to make malware more destructive

02

Protecting supply chains will accelerate industry collaboration

03

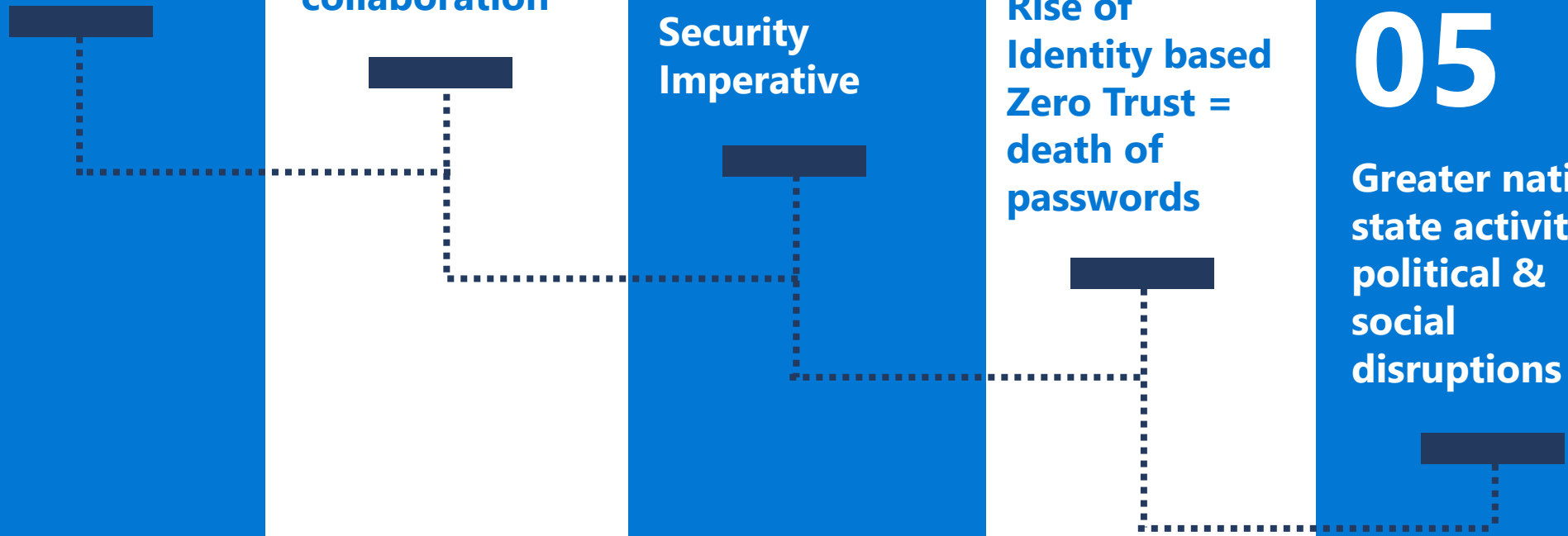
Public Cloud Becomes a Security Imperative

04

Rise of Identity based Zero Trust = death of passwords

05

Greater nation state activity + political & social disruptions



Microsoft

01

Adversaries will increasingly use AI to make malware more destructive

Microsoft

01 Adversaries will increasingly use AI to make malware more destructive

Risks

*"It takes organizations an average of 206 days to identify a data breach, and another 73 days to contain it" **

**Ponemon Institute Cost of a Data Breach Report, 2019*

The rise of AI capabilities provide **new opportunities** for attackers to create malware that hides from detection while hunting down targets

Industry experts believe AI-powered malware is already in use, but often goes **undetected**

Microsoft

01 Adversaries will increasingly use AI to make malware more destructive

Counter Measures

- Threat signal and compute power with companies like Microsoft, allowing to detect and react to “patient zero” threats in near real time
- Security experts that track threats and train their own AI and ML based protection based on a wide range of risk factors – not just previously discovered malware
- Teams like Microsoft’s Digital Crimes Unit (DCU) proactively identify criminal organization creating malware and work with law enforcement to disrupt their activities

