Microsoft

# Better security starts at the OS

## with Windows Server 2016

## Increasingly sophisticated attacks require new layers of security

Evolving cyber threats have made it harder than ever for IT to secure their applications and data. Attackers are getting more sophisticated, often using compromised, highly privileged admin credentials to control access. These credentials make it easy for them to remain undetected for long periods of time or create an instant, devastating attack.

Virtualized environments are particularly at risk. Virtual machines don't have the hardware-rooted security capabilities of physical servers. Since virtual machines are instantiated from files that can be copied and modified, any attacker that is able to access the fabric storage, network, or compute resources immediately has unchecked privileges for all virtual machines. An attacker can simply copy your SQL and domain controller VMs into a USB drive and walk out with your crown jewels.

### Protect, detect, and respond

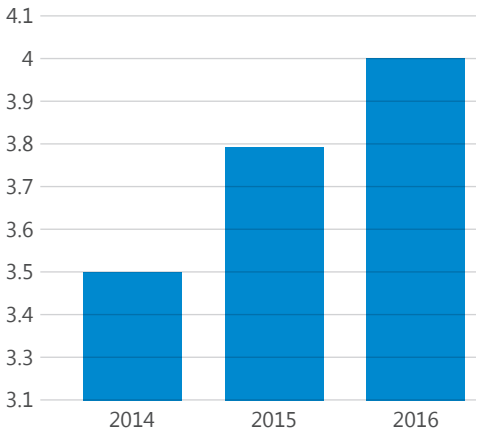
Windows Server 2016 includes built-in breach resistance mechanisms to thwart attacks on your systems and help meet compliance goals. Even if someone finds a way into your environment, the layers of security built into every Windows Server 2016 system limit the damage they can cause. Several credential isolation and threat defense capabilities are activated upon deployment. Other security features can be enabled as needed to help you:

- Block Pass-the-Hash attacks and other attempts to compromise admin credentials.
- Prevent malware and ransomware from being injected into servers.
- Quickly identify behavior that indicates a server breach.
- Extend protection that exists for your physical servers to your virtual machines.

"Shielded Virtual Machines remove a hosting obstacle and are a huge competitive differentiator. No one but Microsoft has this technology now."

– Philip Moss
Chief Product Officer
Acuutech

### Global data breach costs per organization ($M)




The cost of data breaches continues to grow every year and now averages $4M per incident.

Source: Cost of Data Breach Study, IBM, Ponemon

# Better security starts at the OS

Windows Server 2016 provides enterprise-scale security, enabling organizations to comply with the strictest organizational and industry-standards. Infrastructure and applications are protected on-premises and in the cloud, on physical and virtual servers.

"Shielded Virtual Machines simplifies the way we secure VM workloads; in the past, it was complex or impossible. Now, we shield it and we're done."

– Rand Morimoto, President, Convergent Computing

| Enterprises need to: | Example threat: | Windows Server 2016 helps: |
|---|---|---|
| Protect admin credentials | A Pass-the-Hash attack provides an attacker with admin credentials on a hospital network, which the attacker uses to access confidential patient data. | Provide **Just Enough Administration** and **Just-in-Time Administration** to help ensure attackers can't access critical data, even if they have compromised admin credentials. **Credential Guard** helps prevent admin credentials from being stolen by Pass-the-Hash and Pass-the-Ticket attacks. **Remote Credential Guard** delivers Single Sign-On for Remote Desktop Protocol (RDP) sessions, eliminating the need to pass credentials to the RDP host. |
| Protect servers, detect threats and respond in time | Ransomware on university servers locks users away from critical student and research data—until a ransom is paid to the attacker. | Help ensure only permitted binaries are executed with **Device Guard**. Help protect against classes of memory corruption attacks with **Control Flow Guard**. **Windows Defender** also helps protect against known vulnerabilities without impacting server roles (such as Web Servers). |
| | A line-of-business application developer downloads code from the public internet to integrate into her application. The downloaded code includes malware that can track activity in other containers through the shared kernel. | Help protect containerized applications with **Hyper-V isolation** without requiring any changes to the container image. Minimize the attack surface further using **Nano Server**, which is optimized to run inside containers. |
| Quickly identify malicious behavior | Malware tries to access the credential manager on a Windows server to gain access to user credentials. | Optimize security auditing with **Enhanced Logging** for threat detection. This includes providing auditing access to kernel and other sensitive processes—detailed information which helps **Microsoft Operations Management Suite (OMS)**, a security and information event management system, provide intelligence on potential breaches through its **Log Analytics** feature. |
| Virtualize without compromising security | Attacker compromises fabric admin credentials at a bank, giving him access to virtualized Active Directory Domain Controllers and SQL databases where client account information is stored. | Create **Shielded Virtual Machines**—generation 2 VMs that have a virtual TPM, are encrypted using BitLocker, and can only run on approved hosts in the fabric. **Host Guardian Service** requires every host to attest to its security health before Shielded Virtual Machines will boot or migrate. |

Take the next step. Learn more at
www.microsoft.com/en-us/cloud-platform/windows-server-security

Microsoft