Windows Server 2016 Security

Better protection begins at the OS

Microsoft

Contents

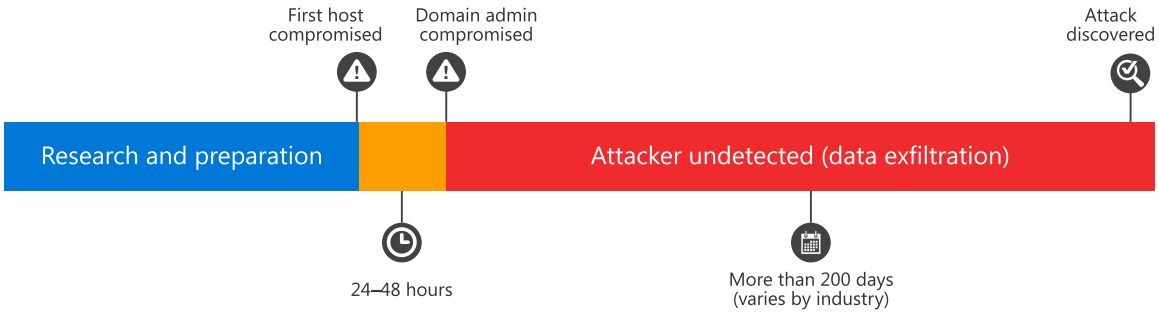
Getting out in front of cyber attacks

In today's business environment, cyber attacks have become a normal occurrence for companies of all sizes, across all industries. The attacker profile has grown beyond independent actors, and now includes organized crime, nation states, and terror groups. These groups not only go after the biggest companies to steal information for the biggest payoff, they are also focused on interrupting businesses for profit or other malicious intent.

Ransomware is another emerging threat used to disrupt business for financial gain. Attackers rely on human error to create swift attacks that hold data hostage. It might start, for example, when an employee clicks on a malicious URL in an email, which downloads malware that quickly traverses the network and encrypts all of the organization's file servers or locks employees out of their systems. The attackers don't even need to worry about staying hidden on the network.

How attacks work

Most attackers use malware toolkits – available to anyone on the internet – to gain access to your network. Once inside, they immediately attempt to compromise administrator credentials, which typically takes them 24 to 48 hours. At that point, with domain administrator credentials in hand, they have free rein to access nearly any system in your infrastructure. Because they are using valid credentials, they can operate for months before being discovered.



In a typical breach, attackers compromise domain admin credentials within 48 hours, giving them nearly unlimited access to internal systems and the ability to operate for months without discovery.

If we know all of this, why are attackers still so successful? The issue is that most organizations rely on a security model that stresses building infrastructure defenses to keep the bad guys out, rather than finding them once they're inside. With ever-growing numbers of mobile devices and remote workers, along with readily available malware toolkits, it's no longer a matter of whether you'll be breached, but when. Adopting an "assume breach" defense allows IT security teams to spend more time and effort on detecting breach activity and creating roadblocks that prevent attackers from making any progress once inside. By making it incredibly difficult to compromise administrator credentials or exploit vulnerabilities, attackers are forced to spend weeks, not just a day or two, to gain broad access to internal resources. They also make a lot of noise during their extended search, giving IT a much better chance of spotting the malicious activity and responding before corporate resources can be compromised.

Windows Server 2016: Active defense and compliance

Windows Server 2016 was designed to defend server infrastructures against the methods attackers use to compromise data and interrupt business: stealing credentials, inserting malware into servers and applications, and targeting virtualization vulnerabilities. New protections at the identity, OS, and virtualization layers work to disrupt standard attacker toolkits and isolate vulnerable targets, making the server OS an active participant in its own defense. The security features in Windows Server 2016 also help slow down attacker progress within the network by protecting administrator credentials and alerting administrators to malicious activity. So even if an attacker gains a foothold in your environment, the attacker can't move any further.

Improved protection of vulnerable infrastructure and credentials through OS security gives organizations a way to get out in front of attackers before they can cause damage. It also supports compliance with government and industry regulations for protecting data, such as HIPAA, SOX, ISO 27001, PCI, and FedRAMP. Using built-in security components, Windows Server 2016 can now directly help address certification requirements for these regulations, such as managing access privileges, protecting data in shared resources, and security auditing. This is not surprising, given that both these regulations and Windows Server 2016 are designed to combat the cyber threats that undermine corporate security.

