Pulse Secure®

Preventing WannaCrypt Type of Cyberattacks with Host Checker

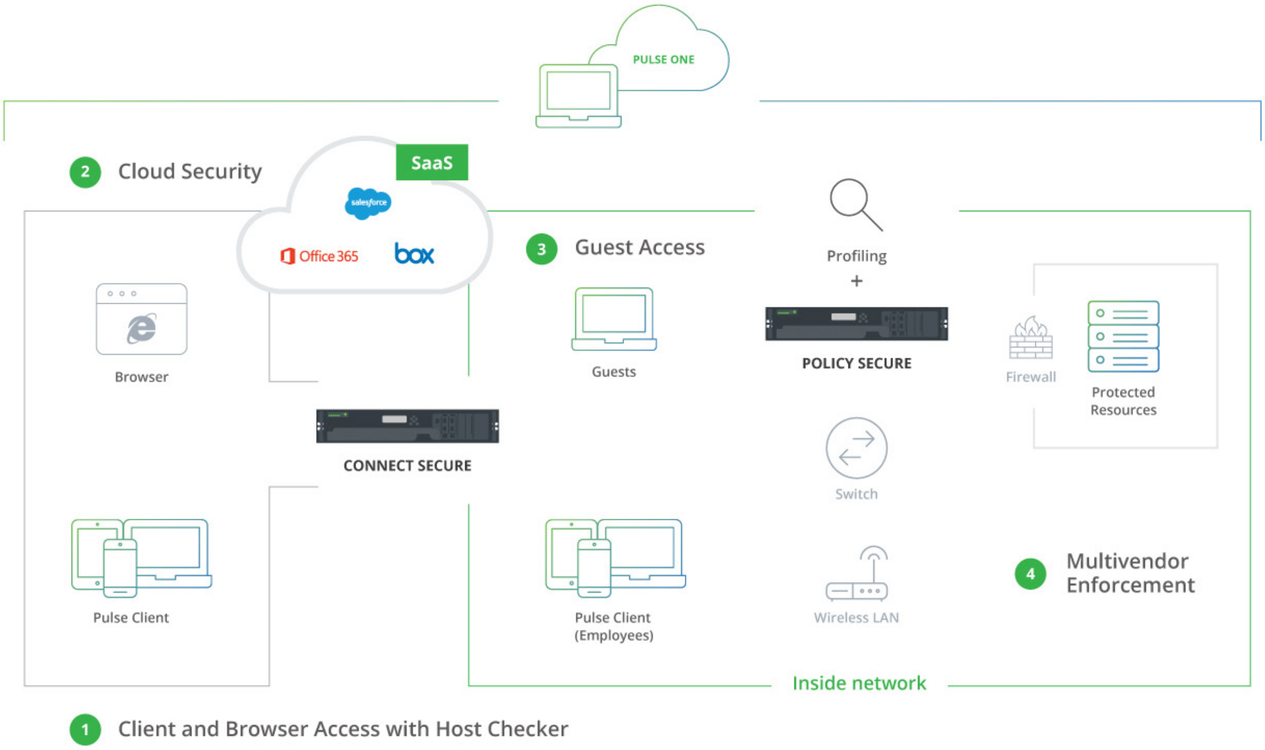
A Rude Surprise

We have grown accustomed to computer viruses but the latest WannaCrypt worm attack was a Friday surprise that took the world by storm. It claimed more than 200,000 victims in less than 48 hours, according to one count by Europol, Europe's policing agency. The Associated Press also reported that the ransomware spread to 150 countries, and victims included Chinese gas stations, Japanese broadcasters, British hospitals, and German railways. WannaCrypt is particularly malicious because it takes just one person to click on an infected link or email attachment to spread the virus. Once infected, the host machine scans the organization's intranet and the internet for other vulnerable machines leading to rapid spread of the virus in a vastly interconnected world.

Can organizations protect themselves from this type of cyber-attacks? The answer is yes, and we will explain how the Pulse Secure Host Checker function provides a proactive defense.

Secure Access by Pulse Secure

Pulse Secure provides Secure Access solutions for people, devices, things and services. Our solutions are proven with over 15 years of R&D investment, 20,000 customer deployments and 20 million connected endpoints. Foundational to our Secure Access solutions for both the cloud and data center is the Host Checker function. This robust compliance enforcement tool ensures that only secured devices are given access to the corporate network, applications and services.



Enterprises rely on Pulse Secure, with capabilities such as Host Checker, to protect their data center. Now we've extended those capabilities to protect mobile access, enable secure cloud use, and secure IoT devices on internal networks. We've also bundled all of these product capabilities in the Pulse Access Suite. As shown above, (1) this solution suite provides client and browser access, with Host Checker function, which gives users seamless access to enterprise resources inside and outside of the network. Pulse Connect Secure manages and secures remote and mobile access of data center and cloud resources while Pulse Policy Secure oversees local connectivity to the corporate network. (2) Cloud access is afforded the same security as the data center. (3) Policy Secure also provides Guest Access capabilities that are easy to setup by IT and self-provision by guest users. (4) Finally integration between Policy Secure and third-party vendors such as Palo Alto, Ruckus, HP and Juniper enable a highly secure internal network. While Pulse Profiler is used to discover unknown network devices, Policy Secure is used to enforce security on those devices by providing granular contextual user and device information to third-party enforcement points. All of this is controlled from the Pulse One centralized management console.

