Trustworthy Computing: Stay Secure and Productive in a connected, mobile world

Chris Papaphotis
Commercial and Partner Director, Microsoft
Cloud is transforming Technology
Technology is transforming Business

Our Customers need to evolve in the new Era while Building their Infrastructure on Trust
Technology is transforming Businesses

- 26% set a clear vision for digital transformation
  - Source: Digital Transformation Infographic by Forrester

- 19% believe their companies have the technology to transform
  - Source: Digital Transformation Infographic by Forrester

- 73% of Fortune 500 CEOs said pace of technology change is a challenge
  - Source: Fortune 500 CEO Survey
In a Connected, Mobile World, Cyber Threats are the **MAJOR IT RISK**

$3.0$ **TRILLION**  
Impact of lost *productivity and growth*

$3.5$ **MILLION**  
Average *cost of a data breach*  
(15% YoY increase)

$500$ **MILLION**  
Corporate *liability* coverage.

“**CYBER SECURITY IS A BUSINESS OWNER ISSUE.**”
Evolving Threats:

- **Mischief**
  - Script Kiddies
  - Unsophisticated

- **Fraud and Theft**
  - Organized Crime
  - More sophisticated

- **Damage and Disruption**
  - Nations, Terror Groups, Activists
  - Very sophisticated and well resourced
Data Breaches & Cybercrime

France fines Google nearly $57 million for first major violation of new European privacy regime

Google to shut down Google+ after failing to disclose user data leak

Company didn’t disclose leak for months to avoid a public relations headache and potential regulatory enforcement

Hilton was fined $700K for a data breach. Under GDPR it would be $420M

Facebook says data breach affected 29 million users

The company said it would message affected users over the coming days to tell them what type of information had been accessed in the attack.
Traditional Workplace

- Single Device
- Business Owned
- Corporate Network & Legacy Apps
- Manual
- Reactive
- High-touch

Modern Workplace

- Multiple Devices
- User and Business Owned
- Cloud Managed & SaaS Apps
- Automated
- Proactive
- Self-Service
Company-owned and personal devices
In the Era of Cloud Apps and Mobility, IT goes beyond legacy Infrastructure.
The market is segmented and confusing

- Discovery
- Identity governance
- Single-sign on

Mobile Device & Application Management
- Conditional access
- Cloud visibility

Identity & Access Management
- Cloud Access Security Broker

Data Loss Prevention
- Mobile Data Loss Prevention
- Cloud Data Loss Prevention

Secure collaboration

Cloud Access Broker

Data Loss Prevention

Information Rights Management
- User & Entity Behavioral Analytics

SIEM

Cloud anomaly detection

Threat Detection

Secure collaboration

Identity & Access Management
- Cloud Data Loss Prevention
Enterprise Security without compromising Productivity

Holistic and innovative solution for protection across users, devices, apps and data

Mobile device & app management

Threat protection

Identity and access management

Information protection

Protect at the front door

Protect your data anywhere

Detect & remediate attacks
Windows 10 Security on Modern Devices
(Fresh Install or upgraded from 64-bit Windows 8)

**Virtualization Based Security**
- UEFI Secure Boot
- Windows Trusted Boot
- Windows Update
- Trusted Platform Module

**Mobile device & app management**
- SmartScreen
- Windows Firewall
- Windows Defender
- Microsoft Edge

**Threat protection**
- System Guard
- Credential Guard

**Information protection**
- Windows Information Protection
- BitLocker Admin and Monitoring

**Identity and access management**
- Windows Hello Companion Devices
- Windows Hello

**Detect and Remediate Advanced Attacks**
- BitLocker
- BitLocker to Go
- Windows Defender Advanced Threat Protection

**Security Management**
- Conditional Access
- Detect and Remediate Advanced Attacks
Built in to Windows
No additional deployment & infrastructure. Continuously up-to-date, lower costs.

Behavior-based, cloud-powered breach detection
Actionable, correlated alerts for known and unknown adversaries. Real-time and historical data.

Rich timeline for investigation

Unique threat intelligence knowledge base
Unparalleled threat optics provide detailed actor profiles 1st and 3rd party threat intelligence data.
Enable Mobile Productivity without compromising Security

**Mobile Productivity**
Enable a mobile experience that works the way employees want it to.

- Device choice
- Easy access to resources
- Self-service options
- Familiar Office apps

**Data Protection**
Ensure that the right data protection is applied to the right scenarios.

- User, device, app, file control
- Conditional access
- Protection after access

**Management**
Tools and services that empower IT pros to do strategically more with less.

- Unified management
- Cloud-based scalability and reliability
- 24/7 Deployment support
Microsoft 365
Digitally Transforming the Modern Workplace

Lead your Customers to Cloud with Modern Desktop deploying Genuine Windows 10 & Office 365. Evolve to Microsoft 365.

- Creativity
- Communication
- Collaboration
- Productivity
- Security & Compliance
- Simple Administration
- Lower TCO
- New culture of Work

Unlocks creativity
Built for teamwork
Integrated for simplicity
Intelligent security

Turn ideas into action with simplified, intelligent services across all devices.
Connect people, data, and insights with a universal toolkit that fosters collaboration.
Stay productive and up to date with simple, unified tools and predictable processes.
Protect your information, apps, and identities with comprehensive, proactive enterprise security.
Microsoft cloud services make it easier to locate and identify the personal data you collect, so you can more easily find and evaluate the data across your organization.

Microsoft cloud services make it possible to centralize processing by more effectively managing applicable policies, data categorizations, and use cases.

Microsoft cloud services synthesize threat intelligence and provide tools that help you get the greatest benefit from that intelligence for your security efforts.