PCI DSS 3.2	ISO 27001:2013	FedRAMP
6.4.2 – Separation of duties between test and production environments	A.6.1.2 – Segregation of duties	AC-2 – Account management
7.1 – System components and cardholder data access restricted to job-based needs	A.9.1 – Business requirement of access control	AC-2 (4) – Automated audit actions
7.1.1 – Define role access needs	A.9.1.2 – Access to networks and network services	AC-2 (7) Account role-based schemes
7.1.2 – User ID access based on least privileges	A.9.2.2 – User access provisioning	AC-2 (12) – Account monitoring
7.1.3 – Assigning access to job function and classification	A.9.2.3 – Management of privileged access rights	AC-3 – Access enforcement
7.1.4 – Documented approval of access privileges	A.9.4.1 – Information access restriction	AC-5 – Separation of duties
7.2 – User access control on need-to-know basis	A.9.4.5 – Access control to program source code	AC-6 – Least privilege
7.2.2 – Assigning privileges to job function and classification	A.12.1.4 – Separation of development, testing, and operational environments	AC-6 (1) – Authorize access to security functions
7.2.3 – Default "deny-all" setting	A.12.4.1 – Event logging	AC-6 (2) – Non-privileged access for non-security functions
10.2.2 – Logging actions by root privileges individual	A.12.4.3 – Administrator and operator logs	AC-6 (5) – Privileged accounts
10.2.5 – User changes logging		AC-6 (9) – Auditing use of privileged functions
12.5.4 – Administer user accounts		AC-6 (10) – Prohibit non-privileged users from executing privileged functions
12.5.5 – Monitor and control all access to data		AU-2 – Audit events
		AU-9 (4) – Audit access by subset of privileged users
		AU-12 – Audit generation
		CM-5 – Access restrictions for change
		CM-5 (1) – Automated access enforcement
		CM-5 (5) – Limit production / operational privileges

Windows Server 2016 helps organizations meet many government and industry compliance regulations. For example, the Just Enough and Just-in-Time Administration features in Windows Server 2016 fulfill all of the above PCI, ISO, and FedRAMP compliance requirements out of the box. For detailed information on Windows Server 2016 compliance support, see Implementing Microsoft Privileged Identity Management Features for ISO 27001, PCI, and FedRAMP.

Protect credentials and limit administrator privileges

Because attackers typically access sensitive data through compromised administrator credentials, securing administrator identities is key to blocking attacks. In many ways, identity has become the new perimeter when it comes to defending infrastructure and data. If your privileged credentials are secure, then you can keep attackers at bay – even if they are inside your network.

If an attacker does gain access to a system, Windows Server 2016 helps prevent them from using that system as a launching point for further intrusions by copying the credentials from that box. In addition, privileged credentials can be limited in time and scope to help prevent a compromise from turning into a widespread attack.

Credential Guard

Windows Server 2016 includes the same technology used in Windows 10 to protect credentials from being stolen via Pass-the-Hash or Pass-the-Ticket type attacks. A common scenario for these attacks is that a user, who does not realize they have malware on their machine, has an issue with their system and calls the helpdesk for assistance. The first thing the helpdesk admin does – either in person or remotely – is to log into the machine to see what's wrong. The malware then copies those credentials and immediately tries to use them against any system it can find to access system data or steal even higher privileged admin credentials.

Credential Guard uses virtualization-based security to isolate credential information, preventing password hashes or Kerberos tickets from being intercepted. It uses an entirely new isolated Local Security Authority (LSA) process, which is not accessible to the rest of the operating system. All binaries used by the isolated LSA are signed with certificates that are validated before launching them in the protected environment, making Pass-the-Hash type attacks completely ineffective.

Remote Credential Guard

Windows Server 2016 and Windows 10 Anniversary Update also protect credentials for users with remote desktop connections. Previously, anyone using Remote Desktop Services would have to log on to their local machine and then be required to log on again when they performed a remote connection to their target machine. This second login would pass credentials to the target machine, exposing them to Pass-the-Hash or Pass-the-Ticket attacks.