How to Prevent Cyberattacks like WannaCrypt?

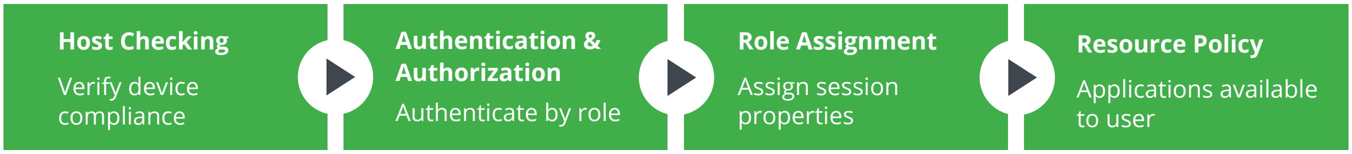
Cyber-attacks are often motivated by economic gains or industrial espionage. Just like most break-ins happen to homes or cars that are unlocked, many cyber-attacks happen to enterprises simply because they did not have proper protection in place. That's the case with the latest ransomware attack.

The WannaCrypt ransomware exploits a known Microsoft Windows vulnerability (MS17-010) contained within their implementation of the Server Message Block (SMB) protocol. Microsoft released a "Critical" advisory and security patch two months prior to the May 12th attack. IT organizations that updated user devices with the provided patch were not victim to the attack.

The Host Checker function of the Pulse Access Suite is an important tool for IT to enforce security compliance. When a user attempts to connect to the corporate network remotely or via the local WiFi access point, the Host Checker function automatically verifies the user's device for compliance with antivirus, firewall, anti-spyware, OS version and patch management policies. If the policy check fails, the device is blocked from accessing the network.

Now how can Host Checker help administrators prevent or contain the WannaCrypt attack? When Microsoft published the security update for the MS-170 exploit in March, Host Checker automatically prevented users without the patch from logging into the network and prompted them to install the latest patch. In addition, administrators had the option to block or restrict access for devices using outdated/unsupported versions of Windows such XP or Vista.

The Host Checker function is an essential part of how the Pulse Access Suite helps IT manage user access to information based on user identity, user role, desired resource and device compliance. Policies can be enforced at user login, and access can be subsequently further controlled based on device compliance status and the user's role. Verifying device compliance is a key first step in securing enterprise access and provides a proactive way to counter malware threats using a variety of device checks while also continuously monitoring device system health.



Host Checking
Verify device compliance

Authentication & Authorization
Authenticate by role

Role Assignment
Assign session properties

Resource Policy
Applications available to user

Host Checker works with both client and browser based access using sophisticated checks that contain one or more rules. Checks are provided for different device platforms including Windows, Mac, Linux, Solaris, iOS, and Android. Predefined policies include policy checks for antivirus, firewall, anti-spyware, hard disk encryption and patch level. Custom policies can also be created that verify port use, process execution, file presence, registry settings, NetBIOS name, MAC address, and machine certificates. Based on your company's desired security posture, Host Checker can be configured for periodic and continuous policy evaluation.

What to do for non-compliant devices? Host Checker provides remediation when an endpoint does not meet policy requirements. For example, a remediation page can be displayed to the user that contains specific instructions and links to resources to help the user bring their endpoint into compliance with your security policy. The user can also be sent a message that includes a reason string returned by Host Checker that explains why the device is not compliant. For example, the user might see a remediation page that contains custom instructions, a link to resources, and reason strings with further details. Host Checker can also be configured to automatically remediate the user's computer. In this case, when the initial policy fails, actions can be taken to kill processes, delete files, or allow automatic remediation by an antivirus rule, a firewall rule, or a registry setting rule.

The Pulse Access Suite provides the administrator a single pane-of-glass to manage access for local, remote and mobile users. Compliance visibility is provided for BYOD, mobility and IOT devices running Windows, Android, iOS and Linux OS. Centralized visibility and management simplifies the enforcement of consistent security policies across multiple network segments, providing a robust defense against intruders from the outside and rogue users from the inside.

Conclusion

Cyberattacks are a common occurrence and only the most spectacular become headline news. WannaCrypt and other malware attacks are preventable and it costs far less to proactively deter an attack verses a messy cleanup after the attack. Raise your security posture with these three easy steps:

1. Ensure all corporate and BYOD devices are fully patched
2. Use Pulse Connect Secure and Pulse Policy Secure Host Checker to test and enforce compliance with security policies
3. Train users not to trust all email they receive

Click here to learn more about Host Checker. Read this article if you want more details on how to mitigate WannaCrypta with Host Checker.