Microsoft

Cyber threats require an ongoing and relentless focus on security

Microsoft Secure—Protecting from Evolving Security Threats Part 1

Cloud computing, mobile devices, the Internet of Things, and the increasing digitization of information and processes in a hybrid computing environment present new challenges to securing data and information.

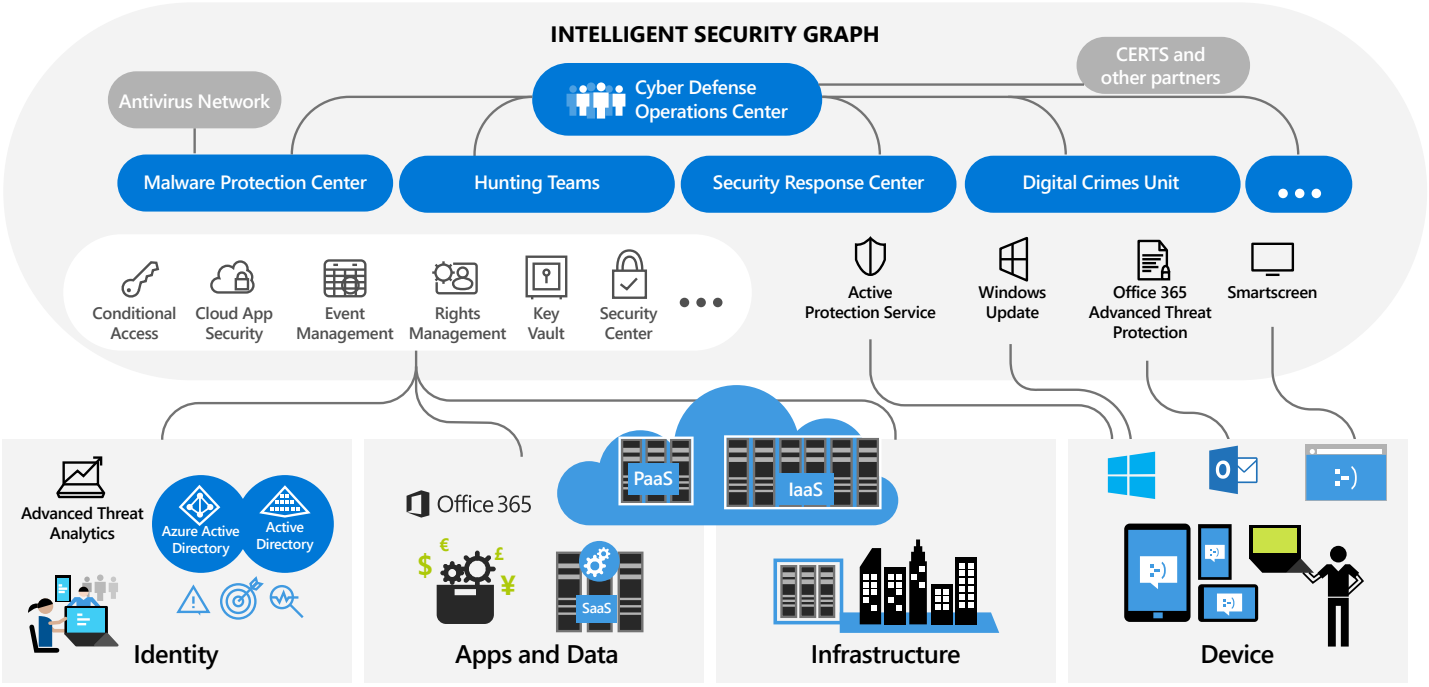
The cyber-threat landscape of today requires an ongoing and relentless focus on security, especially when considering that many current government security, privacy and compliance policies were developed in an on-premises only environment, and where **regulation and policy traditionally lag innovation.** That's why we're using this blog to kick off an ongoing series on security for government agencies.

Citizens expect always-on secure, mobile, smart phone enabled digital services connected to massive hyper-scale clouds and telco bandwidth. Securely delivering these same capabilities to agency information workers and citizens can be challenging, given **the average time between breach and detection is typically over 140 days.** To put that into context: on average, an attacker exists within a company's or agency's infrastructure—free to gather information or worse—for almost four-and-a-half months before being found. It's not that agencies aren't employing security best practices but the reality is all the protection in the world can't stop a determined hacker.

What agencies need to do is shift their focus from a protection-only approach to include equal, if not more, focus on detection after the fact so that they can get the 140 days down to minutes between infiltration and detection. They need to take an "assume breach" mentality. When you approach security as if your environment has already been compromised, you start thinking about how to detect compromises early and recover quickly. Shifting from passive-defense to active-defense changes your security posture—you're aware, you're prepared, you're ready to act.