With Remote Credential Guard, Windows Server 2016 implements single sign-on for Remote Desktop sessions, eliminating the requirement to re-enter your username and password. Instead, it leverages the credentials that you've already used to log on to your local machine. Because your credentials do not need to be passed to the target machine, the password hashes or Kerberos tickets can't be copied.

Just Enough and Just-in-Time Administration

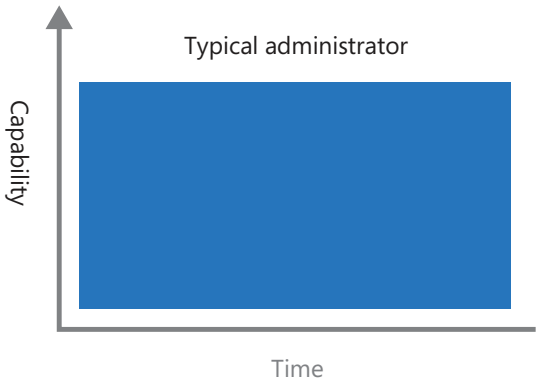
While protecting against Pass-the-Hash or Pass-the-Ticket attacks is important, administrator credentials can still be stolen by other means, including social engineering, disgruntled employees, and brute force. Therefore, in addition to isolating credentials as much as possible, you also want a way to limit the reach of administrator-level privileges in case they are compromised.

Today, too many administrator accounts are over-privileged, even if they have only one area of responsibility. For example, a DNS administrator, who requires a very narrow set of privileges to manage DNS servers, is often granted domain admin-level privileges. In addition, because these credentials are granted for perpetuity, there is no limit on how long they can be used. Every account with unnecessary domain admin-level privileges increases your exposure to attackers seeking to compromise credentials. To minimize the surface

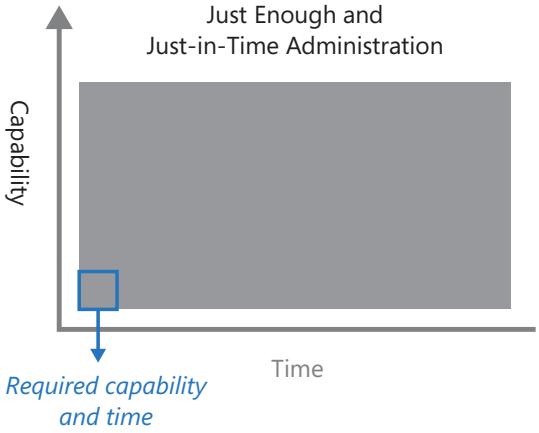
area for attack, you want to provide only the specific set of rights that an admin needs to do the job – and only for the window of time needed to complete it.

Using Just Enough Administration and Just-in-Time Administration, administrators can request the specific privileges they need for the exact window of time required. For a DNS administrator, for example, using PowerShell to enable Just Enough Administration lets you create a limited set of commands that are available for DNS management. If the DNS administrator needs to make an update to one of her servers, she would request access to manage DNS using Microsoft Identity Manager 2016. The request workflow can include an approval process such as two-factor authentication, which could call the administrator's mobile phone to confirm her identity before granting the requested privileges. Once granted, those DNS privileges provide access to the PowerShell role for DNS for a specific time span.

Imagine this scenario if the DNS admin's credentials were stolen. First, since the credentials have no admin privileges attached to them, the attacker wouldn't be able to gain access to the DNS server – or any other systems – to make any changes. If the attacker tried to request privileges for the DNS server, second-factor authentication would ask them to confirm their identity. Since it isn't likely that the attacker has the DNS admin's mobile phone, authentication would fail. This would lock the attacker out of the system, and also alert the IT organization that the credentials might be compromised.



Admin privileges that are too broad and have no time limit create a large window of exposure for attackers searching for credentials.



Just Enough and Just-in-Time Administration reduce the attack surface area for theft of admin credentials.

Note: While Windows Server 2016 makes it much easier to implement credential security, even organizations that have not yet deployed Windows Server 2016 can take steps to protect themselves. Microsoft has put together guidance to help organizations improve security for credentials today – even on previous versions of Windows Server. This step-by-step guidance can be accessed at https://aka.ms/privsec.

