TURNING THE TABLES

Dean Iacovelli
Director, Secure Enterprise
Microsoft State and Local Government
deaniac@microsoft.com
Asymmetrical: this is not a fair fight
You are facing a profit-motivated human adversary
They use your transparency against you
Attacks are now automated, response is not
You can’t just throw people at the problem
Complexity is the chief enemy of security
Breach costs can be enormous and are asymmetrical to org size
SLG 2nd lowest preparedness, 2nd most attacked by industry
76% of breaches financially motivated
90% of attacks begin with phishing email
One bank: 62,000 devices encrypted in 1 hr by Petya
1.8M global unfilled cyber jobs by 2022
Managing 20-30 tools = 5% alert investigation rate
See OPM
“Best of breed” approach can no longer keep up with rate and sophistication of attacks.

“Going it alone” as an individual org with individual org resources is a losing battle.

Basically, all roads lead to CLOUD and AUTOMATION.
"By 2020, 30% of security spending will be on vendors that provide an integrated platform approach to security” – 2017 IDC FutureScape report
AN ARGUMENT FOR UTILITY COMPUTING IN THE CYBER FIGHT

- Hyperscale cloud vendors will far outspend even the Fortune 5 on security because their business model is TRUST.
- Radically different economics - customers get access to 1B in cyber spend, only pay for a “slice”.
- Move to cloud is part of a sound risk management strategy – i.e. transferring risk
- Cloud helps you stay continually patched and compliant
- Certs AND a track record
<table>
<thead>
<tr>
<th>Action</th>
<th>Self-service</th>
<th>Fast Track</th>
<th>Premier</th>
<th>MCS</th>
<th>Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy Azure Backup and Recovery services</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Move doc stores to OneDrive for Business</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Automate info protection and classification</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Deploy Win 10 and Cred Guard to all clients.</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Deploy Endpoint Protection with automated investigation/remediation.</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Monitor and reduce time-to-patch</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Deploy next gen Security Information and Event Management tools</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Deploy behavior-analysis content scanning</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Leverage Microsoft Secure Score best practices across Identity, Office 365, Windows clients and servers.</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Deploy phishproof identities for all users, including Just-In-Time and Just-Enough admin accounts.</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
FINALLY, PLEASE REMEMBER...

BRAKES ARE WHAT ALLOW THE CAR TO GO FASTER.
Q & A
THANK YOU!
Dean lacovelli
deaniac@microsoft.com
“WHAT HAPPENED AT THE CITY OF XXX?”

<table>
<thead>
<tr>
<th>ENTRY</th>
<th>RECON</th>
<th>ESCALATION</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHISHING</td>
<td>Target recon</td>
<td>Pass the hash</td>
<td>Own domain</td>
</tr>
<tr>
<td>Spear, whaling, trusted user</td>
<td>Network traversal</td>
<td>Pass the ticket</td>
<td>Delete backups</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>Mailbox persistence</td>
<td></td>
<td>Exfiltrate data</td>
</tr>
<tr>
<td>Brute force, spray</td>
<td></td>
<td></td>
<td>Redirect funds</td>
</tr>
<tr>
<td>KNOWN VULNERABILITIES</td>
<td></td>
<td></td>
<td>Ransom</td>
</tr>
<tr>
<td>OS, database, apps</td>
<td></td>
<td></td>
<td>Botnet</td>
</tr>
</tbody>
</table>

Video
Our most unique global asset in the fight, informed by trillions of feeds. Machine learning helps sort the signal from the noise. This signal is leveraged across all of Microsoft’s security services.

1.2B devices scanned each month

200+ global cloud consumer and Commercial services

Malware data from Windows Defender

Botnet data from Microsoft Digital Crimes Unit

Shared threat data from partners, researchers and law enforcement worldwide

18+B Bing web pages scanned

750M+ Azure user accounts

400B emails analyzed

Enterprise security for 90% of Fortune 500

1.2B devices scanned each month

450B monthly authentications

1.2B devices scanned each month

200+ global cloud consumer and Commercial services

Malware data from Windows Defender

Botnet data from Microsoft Digital Crimes Unit

Shared threat data from partners, researchers and law enforcement worldwide

18+B Bing web pages scanned

750M+ Azure user accounts

400B emails analyzed

Enterprise security for 90% of Fortune 500

1.2B devices scanned each month

450B monthly authentications