At Microsoft, we've evolved beyond point solutions that address individual security concerns one product at a time and are using machine learning to identify and detect issues early and accurately using an assume breach approach. Our **"built-in" security methods** now enable you to be vigilant from a high level on all fronts. For example, when a new software-as-a-service app is being used by your employees, you can detect it immediately and get data about what risks and threats it may pose to your agency.

MICROSOFT **PROTECTING YOU**



Microsoft has a **vast cyber footprint.** We receive anonymized telemetry from billions of logins, devices and services, on both private and public clouds. Combining that with machine learning, behavioral inspection and expert human analysis, we can detect and respond to what looks like anomalous behaviors and incorporate that to prevent a potential threat. This intelligence is built into our products and solutions to give you visibility and insights into potential compromises. Our cybersecurity experts in the **Digital Crimes Unit** and the **Cyber Defense Operations Center** monitor all this information to identify real threats. This combination of machine learning and human vigilance equals holistic protection.

To help government agencies protect their data from these new and emerging threats, we have capabilities that can be used in concert with existing security solutions. Please stay tuned for our next blog in this series, focusing on **Windows 10 security.** In the meantime, feel free to take advantage of the following Microsoft resources as part of your agency's ongoing and relentless focus on security:

Agencies can start protecting against identity compromise with an enterprise-grade, identity-driven security solution:

- Enterprise Mobility Suite Security

Discover, control and protect cloud applications:

- Microsoft Cloud App Security
- Office 365 Advanced Security Management

Protect against data leakage:

- Microsoft Azure Rights Management
- Office 365 Data Loss Prevention
- Windows BitLocker
- Windows Information Protection
- Azure Information Protection

Protect against malware and phishing attacks:

- Exchange Online Advanced Threat Protection

Respond to compliance and security incidents:

- Office 365 Customer Lockbox
- Office 365 Advanced eDiscovery

Windows 10 for government agencies: helping protect, detect and respond to cyber-attacks

Microsoft Secure—Protecting from Evolving Security Threats Part 2

The number $3.5 million is a huge financial amount—and a figure that troubles every CIO. That's because $3.5 million is the average cost of a single data breach. Even more alarming is the estimated $3 trillion in lost productivity and growth each year, according to **McKinsey & Company** research.

While cybersecurity is top-of-mind for all CIOs, our federal government agencies have even more at stake than material risk: protecting our national security, intelligence and information. State and local government (SLG) organizations also must safeguard extremely sensitive data, including personally identifiable information.

Federal agency and SLG networks are under attack virtually every day and, despite strong cyber-defense initiatives, challenges remain to thwart malicious hackers. That's why I'm always eager to meet with federal and SLG CIOs and IT teams to explain how Windows 10 is disrupting increasingly sophisticated cyber-attacks through revolutionary security measures. This is especially true since the U.S. Department of Defense directed **all DoD agencies to standardize on Windows 10**—the largest enterprise deployment to date—and recent news that **Windows 10-powered Surface devices have gained approval for classified workloads**. Note: this blog is the second in our ongoing **Microsoft Secure—Protecting from Evolving Security Threats** series.

Protect, detect and respond are the core elements of our Windows 10 security mission statement. Our goal for federal, SLG and all customers is to enable Windows 10 devices to be protected from today's sophisticated attacks and, if a breach does occur, provide immediate visibility to respond. **Windows 10 carries out the protect-detect-respond mission through four pillars of built-in defense:**

Device (hardware) protection

Threat resistance

Identity protection

Information protection

Device (hardware) protection

We recognized that older hardware was susceptible to attacks since hackers could more easily drop malicious code onto devices as a **rootkit** before the operating system starts up. As a result, we've made device protection requirements much more robust for manufacturers of Windows 10 devices. By implementing a more modern and secure replacement for BIOS (basic input/output system) for device startup called **UEFI** (Unified Extensible Firmware Interface) Secure Boot, introducing virtualization-based security protection and mandating the use of **Trusted Platform Module**, Windows 10 devices can address hardware-level tampering. Windows 10 device protection is especially important to federal and SLG customers as they replace older, more vulnerable PCs.

Threat resistance

Threat resistance is aimed at addressing viruses, Trojans and malware that can result from clicking on unsafe website links opening up executables and documents that look legitimate but are not. The newest forms of Windows 10 threat protection include **Device Guard** and **Microsoft Edge Application Guard**, which join **Microsoft Edge**, **Windows Defender**, **Windows Firewall** and **SmartScreen**. These technologies work together to provide comprehensive threat resistance since most cyber-attacks are aimed at end users either clicking on legitimate-looking websites, opening malicious email or running harmful apps. This is especially the case for federal and SLG agencies, which recognize that user desktops or PCs are often a primary point of attack.