Secure OS to run your applications and infrastructure

Preventing cyber threats also requires finding and blocking malware and attacks that seek to gain control by subverting the standard operating practices of your infrastructure. If attackers can get an operating system or application to run in a non-predetermined, non-viable way, they are likely using that system to take malicious actions. Windows Server 2016 provides layers of protection that block external attackers running malicious software or exploiting vulnerabilities. The operating system takes an active role in protecting infrastructure and applications by alerting administrators to activity that indicates a system has been breached.

Device Guard

Windows Server 2016 includes Device Guard to ensure that only trusted software can be run on the server. Using virtualization-based security, it can limit what binaries can run on the system based on the organization's policy. If anything other than the specified binaries tries to run, Windows Server 2016 blocks it and logs the failed attempt so that administrators can see that there has been a potential breach. Device Guard is also integrated with PowerShell so that you can authorize which scripts can run on your system.

In earlier versions of Windows Server, administrators could bypass code integrity enforcement by simply deleting the policy from the code file. With Windows Server 2016, you can configure a policy that is signed by your organization so that only a person with access to the certificate that signed the policy can change the policy. Even if the attacker is using stolen credentials, they can't work around Device Guard unless they have physical access to the machine – a very unlikely scenario. Even if the attacker manages to delete the policy, it would require a reboot to take effect. On reboot, the system would realize that it does not have the specified required policy and would refuse to boot.

Control Flow Guard

Windows Server 2016 also includes built-in protection against some classes of memory corruption attacks. Patching your servers is important, but there is always a chance that malware could be developed for a vulnerability that has not yet been identified. Some of the most common methods for exploiting these vulnerabilities are to provide unusual or extreme data to a running program. For example, an attacker can exploit a buffer overflow vulnerability by providing more input to a program than expected and overrun the area reserved by the program to hold a response. This can corrupt adjacent memory that might hold a function pointer. When the program calls through this function, it can then jump to an unintended location specified by the attacker. These type of attacks are also known as jump-oriented programming (JOP) attacks.

Control Flow Guard prevents JOP attacks by placing tight restrictions on what application code can be executed – especially indirect call instructions. It adds lightweight security checks to identify the set of functions in the application that are valid targets for indirect calls. When an application runs, it verifies that these indirect call targets are valid. If the Control Flow Guard check fails at runtime, Windows Server 2016 immediately terminates the program, breaking any exploit that attempts to indirectly call an invalid address.

Control Flow Guard provides an important additional layer of protection to Device Guard. If a white-listed application has been compromised, it would be able to run unchecked by Device Guard, because the Device Guard screening would see that the application has been signed and is considered trusted. But because Control Flow Guard can identify whether the application is executing in a non-predetermined, non-viable order, the attack would fail, preventing the compromised application from running. Together, these protections make it very difficult for attackers to inject malware into software running on Windows Server 2016.

Windows Defender

Windows Server 2016 includes the industry-leading, active detection capabilities of Windows Defender to block known malware. Windows Defender works hand-in-hand with Device Guard and Control Flow Guard to prevent malicious code of any kind from being installed on your servers. It is turned on by default – the administrator does not need to take any action for it to start working. Windows Defender is also optimized to support the various server roles in Windows Server 2016.

In the past, attackers used shells such as PowerShell to launch malicious binary code. In Windows Server 2016, PowerShell is now integrated with Windows Defender to scan for malware before launching the code.

Enhanced security auditing

Windows Server 2016 actively alerts administrators to potential breach attempts with enhanced security auditing that provides more detailed information, which can be used for faster attack detection and forensic analysis. It logs events from Control Flow Guard, Device Guard, and other security features in one location, making it easier for administrators to determine what systems may be at risk. New event categories include:

- **Audit Group Membership:** Allows you to audit the group membership information in a user's login token. Events are generated when group memberships are enumerated or queried on the PC where the login session was created.
- **Audit PnP Activity:** Allows you to audit when plug and play detects an external device – which could contain malware. PnP events can be used to track down changes in system hardware. A list of hardware vendor IDs are included in the event.

Windows Server 2016 integrates easily with security incident event management (SIEM) systems, such as Microsoft Operations Management Suite (OMS), which can incorporate the information into intelligence reports on potential breaches. The depth of information provided by the enhanced auditing enables security teams to identify and respond to potential breaches more quickly and effectively.

Secure virtualization

Enterprises today virtualize everything they can, from SQL Server to SharePoint to Active Directory Domain Controllers. Virtual machines (VMs) simply make it easier to deploy, manage, service, and automate your infrastructure. But when it comes to security, compromised virtualization fabrics have become a new attack vector that is hard to defend against – until now.

