Microsoft technology solutions for cybersecurity

For every phase of this security management life cycle, Microsoft provides trusted advice and technology solutions that play a critical role in helping to ensure the safety and integrity of the enterprise.

Each and every day, cyber attacks against U.S. government computer networks number in the millions. Pentagon systems alone are probed 250,000 times per hour, according to Gen. Keith Alexander, the new head of the U.S. Cyber Command.[1] Whether the attackers' objectives are to steal sensitive data or to disrupt or destroy vital operations, their tools and techniques are growing increasingly sophisticated. To protect their important assets, all government agencies must take these threats seriously and meet them proactively with a system-wide defensive approach employing superior technology.

Microsoft envisions a cybersecurity defense framework that helps guide agencies through the continuous process of safeguarding their networks. The continuum of "protect, detect, respond, and recover" helps organizations anticipate dangers, neutralize and limit the impact of those dangers, and react quickly and effectively in the event of an incident. For every phase of this security management life cycle, Microsoft provides trusted advice and technology solutions that play a critical role in helping to ensure the safety and integrity of the enterprise. Here's how your agency can use them to put the idea of a 360-degree risk-management continuum into practice.

Protect

The first stage of the security management life cycle must focus on stopping attackers before they gain entry, so defenses that block malicious software and unauthorized access are critical. In addition, baseline configuration standards must be established and monitored to prevent deviation and noncompliance that can create vulnerabilities in the system.

These Microsoft products and technologies can help you to protect your IT infrastructure from threats and to establish consistent configuration standards.

- **Microsoft Forefront Protection 2010 for SharePoint** helps prevent malware and out-of-policy content from entering SharePoint libraries.
- **Microsoft Forefront Client Security** provides unified virus and spyware protection, simplified administration, and critical visibility and control.
- **Security technologies** in **Windows 7** and in **Windows Server 2008 R2** include features that can help you secure your networks and devices, including smart card logon, Windows BitLocker, Encrypting File System, AppLocker, Network Access Protection, Direct Access, Active Directory Rights Management Services (AD RMS), and updated Group Policy.
- **Microsoft System Center Configuration Manager** comprehensively assesses, deploys, and updates servers, client computers, and devices—across physical, virtual, distributed, and mobile environments—to help prevent risks from out-of-date systems and security software.
- **Microsoft Security Compliance Manager**, a downloadable tool, enables you to access and automate all of your organization's security baselines in one place.
- **Network Access Protection in Windows** monitors and evaluates the health of user systems before they are able to log on to a network.

Detect

To effectively detect and deter cyber threats, monitoring and analysis tools must provide an overall picture of an environment's security status. This means not only detecting attacks at the network perimeter but also identifying internal threats—whether suspicious activities or system weaknesses caused by drift away from defined security configurations.

These Microsoft products and technologies can help you detect internal and external threats to your IT infrastructure.

- **Forefront Client Security** helps monitor and detect viruses and spyware.
- **Forefront Threat Management Gateway** (TMG) helps users in your organization to use the Internet safely. TMG provides URL filtering, anti-malware inspection, intrusion prevention, application- and network-layer firewall, HTTP/HTTPS inspection, and more.
- **System Center Operations Manager Audit Collection Services** provides your organization with the tools to consolidate security logs into a centrally managed database and filter and analyze events using data analysis and reporting tools provided by Microsoft SQL Server.
- **DirectAccess**, a feature in the Windows 7 and Windows Server 2008 R2 operating systems, enables users to connect to your servers seamlessly, provides Internet Protocol security (IPSec) for authentication and encryption, offers optional smart card user authentication, and integrates with Network Access Protection to help ensure that users' computers comply with system health requirements.

Respond

In the event that your organization does experience an intrusion or disruption, having effective contingency plans, processes, tools, and competencies in place can help you react swiftly to contain and eradicate the threat. With timely incident reports, you can assess any system damage or data loss and move quickly to resume operations.

These Microsoft products and technologies can help you respond to security events.

- **Network Access Protection** can help your organization to move from reactive to proactive management and reaction and can assist with compliance reporting.
- **Microsoft Configuration Manager**, included in the System Center Configuration Manager 2007 Configuration Pack Catalog, includes Microsoft and third-party best practice configuration knowledge to help you better define and maintain system configuration.
- **Group Policy** and **System Center Configuration Manager** can also help you respond quickly to attacks and improve your organization's security posture when used with effective, carefully planned response procedures.

Recover

With recovery procedures and workarounds already thought out, your agency can quickly move forward after an attack to recover lost data or configuration information. Your agency can also move to restore systems and test to help ensure that all enterprise components are again in compliance and that mission assurance and confidence are restored. A continuing review of security audit files provides the opportunity to learn from the incident, so the lessons can be applied to help you improve existing security provisions and prevent a recurrence.

