TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

May 2017

This monthly publication provided courtesy of Richard Lynn, VP Sales & Marketing, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

WannaCry: The implications of the largest ever ransomware Attack

Well, here we are as all members InfoSec community warned. The perfect storm of conditions has led to the largest ransomware attack in history. Over the weekend, according to The Hacker News, 99 countries and 200,000+ machines came under attack from WannaCry (as well as offshoots of it like WanaCrypt0r 2.0). This ransomware is based on the code in the leaked NSA malware.

WannaCry utilizes the DoublePulsar malware to download the EternalBlue exploit (patched a month ago) which enters a system via an exploit in the SMB port 445. Upon infection, WannaCry acts as a worm virus as it quickly tunnels into the machine and subsequently infects any other vulnerable devices in the network. Upon the locking of the machine, the hackers (possibly based in Russia but proxy servers make it difficult to pinpoint definitive locations) demanded, according to Threatpost, roughly $600 worth of Bitcoin ransom to unlock the machine.

As this was the largest ransomware incident to date, the media went insane and proceeded to report with frantic updates. Cybersecurity firms did their best to help the infected and Microsoft released an emergency patch for Windows XP and Windows 8 (the most affected OS), as well as Server 2003 and 2008, that somewhat stopped the bleeding.
Per the patch report, Microsoft states:

"Seeing businesses and individuals affected by cyberattacks, such as the ones reported today, was painful. Microsoft worked throughout the day to ensure we understood the attack and were taking all possible actions to protect our customers… we are taking the highly unusual step of providing a security update for all customers to protect Windows platforms that are in custom support only"

The major points to take away from the incident are frustrating ones, as they were all a result of preventable issues.

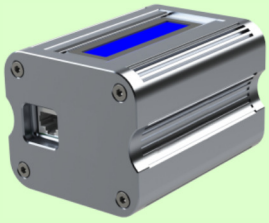
The NHS, for example, was hit hard as they were still running an archaic operating system (Windows XP) that was not patched. The U.K. government chose to ignore countless reports of the dangers of this, reports such as my own, and instead left patients in their system's care at risk due to admins being locked out of vital patient data.

Tying into this, the vast amount of systems that still ran archaic Microsoft systems were a testament to how ill-informed businesses and the general public are with regards to updates. The amount of attack vectors that can be leveraged by hackers in an old OS like XP is beyond description. An obsolete OS, no matter what part of the globe or what industry it is deployed in, is bound to come under attack with ease. An unpatched old OS is a hacker's playground, it is what black hats live for and what white hats dread.

This was no ordinary ransomware attack, however, as this was ransomware developed with malicious code found in leaked NSA malware. The NSA, in addition to previously hoarding exploits (much like the CIA) instead of telling companies about them, decided to create powerful malware that allowed them access to any system around the world. The NSA's recklessness is, without a doubt, the most defiant display of arrogance. To think that they are above the laws of cybersecurity, and as such, able to endanger the entire world to nation-state and criminal threats alike is reprehensible.

Also reprehensible is other government agencies like the U.K.'s GCHQ who sought exploits from their American allies. Really the world governments, through allowing dangerous malware development, as well as not protecting their vital systems via OS updates and public education on InfoSec, should bear the brunt of this blame.

Latest Network Security Device: "NetDefender"



Vulnerability Management Solution

The new NetDefender Vulnerability Management Solution enhances security by proactively identifying, monitoring, and notifying businesses of potential vulnerabilities in their networks—all with breakthrough simplicity and affordability.

Utilizing proprietary software and the compact NetDefender Sensor, NetDefender works in three phases:

1. Identification

The user's network is continuously scanned to locate and identify every connected device with an IP address, from computers and smartphones to printers and smart devices

Includes scanning of external-facing IPs to provide a 360-degree view of network vulnerabilities

2. Monitoring

All connected devices are then scanned 24x7 for vulnerabilities such as missing software patches

3. Notification

All scan information, including vulnerabilities, is displayed in an easy-to-read dashboard, including instructions for remediation

A proprietary "SPF" (Security Protection Factor) scoring system makes it easy to understand the network's health

Users and their IT security providers can be alerted to critical issues via email or text

For more information on this solution please contact your Tech Hero representative at (800) 900-8234 (option 2)

If it were not for them, opportunistic ransomware developers would not have been able to spread powerful malicious code on the Dark Web. Black hats looking to turn a quick profit, no matter if actual lives were endangered (as was the case with the NHS infection), went on to obtain and create WannaCry (which has now been updated in response to the most recent patches).

