Worried about **cybercriminals** taking down your business?

OUTSMART THEM WITH WINDOWS 10

The Threat Landscape is **CHANGING**

The threat landscape has evolved dramatically in recent years. It seems every day we hear another headline about an organization getting breached. We've responded by changing the architecture of Windows 10 so that we're not just building bigger walls against these attacks; we're locking the criminals out. Windows 10 provides a comprehensive set of protections against modern security threats.

IMPACT OF SECURITY BREACH TO BUSINESS:

$3.5 mil

AVERAGE COST OF A DATA BREACH PER INCIDENT

Source: Ponemon. (2014). 2014 Cost of Data Breach: Global Analysis.

2x

According to a recent survey of CIOs, **security spending is increasing at double the rate of overall investment.**

Source: Source: McCarthy, John C.. Brief: technology spending is reaching a tipping point. Forrester Research, Inc.. December 11, 2014.

IDENTITY PROTECTION

75% **of individuals use only three or four passwords** across all of their accounts.

Source: http://www.securityweek.com/study-reveals-75-percent-individuals-use-same-password-social-networking-and-email

PROBLEM: **Passwords are not secure.** Others can access your corporate network by pretending to be you.

SOLUTION: Windows 10 introduces an alternative to passwords with **Windows Hello**[1] and **Credential Guard**[2] that is easy to deploy and use, and safeguards from pass the hash attacks.

INFORMATION PROTECTION

87% **of senior managers** have leaked corporate data to unmanaged personal locations.

Source: Sirote Friedberg. "On The Pulse: Information Security Risk in American Business." 2013.

57% of us have sent data to the wrong person.

Source: Gross, Art. "A look at the cost of healthcare data breaches." HIPAA Secure Now, March 30, 2012.

SOLUTION: Windows 10 provides **Bitlocker**[3] and **Windows Information Protection**[4], with data encryption at the device and now file level, to help ensure corporate data isn't accidentally or intentionally leaked to unauthorized users or locations.

THREAT RESISTANCE

PRE-BREACH

MORE THAN

300,000

New malicious files are being created every day and spread through the internet.

Source: http://www.kaspersky.com/about/news/virus/2013/number-of-the-year

SOLUTION: Windows 10 provides enterprise grade anti-virus protection with **Windows Defender** in-box, **Microsoft Edge**, a sandboxed browser, and **Device Guard** that completely locks down your device, so you can run only trusted applications.

POST-BREACH

200+ DAYS

An attacker can go undetected in your environment, now that people are bringing their own devices to work—that's scary.

Source: Mandiant. (2016). M-TRENDS 2016. Milpitas: Mandiant Consulting.

BONUS: **Windows Defender Advanced Threat Protection** is a new service that enables Windows enterprise customers to detect, investigate, and remediate advanced persistent threats and data breaches on their networks.

DEVICE SECURITY

Addressing todays cyber-threats requires more than software, it requires the combination of hardware compatibility and software to address the modern day attacker.

SOLUTION: Windows 10 offers **UEFI Secure Boot** and **Virtualization Based Security** to help ensure that a genuine version of Windows starts first on your device, and moves some of the most sensitive Windows processes into a secure execution environment to help prevent tampering and prevent attackers from evading detection.

STAY ON THE OFFENSE AGAINST CYBERCRIME BY PROTECTING YOURSELF WITH

WINDOWS 10

1 - Windows Hello requires specialized hardware, including fingerprint reader, illuminated IR sensor, or other biometric sensors.
2 - Requires UEFI 2.3.1 or greater with Trusted Boot; Virtualization Extensions such as Intel VT-x, AMD-V, and SLAT must be enabled; x64 version of Windows; IOMMU, such as Intel VT-d, AMD-Vi; BIOS Lockdown; TPM 2.0 recommended for device health attestation (will use software if TPM 2.0 not present)
3 - Requires TPM 1.2 or greater for TPM based key protection.
4 - Windows Information Protection, formerly Enterprise Data Protection (EDP), requires either Mobile Device Management (MDM) or System Center Configuration Manager to manage settings. Active Directory makes management easier, but is not required.