Microsoft

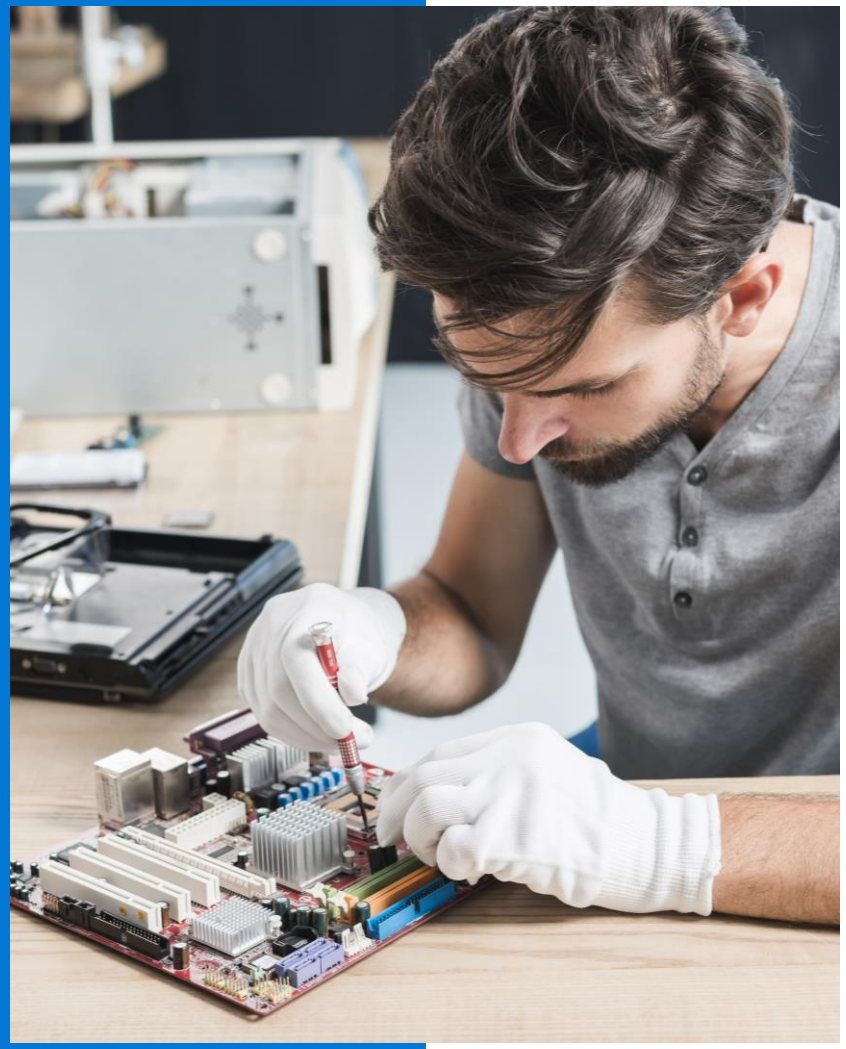
- Azure Sentinel with Power of AI and ML
- Microsoft Defender ATP and Azure ATP
- Automated Playbook and Jupyter Notebook

01 Adversaries will increasingly use AI to make malware more destructive

Tools and Services

Microsoft

02



Protecting supply chains will accelerate industry collaboration

Microsoft

02 Protecting supply chains will accelerate industry collaboration

Risks

The number of devices in the world is expected to exceed 75 billion next year.*

** Morgan Stanley*

- The growth of mobile devices and IoT will give way to even more complex supply chains as we embrace technologies like autonomous machines
- By 2022, more than 50 percent of enterprise-generated data will be created and processed outside the data center or cloud**
- Attackers are already looking for gaps in defenses like outdated software, unsecured devices and default admin accounts

*** Cleanshelf: State of Business' SaaS Spend 2019. **David Cappuccio at Gartner Symposium*

Counter Measures

- Integrated solutions that secure the breadth and depth of their IT investments
- EG: The Microsoft Identity platform which adds security like MFA to 1.4 million unique apps (up 117 %YoY) including brands like ServiceNow, GoogleApps, and Salesforce
- It is also important that vendors work together to track the threats and vulnerabilities impacting their mutual customers and supply chains.