Since these attacks have garnered so much attention from the media, more than any ransomware attack in the past, it is more important than ever that the InfoSec community makes its voice heard. We have to make sure, more than ever, that we get the news out about patches, vulnerabilities, and other security issues so that it isn't just the IT world that knows about it. WannaCry can be a wake-up call to the global community that they have not taken cybersecurity as seriously as they should have. We must make it our mission more than ever before, especially since The Hacker News reports "even after WannaCry made headlines all over the Internet and media, there are still hundreds of thousands of unpatched systems easily available open to the Internet."

Client Spotlight

Epilepsy Association of Central Florida

The Epilepsy Association of Central Florida is dedicated to improving the quality of life for children and adults with epilepsy and seizure disorders throughout Central Florida. Not only does EACF provide services for those with epilepsy and seizure disorders, but we also offer many programs and opportunities for your office/community/group to learn more about epilepsy.

To donate to this amazing organization please visit:
https://www.firstgiving.com/floridaepilepsy

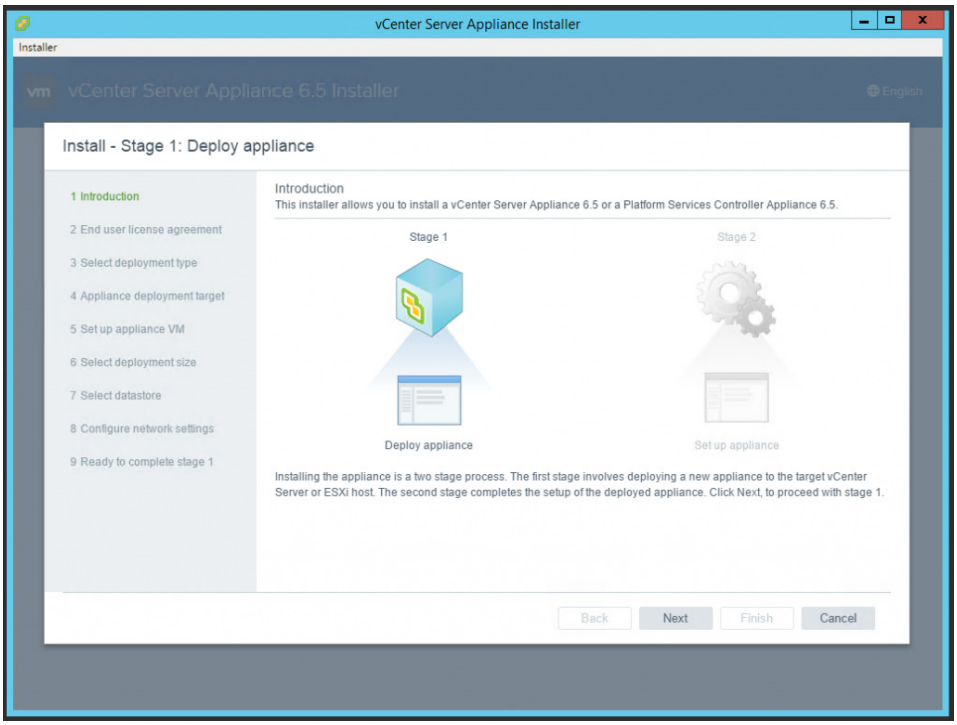
Would you like your company highlighted here in our "Client Spotlight"? Then give us a call today at: 1-800-900-8324 x8840.

10 things you need to know about VMware vSphere 6.5

vSphere was launched by VMware in an effort to consolidate physical server groups into virtualized ones. In an increasingly virtualized IT marketplace, companies required better virtual infrastructure and vSphere was meant to provide this.

However, this appliance has evolved far beyond the scope of computing virtualization, and can now add virtualized storage, perform endpoint computing, and networking tasks. No wonder vSphere is VMware's flagship product for everything virtual. The latest vSphere 6.5 brings plenty of new features to the table. Read on to see the best ones.