Windows Server 2016 fundamentally changes how enterprises can secure virtualization. It includes multiple technologies that allow organizations to create virtual machines that will run only on their own fabric, which are completely isolated from the hosts they run on, and will interact only with the VMs or other systems on your network that you define as safe.

Shielded Virtual Machines

The same things that make virtual machines so easy to migrate, backup, and replicate, also make them easier to modify and copy. A virtual machine is just a file, so it is not protected on the network, in storage, in backups, or elsewhere. Another issue is that fabric administrators – whether they are a storage administrator or a network administrator – have access to all the virtual machines.

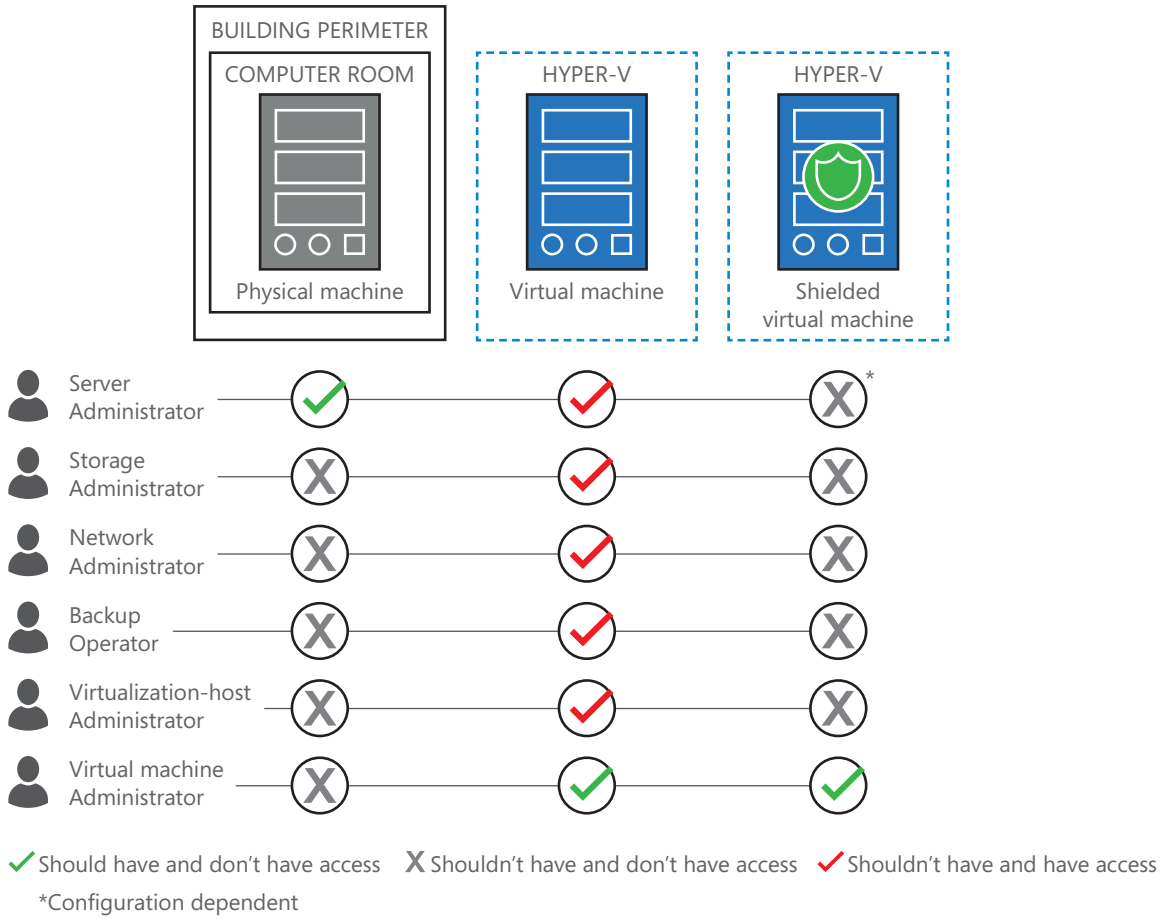
A compromised administrator on the fabric can easily result in compromised data across virtual machines. All the attacker has to do is use the compromised credentials to copy whatever VM files they like onto a USB drive and walk it out of the organization, where those VM files can be run

on any other system. If any one of those stolen VMs were an Active Directory domain controller, for example, the attacker could easily view the content and use readily available brute force techniques to crack the passwords in the Active Directory database, ultimately giving them access to everything else within your infrastructure.