Tools and Services

- Security and Compliance Secure Score
- Compliance Manager
- Service Trust Portal
- Azure Security Centre

Microsoft

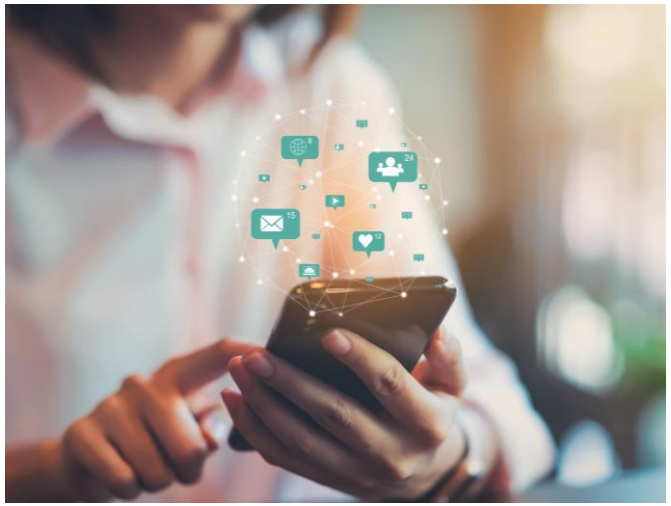
03

Public Cloud Becomes a Security Imperative

Microsoft

03 Public Cloud Becomes a Security Imperative

Risks



*Cybercrime costs more than $1 trillion a year and three times as much as the costs of natural disaster***

***Institute and Accenture: Ninth Annual (2019) Cost of Cybercrime Study*

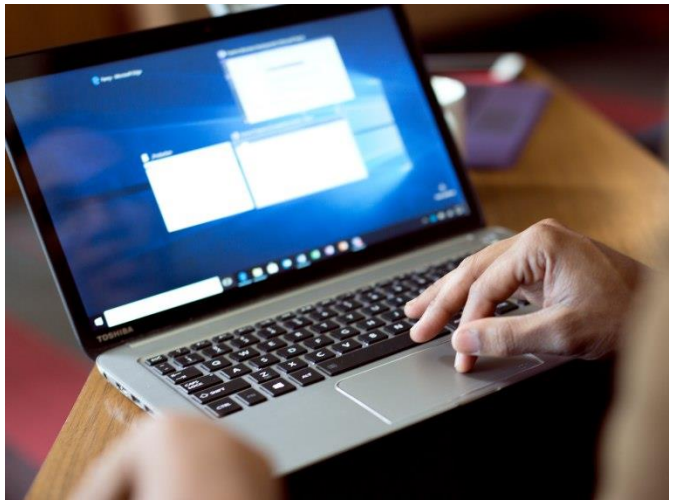
While attackers continue to develop new tools and techniques, traditional methods like phishing remain effective as few have resources to implement security best practices like enabling MFA

IT departments are tasked with providing end users with better mobility and productivity without friction associated with traditional security solutions

Microsoft

03 Public Cloud Becomes a Security Imperative

Risks



Almost no company can defend itself from modern threats without the help of cloud-based protection.

The historical approach of weaving together disparate solutions and/or investing in costly on-premise security tools is now generating too much burden and “white noise” for under-resourced cyber defenders

Shared responsibility model

Customer management of risk

Data classification and data accountability

Shared management of risk

Identity & access management | End point devices

Provider management of risk

Physical | Networking

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability	■	■	■	■
Client & end-point protection	■	■	■	◢
Identity & access management	■	■	◢	◢
Application level controls	■	■	◢	
Network controls	■	◢		
Host infrastructure	■	◢		
Physical security	■			