1. vCenter Server appliance



vCenter is the primary backend tool in charge of managing the virtual infrastructure of VMware. Apart from its ability to build and manipulate virtual components, such as virtual machines (VMs), storage, and networking, from a centralized location, vCenter 6.5 boasts many salient upgraded features. No wonder it's so vital to the user's system. It is like how vital Larry Bird was to the 1981 Boston Celtics when they won the championship or how critical Sam Witwicky was to the human race in Transformers 1, 2, and 3!

The most significant features in vCenter 6.5 include:

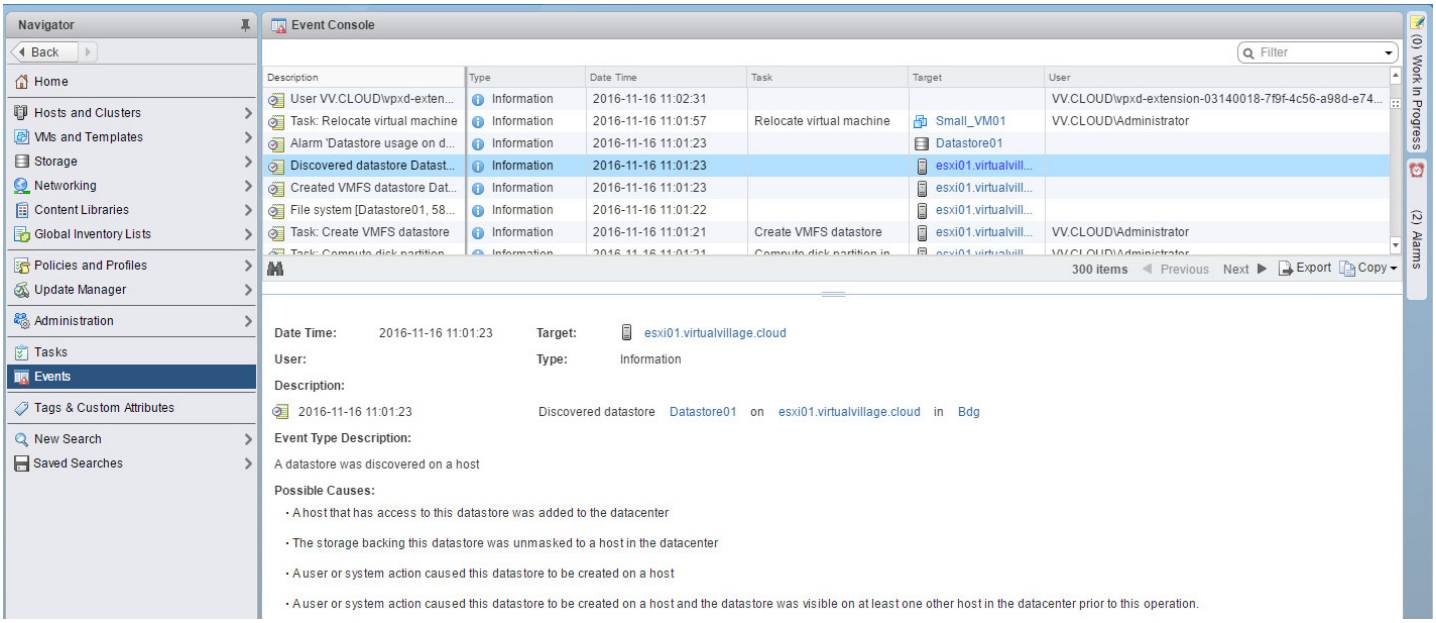
- A migration tool to help with the shift from vSphere 5.5/6.0 to vSphere 6.5.
- The vCenter Server appliance now includes the VUM (VMware Update Manager). This does away with the need for pesky plugins and restarting external VUM tasks.
- VMware has always been attentive to customer feedback, and the vSphere web client has received various cosmetic alterations based on users' suggestions. For instance, the home screen is a lot more organized, tabs have been removed or renamed, and default views are now present.
- High-availability features of the new vCenter 6.5 make use of cloned vCenter instances for maximizing uptime of the appliance as well as its services. Virtualization admins will find this feature to be just what they wanted as a lone vCenter instance was always a vulnerable point.