Identity protection

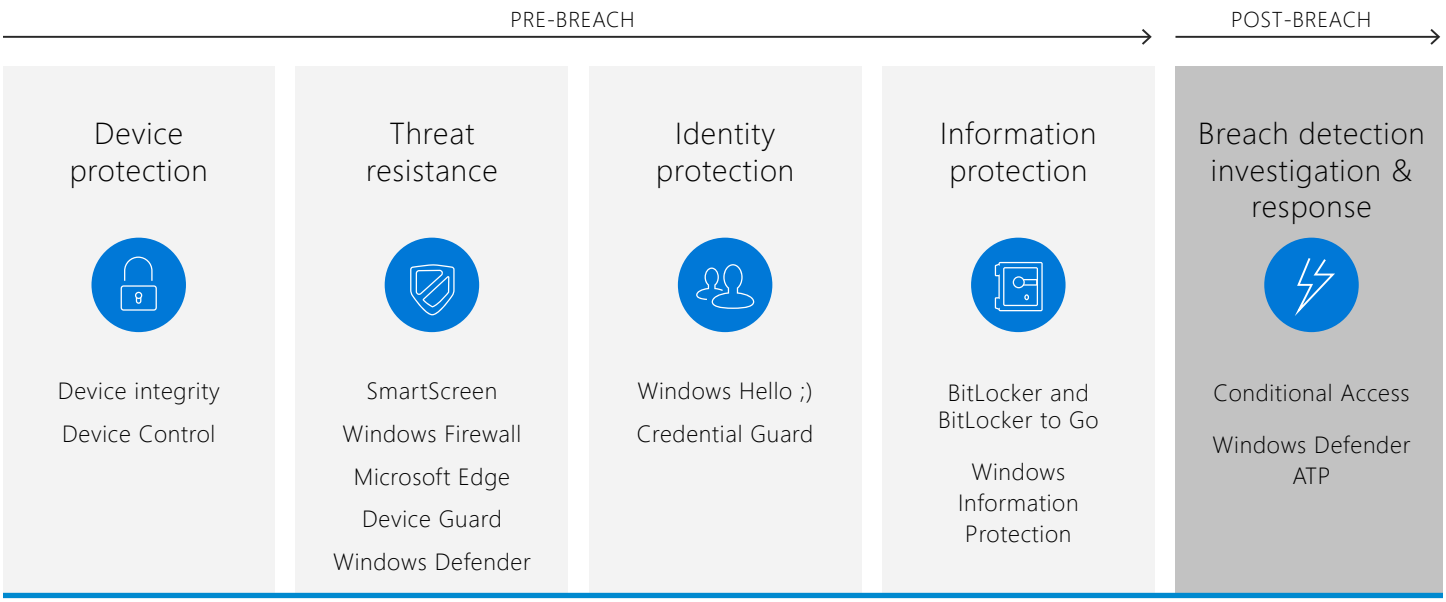
One of the ways that government agencies have been attacked is through compromise or theft of a user's password or credentials, allowing a hacker to retrieve sensitive data or inject malware on a network. We're defending against attacks like "pass the hash" on Windows 10 through **Credential Guard**, which provides authentication services through a virtualized, secure "kernel" that defends a user's passwords and credentials. Credential Guard coupled with **Windows Hello for Business** deliver a superior level of protection for user login, passwords and credentials. Identity protection is a key concern to government agencies due to potential compromises to national intelligence, employee records and other sensitive information.

Information protection

Information is moving around all the time and Windows 10 has many technologies to provide integrated protection against accidental data loss. **BitLocker** and **BitLocker to Go**, along with **BitLocker Admin and Monitoring**, provide comprehensive data at rest **Windows Information Protection**. **Azure Rights Management** encrypts and restricts files so that they are rendered useless if such data should fall into the wrong hands—especially important in the federal and SLG space.

THE **WINDOWS 10** DEFENSE STACK

PROTECT, DETECT & RESPOND



Windows 10 also leads the way in **breach detection, investigation and response**. In today's modern world of cyber threats, we must always assume there's potential for a breach so it's vital to be able to detect advanced threats and have remediation tools to respond. With the newest version of Windows 10, we've introduced post-breach protection with **Windows Defender Advanced Threat Protection**, which provides a security center portal to identify if, where and how an attack is taking place, and provide insights about who the attackers might be. These "post-breach" technologies are enhanced when coupled with **Office 365 Advanced Threat Protection** and **Advanced Threat Analytics**.

When talking about the benefits of Windows 10 security for federal and SLG customers, I would be remiss if I didn't mention that our newest operating system complies with key U.S. government certifications, including: **NIST Federal Information Processing Standard (FIPS) 140-2,** Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs) for **desktop** and **mobile**, **Common Criteria** and others required by U.S. agencies. Our engineering teams work diligently to ensure Windows 10 and other Microsoft products meet the most stringent security mandates and certification programs.