■ Cloud customer ■ Cloud provider

Microsoft

Hybrid solutions are now common, with a total of 67 percent of companies using or planning to deploy a hybrid cloud*

The unique compute power and threat insights from more than 8 trillion signals every day give public cloud companies like Microsoft a unique view into the global threat landscape

03 Public Cloud Becomes a Security Imperative

Counter Measures

Microsoft

03 Public Cloud Becomes a Security Imperative

Counter Measures

- The industry will continue moving toward the public cloud for better security, compliance and Identity protection
- Threat intelligence helps Microsoft deliver near real-time protection to tightly integrated cloud and endpoint solution, and identity management

Microsoft

- Global Datacenter across the world, 8 trillion signal monitoring
- Unique Threat Intelligence network, DCU, CDOC

03 Public Cloud Becomes a Security Imperative

Tools and Services

Cybersecurity Reference Architecture

April 2019 – https://aka.ms/MCRA | Video Recording | Strategies

Security Operations Center (SOC)

Microsoft Threat Experts | Incident Response, Recovery, & CyberOps Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt | MSSP | Cloud App Security | Azure Security Center | Microsoft Defender | Office 365 | Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Software as a Service

Office 365

- Secure Score
- Customer Lockbox

Dynamics 365

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Microsoft Defender ATP

Secure Score | Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

Extranet

- NGFW
- Edge DLP
- SSL Proxy
- IPS/IDS

Azure Firewall | Security Appliances

Express Route

Intranet Servers

Windows Server 2019 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...

Shielded VMs | Azure Stack | VMs

Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Application & Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation+Monitor

Information Protection

Classification Labels

Cloud App Security

Azure Information Protection (AIP)

- Discover
- Classify
- Protect
- Monitor

Hold Your Own Key (HYOK)

AIP Scanner

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Windows 10 Enterprise Security

Network protection | Credential protection | Exploit protection | Reputation analysis | Full Disk Encryption | Attack surface reduction

App control | Isolation | Antivirus | Behavior monitoring

S Mode

IoT and Operational Technology

Windows 10 IoT | Azure IoT Security | Azure Sphere | IoT Security Maturity Model | IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center | **Intelligent Security Graph**

Microsoft

Microsoft

04

Rise of Identity based Zero Trust = death of passwords

Microsoft

04 Rise of Identity based Zero Trust = death of passwords

Risks

- This year alone, over 4 billion records have already been exposed due to data breaches*
- Poorly secured accounts and identities continue to be the weak link - by 2025 it's estimated there will be over 160 Zettabytes of data**
- AI based malware and the complexity of supply chains will continue to overwhelm traditional perimeter-based security models