2. Backup and restore

Technically, the backup and restore capabilities are part of the vCenter Server 6.5 appliance. However, it deserves special mention due to its powerful performance. This excellent out-of-the-box functionality allows clients to back up any Platform Services Controller appliances or vCenter Server directly from the API (Application Programming Interface) or VAMI (Virtual Appliance Management Interface).
Moreover, it is capable of backing up both Auto Deploy running and VUM embedded within the appliance. This backup will consist of files that are going to be streamed to a storage device of the client's choice, through HTTP(s), FTP(s), or SCP protocols.

This backup will also fully support vCenter Server appliances featuring external and embedded Platform Services Controllers. Restore workflow option can now be launched from the same ISO used to originally upgrade or deploy the PSC or vCenter Server Appliance.

3. Secure boot

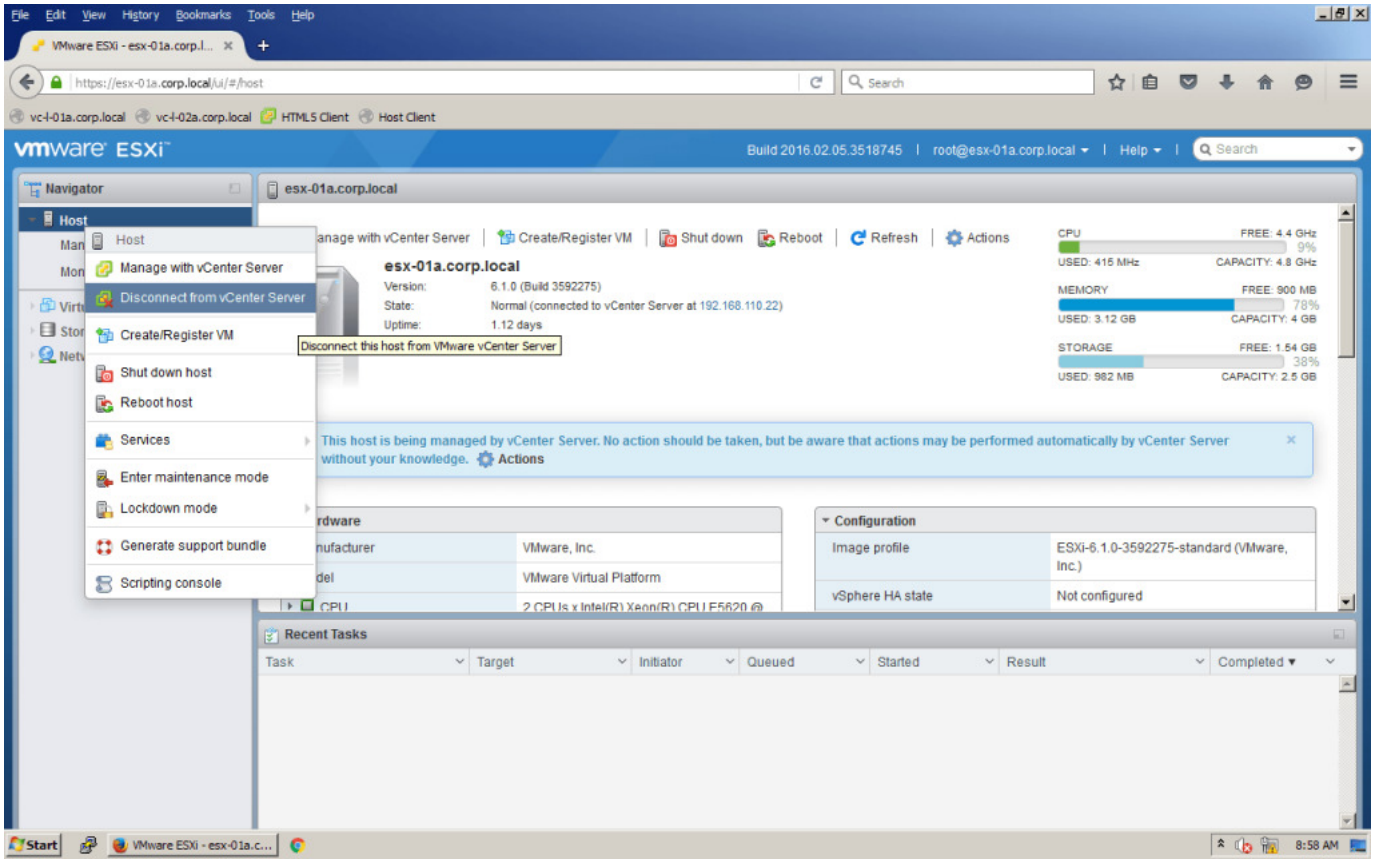


The secure boot feature of vSphere encompasses the EFI-enabled virtual machines. This is available in both Windows and Linux VMs, allowing secure boot to be completed via the clicking of a simple checkbox that is located in the VM properties. Once enabled, only the VMs that are properly signed can use the virtual environment to boot.

4. vSphere client

Before, the front-end client used for accessing vCenter Server was quite clunky and outdated. However, in vSphere 6.5, it's received a much-needed HTML5 makeover. Apart from the inevitable upgrades in performance, the change makes the tool a lot more mobile-friendly and cross-browser compatible. The UI has been swapped for a more modern aesthetic based on the Clarity UI from VMware. The best part is that plugins are no longer required.

5. ESXi



To offer a cryptographically clean booting process to the virtual and physical server, VMware has added secure boot to its toolkit. Any server using the UEFI (Unified Extensible Firmware Interface) secure boot must have the ESXi components digitally signing-in to the firmware for booting the operating system (OS) of the host system.

If any vSphere Installation Bundle (VIB) is signed incorrectly, not only will the boot process halt but the server will flash a "purple screen of death." This is meant to avoid tampered threats that come from booting up alongside the host system.

6. Advanced automation capabilities

When it comes to automation, vSphere 6.5 works wonders by virtue of its new upgrades (it is like eating the perfect Whopper from Burger King!). The addition of a new PowerCLI tweak has been a thoughtful move on the part of VMware, as it's entirely module-based and APIs are currently in high demand. This enables the admins to completely automate down to the virtual machine level (you know, where us little people live!).