These Microsoft products and technologies can help you recover from attacks and intrusions.

- **Virtualization technologies**, including Windows Server 2008 Hyper-V and System Center Virtual Machine Manager, can assist in restoring new server and client systems based on known good, approved images.
- **Microsoft Configuration Manager**, by helping define and maintain system configuration, can assist in restoring a known good configuration or image after an attack.
- **Microsoft Desktop Optimization Pack**, available as a subscription for Software Assurance customers, includes virtualization technologies and manageability components that can help you recover and return to optimum operations more quickly.
- **Microsoft desktop optimization solution** can help you recover the desktop and laptop systems in your organization and reduce downtime in the case of an attack.
- **U.S. Government Configuration Baseline solution**, formerly known as Federal Desktop Core Configuration (FDCC), can help your organization to recover the standard configuration for your desktop systems quickly.
- **Federal Server Core Configuration (FSCC) solution** is a standardized server configuration that can also make recovery faster and more efficient.

The Microsoft commitment

In today's constantly evolving threat landscape, public sector agencies face unprecedented challenges in combating persistent, ingenious enemies. The need for a strong, comprehensive strategy for protecting government networks is clear. The cybersecurity defense framework lays out an effective road map for implementing that strategy. But the strategy must be supported with the right tools to make it a reality, and it's critical that the public and private sector ally themselves. Microsoft is committed to meeting that challenge, with its portfolio of business-ready security technologies and world-class solution services offerings that can help government agencies to successfully defend their information infrastructures—so they can focus more on their core missions and worry less about the next attack.

Contact cybersecurity@microsoft.com to arrange for an initial cybersecurity review or a cybersecurity workshop.

Learn more at microsoft.com/govsecurity.

[1] Security Threat.info. "Pentagon probed 6 million times daily." June 8, 2010. http://securitythreat.info/online-security-news/pentagon-probed-6-million-times-daily/

[2] Lockheed Martin. "Awareness, Trust and Security to Shape Government Cloud Adoption." April 2010. http://www.lockheedmartin.com/data/assets/isgs/documents/CloudComputingWhitePaper.pdf

Security in the cloud

A growing number of cloud computing services promise appealing cost savings and flexibility for government agencies. Yet cloud computing may seem risky due to many uncertainties. The cloud security perimeter is elusive—where are a cloud's boundaries for governance, risk management, and compliance? How do you ensure the security of data hosted in cloud data centers?

The Lockheed Martin Cyber Security Alliance conducted a survey of federal government, defense and military, and intelligence agencies. Their conclusion: The awareness, trust, and security issues that limit federal government adoption of cloud computing appear to be more perceptual than prohibitive.[2]

Whether you host information and services in data centers that are on your premises or in the cloud, the same security principles apply. You need a strategic and operational framework for cyber protection, detection, response, and recovery—in addition to the technology to carry out that strategy. You must look carefully at how well cloud providers protect key functions and sensitive data and then tailor your security tactics to the service you use, whether that service is software, databases, storage, or platforms.

When you are evaluating security in cloud services, take these issues into account:

- Be sure the vendor's technologies integrate with technologies you already use, such as Active Directory.
- Verify that the vendor can meet privacy requirements for your organization's data.
- Make sure the vendor employs policies and practices to prevent access violations.
- Ensure the vendor's location does not conflict with potential jurisdiction requirements. For example, you may be required to keep data within your legal jurisdiction.
- Review the vendor's security response plan, and be sure you know how and why the vendor will contact you.
- Based on the review, prepare a response that will coordinate with the vendor's plan.

The National Institute of Standards and Technology (NIST) has also provided cloud computing security information for government agencies. NIST is advising the Federal Risk and Authorization Management Program (FedRAMP) to help develop Federal Information Security Management Act (FISMA) criteria related to cloud computing. Learn more about the FedRAMP efforts, and read general information about NIST cloud computing work.

Virtualization capacities are expanding exponentially, and the necessary technologies to safeguard virtualized infrastructures and data must keep pace. The following Microsoft offerings for government agencies can also help to provide more secure cloud services:

- **Microsoft Business Productivity Online Suite** is a set of online messaging and collaboration solutions hosted by Microsoft. The suite includes Microsoft Exchange Online, Microsoft SharePoint Online, Microsoft Office Live Meeting, and Microsoft Office Communications Online.
- **The Windows Azure platform** is a flexible environment where you can create cloud applications without adding to your infrastructure. The platform includes Windows Azure, Microsoft SQL Azure Database, AppFabric, and Microsoft Codename "Dallas."