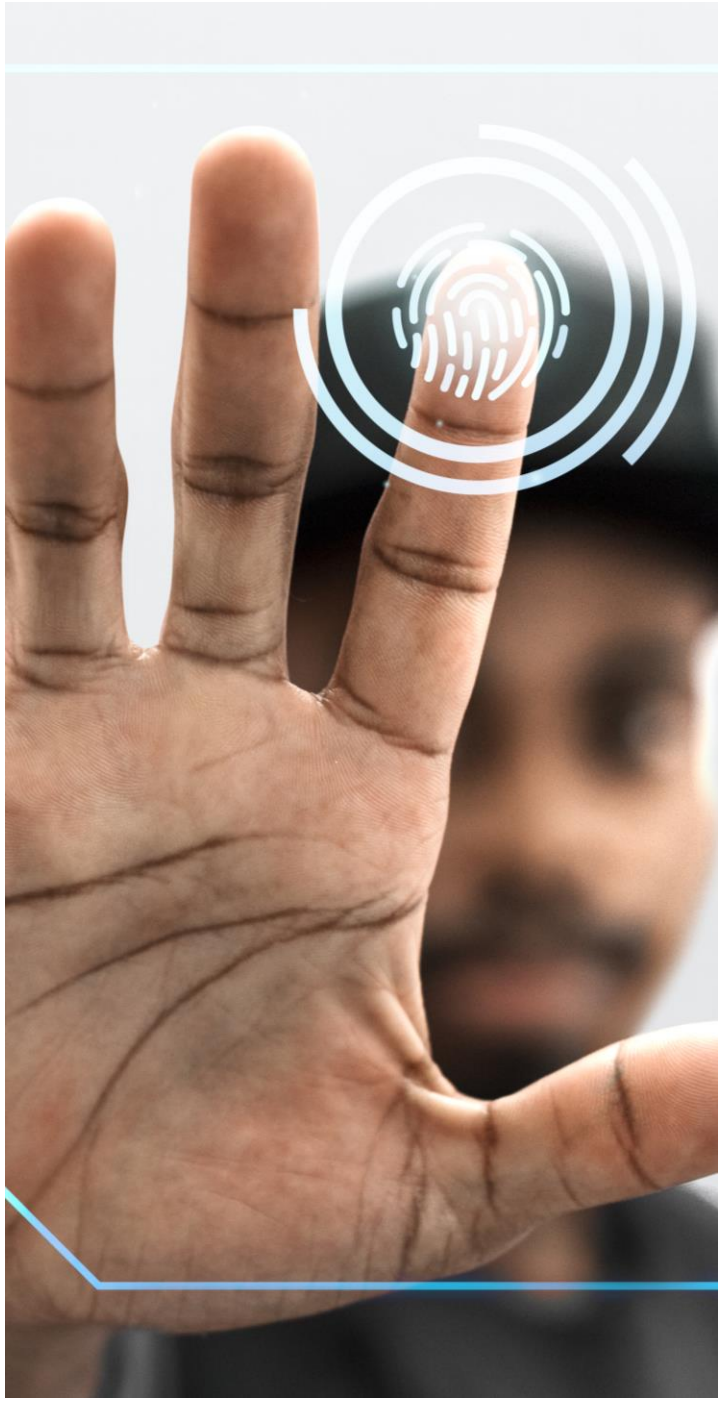
**Risk Based Security: The 2019 MidYear Data Breach QuickView Report*
*** IDC: Data Age 2025*

