WINDOWS DEFENDER
ADVANCED THREAT PROTECTION (**ATP**)

A service that enables enterprise customers to **detect, investigate, and respond to advanced and targeted attacks** on their networks

200+ days
attackers are present on a victims network before detection

Source: http://www.fireeye.com/news-events/press-releases/read/fireeye-releases-annual-mandiant-threat-report-on-advanced-targeted-attacks

80 days
after detection to full recovery

Source: Infosec Institute, "The Rise of Cyber Weapons and Relative Impact on Cyberspace"

$3 trillion
Impact of lost productivity and growth

Source: http://www.mckinsey.com/insights/business_technology/why_senior_leaders_are_the_front_line_against_cyberattacks

$3.5 million
average cost of a data breach (15% YoY increase)

Source: http://www.ponemon.org/blog/ponemon-institute-release-2014-cost-of-data-breach-global-analysis

Windows 10 is the **most secure enterprise platform** today

Building on the existing security defenses Windows 10 offers today (pre-breach), we have developed Windows Defender Advanced Threat Protection (ATP). It provides enterprises a post-breach layer of protection to the Windows 10 security stack.

Windows Defender Advanced Threat Protection

Protect
Today's cloud-first, mobile-first world demands the highest level of identity & data security.

Detect
Comprehensive monitoring tools to help you spot abnormalities and respond to attacks faster.

Respond
Leading respose and recovery technologies plus deep consulting expertise.

Protecting our enterprise customers has never been more challenging.

Even the best endpoint defenses will be breached eventually as cyberattacks become more sophisticated and targeted. Sophisticated attackers are using social engineering, zero-day vulnerabilities, or even misconfigurations to break into networks.

MALWARE & VULNERABILITIES
are not the only thing to worry about

46%
of compromised systems had **no malware** on them

99.9%
of exploited vulnerabilities were used **more than a year after** the CVE was published

FAST PHISHING ATTACKS
give you little time to react

23%
of recipients **opened phishing messages** (11% clicked on attachments)

50%
of those who open and click attachments do so **within the first hour**

ONLY 40% OF ATTACKS use malware as the means of carrying out attackers' goals. The rest consist of adversarial activity that doesn't use malware for which signatures can be written. The better way is to detect these attacks with behavioral analysis.

Source:
Ponemon Institute, "The Post Breach Boom", 2013
Ponemon Institute, "2014 Global Report on Cost of Cyber Crime"
Mandiant 2014 Threat Report

Why **Windows Defender ATP**

Windows Defender ATP gives you the ability to detect, investigate and remediate Advanced Attacks and data breaches on your networks.

Detecting the undetectable
Sensors built deep into the operating system kernel, Windows security experts, and unique optics from over 1B machines and signals across all Microsoft services.

Built in, not bolted on
Agentless with high performance and low impact, cloud-powered; easy management with no deployment.

Single pane of glass for windows security
Explore 6 months of rich machine timeline that unifies security events from Windows Defender ATP, Windows Defender Antivirus and Device Guard.

The power of the Microsoft graph
Leverages the Microsoft Intelligence Security Graph to integrate detection and exploration with Office 365 ATP subscription, to track back and respond to attacks.

Windows Defender ATP is composed of three parts:

The Client
The client logs relevant security events and behaviors from the endpoint using the end-point behavioral sensor, built into Windows 10 (Windows 10 Anniversary update, Windows Insider Preview Build number 14332 and later) and activated upon service enrollment.

Cloud analytics service
The cloud analytics service runs on the Microsoft scalable big data platform and uses a combination of Indicators of Attacks (IOAs), generic analytics and machine learning rules, as well as Indicators of Compromises (IOCs) collected from past attacks. It processes data from endpoints in combination with historical data and Microsoft's wide data repository to detect anomalous behaviors, adversary techniques and similarity to known attacks.

Microsoft and community intelligence
Our Hunters and researchers investigate the data, finding new behavioral patterns and correlating the data with existing knowledge from the security community.

STAY ON THE OFFENSE AGAINST CYBERATTACKS BY PROTECTING YOUR ENTERPRISE BUSINESS WITH **WINDOWS DEFENDER ATP**

LEARN MORE: **aka.ms/windows-atp**

Microsoft