In addition to the links embedded throughout this blog, you can learn more about Windows 10 security features that **protect, detect** and **respond** at the following sites:

- **Windows 10 Security Overview**
- **Keep Windows 10 Secure guides**
- **Windows 10 Security Hardware Requirements**
- **Windows 10 Threat Resistance Overview**

Strengthening cybersecurity for federal government agencies

Microsoft Secure—Protecting from Evolving Security Threats Part 3

Cloud computing, mobile devices, the internet of things (IoT) and the increasing digitization of information in a hybrid computing environment present new challenges to securing data in what was once an on-premises-only environment.

Adding to the challenge is the fact that the average time between breach and detection is typically **over 170 days, per the Ponemon Institute.** This can leave government agencies vulnerable to compromising highly sensitive information, potentially paralyzing services and costing millions in lost productivity. With threats evolving and the reality that all the protection in the world can't stop a determined hacker, our federal government must be vigilant in protecting our country's data and information from malicious attacks, such as the **recent WannaCrypt attack.**

The significance of addressing security also was emphasized in the recent **Presidential Executive Order** that is requiring all agencies to meet and document compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) within a limited window of time. Today, we released an **Azure Blueprint Customer Responsibilities Matrix** (CRM) for the NIST CSF.

The Matrix explicitly identifies the NIST CSF controls where an agency customer holds responsibility for control implementation. The CRM also provides detail on controls that Microsoft Azure implements on the customer's behalf and how **Azure Government** meets the NIST CSF requirements.

At Microsoft, we are committed to helping our customers comply with the NIST CSF in our government cloud and on-premise solutions. In the new world we live in, the security paradigm has changed to an approach where:

- Identity is the firewall, with tools such as **Azure Active Directory** securing a user's identities
- Devices are the perimeter, with **Microsoft Enterprise Mobility + Security** and **Office 365 for U.S. Government** helping devices stay secure
- Assume breach" is the security model

Against this backdrop, we continue to focus on helping customers—especially government agencies—implement initiatives to protect, detect and respond to breaches.

Holistic, cloud-based protection

To help thwart attacks, we have found that a holistic, end-to-end approach is needed, with hardware, infrastructure and applications protected through the latest threat intelligence that only cloud computing can provide. The May 11 executive order makes migrating to shared services and the cloud priorities for IT modernization and cybersecurity efforts.

Our **Azure Government** cloud platform serves nearly 6 million government users across 7,000-plus federal, state and local organizations. Microsoft is committed to delivering secure, compliant cloud offerings and meeting the most stringent requirements specific to government agencies. For example:

- Microsoft is the only cloud provider that offers a cloud that is **DoD Impact Level 5 Provisional Authorization (PA)**-ready for infrastructure, platform and productivity services.
- Azure Government meets a **multitude of certifications and accreditations**, including **FedRAMP**, **FBI CJIS** agreements with 27 states, **HIPAA** and many more, which can be reviewed at our **"Check the facts: Not all clouds are created equal"** site.

Cybersecurity and infrastructure leadership

Just recently, I wrote about the **U.S. Department of Veterans Affairs** giving veterans access to healthcare information that is both clear and easy to understand through **Access to Care**, a new online tool powered by Azure Government and **SQL** Server technology. This is just one example of how our government shared-services cloud platform is enabling better support while helping to ensure security and compliance.

Microsoft also is using data science, machine learning, automation, behavioral analysis and expert threat researchers to forge the next generation of security solutions. Our **Intelligent Security Graph (ISG)** is informed by trillions of pieces of data from billions of devices we receive across our endpoints, consumer services, commercial services and on-premises technologies. This unique intelligence is built into our products and solutions to give customers visibility and insights into potential compromises. Our cybersecurity experts in the Digital Crimes Unit and the Cyber Defense Operation Center monitor all this information to identify real threats. This combination of artificial intelligence, machine learning and human vigilance equals holistic protection.

In addition to this post, you can learn more about our cybersecurity efforts at our **Microsoft Secure** site, by downloading our new white paper on **The Evolution of Malware Prevention** and in our ongoing **"Microsoft Secure—Protecting from Evolving Security Threats" blog series:**

- **Windows 10 for government agencies: helping protect, detect and respond to cyber-attacks**
- **Cyber threats require an ongoing and relentless focus on security**
- **Windows 10-powered Surface devices gain approval for classified workloads**

Lead your agency's digital transformation with Microsoft. **Learn more**

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES EXPRESS OR IMPLIED AS TO THE INFORMATION IN THIS DOCUMENT.
This document is provided "as-is." Information and views expressed in this document, including URL and other internet Web site references, may change without notice.

©2016 Microsoft Corporation. All rights reserved.