Windows Server 2016 introduces Shielded Virtual Machines to help protect against scenarios like the one just described. Shielded Virtual Machines include a virtual TPM device, which enables organizations to apply BitLocker to the virtual machines and ensure they run only on trusted hosts to help protect against compromised storage, network, and host administrators.

Shielded Virtual Machines are created using Generation 2 VMs, which support Unified Extensible Firmware Interface (UEFI) firmware and have virtual TPM. Once encrypted using BitLocker, the VM will run only on approved hosts in the virtualization fabric. This means that even if an attacker compromises the host, as in the case of a malicious administrator, the attacker wouldn't be able to access the data in any individual VM. This protection – combined with the Host Guardian Service – brings VMs a level of protection never before available. Only the designated VM administrator has access to a Shielded Virtual Machine, preventing access by hackers with administrator credentials.

Note: You can shield Generation 2 virtual machines, including Windows Server 2012 R2, Windows Server 2012, and Windows 8 – Windows 10.



Shielded VMs reduce attack surface area by limiting access to designated VM administrators.

Host Guardian Service

Alongside Shielded VMs, the Host Guardian Service is an essential component for creating a secure virtualization fabric. Its job is to attest to the health of a Hyper-V host before it will allow a Shielded Virtual Machine to boot or to migrate to that host. It holds the keys for Shielded Virtual Machines and will not release them until the security health is assured.

There are two ways that you can require Hyper-V hosts to attest to the Host Guardian Service. The first, and most secure, is hardware-trusted attestation. This solution requires that your Shielded Virtual Machines are running on hosts that have TPM 2.0 chips and UEFI 2.3.1. This hardware is required to provide the measured boot and OS kernel integrity information required by the Host Guardian Service to ensure the Hyper-V host has not been tampered with. IT organizations have the alternative of using Admin-trusted attestation, which may be desirable if TPM 2.0 hardware is not in use in your organization. This attestation model is easy to deploy. Hosts are simply placed into a security group and the Host Guardian Service is configured to allow Shielded Virtual Machines to run on hosts that are members of the security group. With this method, there is no complex measurement to ensure that the host machine hasn't been tampered with. However, you do eliminate the possibility of unencrypted VMs walking out the door on USB drives, because the VM files would not run on any machine other than those in the designated group. If you do not yet have TPM 2.0 hardware, you can start with Admin-trusted attestation and switch to hardware-trusted attestation when your hardware is upgraded.

Host Guardian Service holds the keys for Shielded Virtual Machines and will not release them until security health is assured.

Distributed network firewall using software-defined networking

One way to improve protection in highly virtualized environments is to segment the network in a way that allows VMs to talk only to the specific systems required to function. For example, if your application doesn't need to connect with the Internet, you can partition it off, eliminating those systems as targets from external attackers.

The software-defined networking (SDN) in Windows Server 2016 includes a distributed network firewall that allows you to dynamically create the security policies that can protect your applications from attacks coming from inside or outside a network. This distributed network firewall adds layers to your security by enabling you to isolate your applications in the network. Policies can be applied anywhere across your virtual network infrastructure, isolating VM-to-VM traffic, VM-to-host traffic, or VM-to-Internet traffic where necessary – either for individual systems that may have been compromised or programmatically across multiple subnets.

Windows Server 2016 software-defined networking capabilities also enable you to route or mirror incoming traffic to non-Microsoft virtual appliances. For example, you could choose to send all of your email traffic through a Barracuda virtual appliance for additional spam filtering protection. This allows you to easily layer in additional security both on-premises or in the cloud.