Microsoft

04 Rise of Identity based Zero Trust = death of passwords

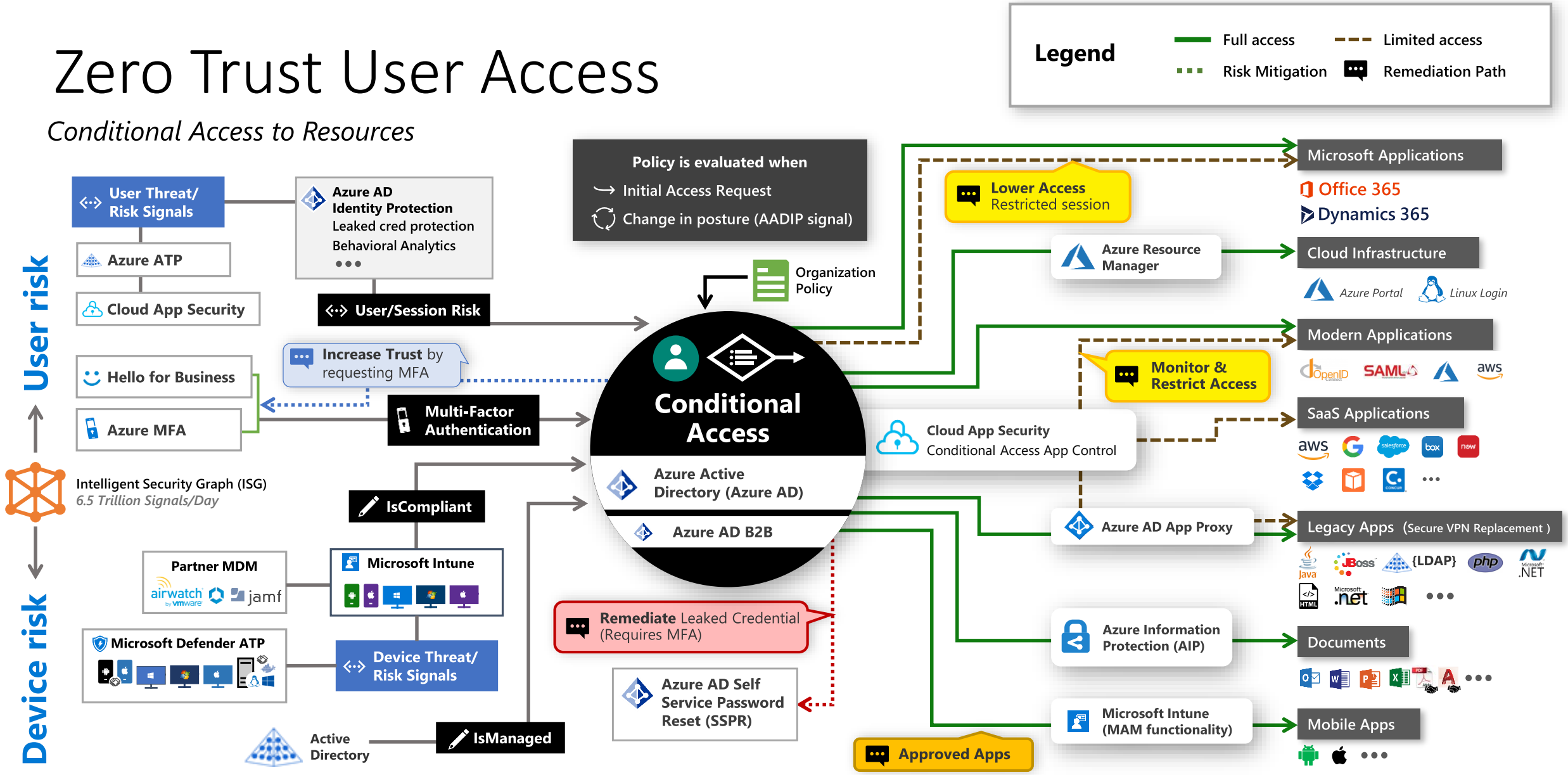
Counter Measures

- Shift toward “Zero Trust” security models that safeguard identities over perimeter-based protection
- Focus on Identity based Zero Trust security to reduce organization risk while simultaneously improving end user experience
- Industry partnerships on identity solutions through groups like FIDO to reach scale needed and combat modern threats, through biometrics and other authentication tools



Zero Trust User Access

Conditional Access to Resources



Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

Microsoft

05

Greater nation state activity + political & social disruptions

Microsoft

05 Greater nation state activity + political & social disruptions

Risks

- Microsoft Threat Intelligence Center is aware of more than 110 Activity Groups engaged in malicious cyber activity worldwide
- Adversaries continue to target political campaigns with phishing attacks, and social platforms remain primary sources of misinformation campaigns
- EG: Efforts to disrupt or influence US elections in 2016 were a watershed moment in the industry

Microsoft

05 Greater nation state activity + political & social disruptions

Counter Measures

- Microsoft pairs world-class cyber defenders like the MSTIC team with unique insights from 8T daily signals to identity and track Activity Groups associated with state sponsored activity

- EG: Defending Democracy Program to protect political campaigns from hacking and disinformation efforts

Microsoft

Counter Measures

- In October 2019 Microsoft disclosed that the threat group known as “Strontium” targeted 16 international sporting and anti-doping organizations across three continents ahead of the 2020 Tokyo Summer Games

- Education through industry wide efforts to create awareness on best practices and how to spot phishing scams or disinformation campaigns

Microsoft

Even as attackers continue to increase complexity of threat tactics and techniques, organizations need to embrace modern solutions

Would you like to:

- Document your **security strategy**, set-up measurements and clear roadmap for the benefit of key stakeholders?
- **Identify real threats** to your cloud environment by doing Threat Check?
- Better understand how to **accelerate your security journey** using the latest tools?

Ask your account manager or
Robert.Havranek@microsoft.com
for Security Workshop & Assessment.