THECHANNELCO.
CRN
MSP 500
2017

Tech Hero

has made the Pioneer 250 list of CRN's 2017 Managed Service Provider 500 List!

The 2017 MSP 500 list recognizes companies in North America whose approach to delivering managed services is one innovative step ahead.

The MSP Pioneer 250 is a list of channel companies with business models weighted toward managed services and largely focused on SMB market.

7. Harbor and Admiral

vSphere 6.5 has added two essential components to the vSphere Integrated Containers service. For starters, it's provided an interface compatible with Docker for developers. Apart from the VIC (Vsphere Integrated Container) engine, VMware has officially added a container registry, known as Harbor, and a container management portal, named Admiral (wow, someone likes the Navy; do not worry, Army folks, you are respected too!).

- **Harbor:** An enterprise registry meant for the storage and distribution of containers, Harbor is developed off the fork used for creating Docker Hub. Several new features have been added by VMware to assure Harbor is enterprise worthy, such as image replication, role-based access control, auditing, and more.

- **Admiral:** This offers an isolated portal to admins and developers for managing containers running on vSphere. Independent of regular vSphere user interfaces, Admiral comes with features like live status updates, rule-based resource management, and management of container templates for deployment of containerized apps.

8. vMotion encryption

vMotion encryption has been added to vSphere 6.5. This does not need any sort of network-level encryption. Rather, designated virtual machines achieve a randomly generated vCenter certificate, which is then packaged and forwarded to the hosts for the transfer of the virtual machine. This protects any data-in-motion.

9. VM encryption

VM encryption in vSphere 6.5 secures at the hypervisor level. The majority of the work gets done using the kernel (get those thoughts of corn on the cob out of your head now!), and this means the virtual machine doesn't need to run its encryption processes. Admins are also allowed to set policies that function across different VMs, as opposed to case-by-case instances. vSphere 6.5 also addresses new encryption standards used in modern processors, such as AMD and Intel.

10. Improved auditing

The vSphere 6.5 provides clients with improved audit-quality logging features. This helps access more forensic details regarding user actions. IT is now better able to understand what was done when, by whom, and whether any investigation is necessary into security threats and anomalies.

Now that you are aware of these 10 VMware vSphere 6.5 features, you can unleash its full usage and potential. Get ready to ride the wave to virtual bliss!