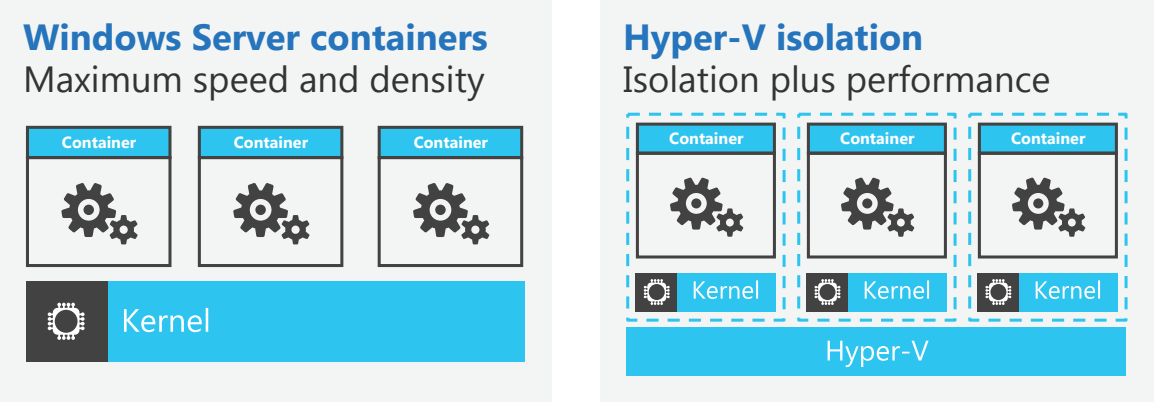
Security for developers

In addition to protecting your infrastructure, Windows Server 2016 also helps developers incorporate security into their application development process in ways that were not previously possible. There are many technologies that developers use today to ensure that they can deliver applications faster, cheaper, and more effectively. Windows Server 2016 helps add a layer of security to Windows Server and Linux containers that enables IT administrators and developers to ensure proper isolation and provide identities for applications.

Hyper-V isolation for containers

Containers are great for streamlining development and increasing application efficiency. Unlike VMs, however, typical containers are not fully isolated. Instead, container technology shares the host kernel among all running containers. This may result in one container impacting another container or the host itself.

Hyper-V isolation helps ensure Windows Server or Linux can't affect the host or other containers running on that host by isolating each container in a highly optimized virtual machine. This way, each container has its own instance of the kernel that is not shared with the host. As a result, you can run as many containers as you want without affecting the host or other containers on the same system.



Hyper-V encapsulates the container and OS kernel, preventing the container from affecting the host or other containers, and vice versa. Hyper-V isolation enables the same isolation and management experience for Windows Server containers and Linux containers, side by side on the same host.

Windows Server 2016 is the first and only operating system to offer this security boundary between containers and hosts, enabling customers to ensure the security of their application development and production infrastructure – especially those in industries with strict regulatory and compliance requirements. Using Hyper-V isolation doesn't change the development model at all. Create containers exactly the same way as Windows Server containers, using the same write once, deploy anywhere model. The only difference is that at run time, you add the appropriate isolation to achieve your IT security goals. More great news for developers is that Hyper-V isolation enables you to run Linux containers natively on a Windows host.

Windows Server also enables developers and IT administrators to provide Active Directory identity to Windows Server containers so that containers can fully participate in access to network resources without needing to store credentials or secrets within the container itself.

Nano Server

For additional security, IT organizations and developers can benefit from using Nano Server as the container image. Nano Server is optimized for container-based development, offering high performance and a reduced attack surface. Nano Server functions beautifully for modern distributed and cloud-based apps, including those that leverage containers and microservices architectures. In this way, developers are building security into their applications from the ground up.

Conclusion

The server operating system sits at a strategic layer in an organization's infrastructure, affording new opportunities to create layers of protection from attacks that could steal data and interrupt your business. Working to help protect the identity, OS, and virtualization layers, Windows Server 2016 helps block the common attack vectors used to gain illicit access to your systems: stolen credentials, malware, and a compromised virtualization fabric. In addition to reducing business risk, the security components built into Windows Server 2016 help address compliance requirements for key government and industry security regulations.

These identity, OS, and virtualization protections enable you to better protect your datacenter running Windows Server as a VM in any cloud, and limit the ability of attackers to compromise credentials, launch malware, and remain undetected in your network. Likewise, when deployed as a Hyper-V host, Windows Server 2016 offers security assurance for your virtualization environments through Shielded Virtual Machines and distributed firewall capabilities.

With Windows Server 2016, the server OS becomes an active participant in its own defense.

Take the next step.

Learn more at www.microsoft.com/windowsserver2016

Microsoft