Microsoft cloud services centralize and streamline technical and administrative steps that are required for compliance, such as demonstrating due diligence and handling data access requests.

<table>
<thead>
<tr>
<th>Discover</th>
<th>Manage</th>
<th>Protect</th>
<th>Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft cloud services make it easier to locate and identify the personal data you collect, so you can more easily find and evaluate the data across your organization.</td>
<td>Microsoft cloud services make it possible to centralize processing by more effectively managing applicable policies, data categorizations, and use cases.</td>
<td>Microsoft cloud services synthesize threat intelligence and provide tools that help you get the greatest benefit from that intelligence for your security efforts.</td>
<td>Microsoft cloud services centralize and streamline technical and administrative steps that are required for compliance, such as demonstrating due diligence and handling data access requests.</td>
</tr>
</tbody>
</table>

**Office & Office 365:**
- Data Loss Prevention
- Advanced Data Governance
- Office 365 eDiscovery

**Enterprise Mobility + Security (EMS):**
- Microsoft Cloud App Security

**Windows 10:**
- PowerShell

**Dynamics 365:**
- Audit Data and User Activity
- Report & Analytics with Dynamics 365
- Dynamics 365 metadata & data models

**SQL Server and Azure SQL Database:**
- SQL Query Language

**Microsoft Azure:**
- Microsoft Azure Data Catalog

**Windows 10 & Windows Server 2016:**
- Microsoft Data Classification Toolkit

**Office & Office 365:**
- Advanced Data Governance

**Enterprise Mobility + Security (EMS):**
- Microsoft Azure Information Protection

**Windows 10:**
- Permissions

**Dynamics 365:**
- Security concepts for Microsoft Dynamics 365

**Enterprise Mobility + Security (EMS):**
- Microsoft Azure Information Protection

**SQL Server and Azure SQL Database:**
- Azure SQL Database firewall
- SQL Server authentication
- Dynamic Data Masking (DDM)
- Row-Level Security (RLS)
- Transparent Data Encryption
- Always Encrypted
- Auditing for SQL Database and SQL Server audit
- SQL Database Threat Detection

**Microsoft Azure:**
- Azure Security Center
- Data Encryption in Azure Storage
- Azure Key Vault
- Log Analytics

**Windows 10 & Windows Server 2016:**
- Windows Hello
- Windows Defender Antivirus
- Windows Defender Advanced Threat Protection
- Device Guard
- Credential Guard
- BitLocker Drive Encryption
- Windows Information Protection
- Shielded Virtual Machines
- Just Enough Administration and Just in Time Administration

**Office & Office 365:**
- Advanced Threat Protection
- Threat Intelligence
- Advanced Security Management
- Office 365 Audit Logs

**Windows 10:**
- Windows Defender Advanced Threat Protection (ATP)

**Dynamics 365:**
- Report & Analytics with Dynamics 365

**Microsoft Azure:**
- Azure Auditing and Logging
BUSINESS IS BUILT ON TRUST. TRUST IS BUILT ON GENUINE

PROTECT YOUR IT INVESTMENT USING MODERN DEVICES WITH PROPERLY LICENSED SOFTWARE

Identity and Access Management

Threat Protection and Information Protection

Compliance and Data Protection

Virtualization Based Security / Advanced Threat Protection

BUSINESS IS BUILT ON TRUST.

TRUST IS BUILT ON GENUINE

PROTECT YOUR IT INVESTMENT USING MODERN DEVICES WITH PROPERLY LICENSED SOFTWARE
<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of corporate/personal data</td>
<td>46%</td>
</tr>
<tr>
<td>Unauthorized access</td>
<td>40%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>30%</td>
</tr>
<tr>
<td>System outages/downtime</td>
<td>28%</td>
</tr>
<tr>
<td>Time and cost to disinfect</td>
<td>25%</td>
</tr>
<tr>
<td>Loss of IP/proprietary information</td>
<td>24%</td>
</tr>
<tr>
<td>Costs to deal with breaches</td>
<td>22%</td>
</tr>
<tr>
<td>Impact on customers</td>
<td>21%</td>
</tr>
<tr>
<td>Impact on organization reputation</td>
<td>20%</td>
</tr>
<tr>
<td>Cost to prevent</td>
<td>13%</td>
</tr>
</tbody>
</table>

Source: BSA
## CIOs Report the Top Benefits of Strong Software Compliance

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower security risks</td>
<td>54%</td>
</tr>
<tr>
<td>Less risk of legal issues</td>
<td>43%</td>
</tr>
<tr>
<td>Increased IT productivity</td>
<td>35%</td>
</tr>
<tr>
<td>Protection of corporate brand</td>
<td>28%</td>
</tr>
<tr>
<td>Customer or trading partner satisfaction</td>
<td>26%</td>
</tr>
<tr>
<td>Increased end user productivity</td>
<td>26%</td>
</tr>
<tr>
<td>Lower software costs</td>
<td>20%</td>
</tr>
<tr>
<td>Less disruption from audits</td>
<td>19%</td>
</tr>
<tr>
<td>Better relationship with vendors</td>
<td>16%</td>
</tr>
</tbody>
</table>

Source: BSA
Workshop:
A survival guide on building a secure IT Infrastructure in Modern Workplace
It is very likely that Customers are victims of Piracy when:

- **Software price is too good to be true.**
- **Software comes from file sharing apps or is circulated through email, social networks or websites.**
- **Product keys are sold separately from software or they come in bundles of multiple product keys.**
- **Packaging has been opened or is not standard Microsoft packaging.**
- **Product key or installation code doesn't work, or the software cannot be activated.**
- **Software comes in non-standard or unprofessional packaging.**
- **They are asked to download files to complete activation.**
- **Their PC or other device comes with software already activated.**
THANK YOU