

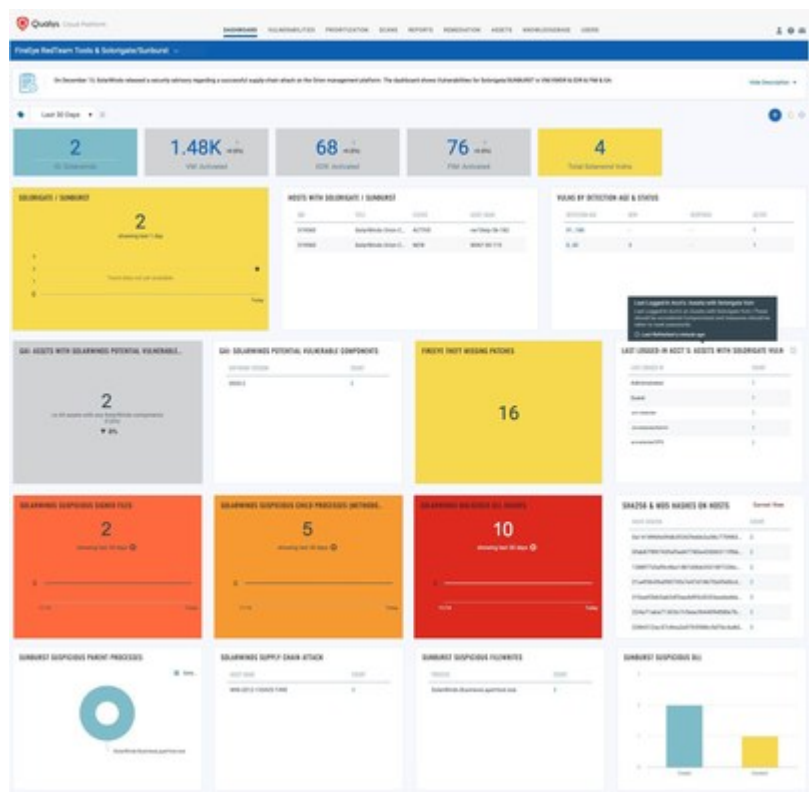


## Qualys Researchers Identify 7+ Million Vulnerabilities Associated with SolarWinds/FireEye Breach by Analyzing Anonymized Vulnerabilities across Worldwide Customer Base

December 22, 2020

*Qualys offers free 60-day integrated Vulnerability Management, Detection and Response service to help organizations quickly assess devices impacted by SolarWinds Orion vulnerabilities, SUNBURST Trojan detections, and FireEye Red Team tools, and to remediate and track results via dynamic dashboards*

FOSTER CITY, Calif., Dec. 22, 2020 /PRNewswire/ -- [Qualys, Inc.](https://www.qualys.com) (NASDAQ: QLYS), a pioneer and leading provider of cloud-based security and compliance solutions, today announced its research team, using the Qualys Cloud Platform, has identified 7.54 million vulnerabilities related to FireEye Red Team assessment tools and compromised versions of SolarWinds Orion, tracked as Solorigate or SUNBURST, across its 15,700-member customer base.



Of the vulnerabilities identified, researchers noted that across 5.29 million unique assets most are related to the FireEye Red Team tools. These findings highlight the scope of the potential attack surface if these tools are misused. The research team further identified that 99.84% of the 7+ million vulnerability instances are from eight vulnerabilities in Microsoft software that have patches available.

To help mitigate risk and exposure from this breach, Qualys is providing IT and security teams free 60-day access to its integrated Vulnerability Management, Detection and Response service, which leverages the power of the Qualys Cloud Platform.

More information can be found on the Qualys advisory blog at [qualys.com/solarwinds-fireeye-advisory-blog-post](https://www.qualys.com/solarwinds-fireeye-advisory-blog-post).

"The Qualys free solution provides much-needed visibility and response in a single app that many need at a time when IT and security organizations around the world are scrambling to shore up their systems," said Frank Dickson, program vice president, Security and Trust at IDC. "Qualys' solution draws from its native security and compliance platform to deliver vulnerability management, detection and response, the ability to detect malware, and the integrity of files. It is great solution, easy to use and deploy, and it's hard to beat as it is free."

"The scope of this nation-state attack is massive, as overnight a widely used and trusted piece of software turned into known malware," said Smedh Thakar, president and chief product officer at Qualys. "Since its discovery, Qualys teams have been actively researching the issue and helping customers assess their environments. The good news is that nearly all of the CVE's are patchable, and we've made this solution available to the industry so they can immediately work to protect themselves from being exploited by these vulnerabilities."

Qualys is offering a fully functional license free for 60 days. The license enables full situational awareness, detection, and remediation to reduce risk and exposure from the SolarWinds and FireEye breaches. It includes:

- Real-time, up-to-date inventory and automated organization of all assets, applications, and services running across the hybrid-IT environment
- Continuous view of all critical vulnerabilities and their prioritization based on real-time threat indicators and attack surface
- Automatic correlation of applicable patches for identified vulnerabilities
- Patch deployment via Qualys Cloud Agents with zero impact to VPN bandwidth
- Security configuration hygiene assessment to apply as compensating controls to reduce vulnerability risk
- Unified dashboards that consolidate all insights for management visualization via a single pane of glass

"As our teams assessed the very sophisticated SolarWinds / FireEye nation-state attack, we realized that we could help the industry through our very powerful unified Cloud Platform. The integrated security solution provides real-time visibility across the entire global and hybrid IT environment allowing it to detect and prioritize critical vulnerabilities, identify malware and effectively respond all from one single pane of glass," said Philippe Courtot, chairman and CEO of Qualys.

To sign up for the free 60-day service visit [www.qualys.com/solarhack/](http://www.qualys.com/solarhack/).

#### Qualys Webinar

Please join us on Thursday, Dec. 24, for a webcast with the Qualys vulnerability and malware research team to discuss the recent Solorigate/SUNBURST attack and get more information on using Qualys' free 60-day service to mitigate risk and exposure from the breach. Register at [qualys.com/solarwinds-fireeye-webcast](http://qualys.com/solarwinds-fireeye-webcast).

#### Additional Resources

- Read the [Qualys Security Advisory](#) blog
- Details on the [Qualys Cloud Platform](#)
- Learn about the [Qualys Cloud Agents](#)
- Follow Qualys on [LinkedIn](#) and [Twitter](#)

#### About Qualys

Qualys, Inc. (NASDAQ: [QLYS](#)) is a pioneer and leading provider of cloud-based security and compliance solutions with over 15,700 active customers in more than 130 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and consolidate their security and compliance solutions in a single platform and build security into digital transformation initiatives for greater agility, better business outcomes, and substantial cost savings.

The Qualys Cloud Platform and its integrated Cloud Apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance, and protection for IT systems and web applications across on premises, endpoints, cloud, containers, and mobile environments. Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading cloud providers like Amazon Web Services, Microsoft Azure and the Google Cloud Platform, and managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, DXC Technology, Fujitsu, HCL Technologies, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance. For more information, please visit [www.qualys.com](http://www.qualys.com).

*Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.*

#### Media Contact:

Tami Casey, Qualys  
(650) 801-6196  
[Tcasey@qualys.com](mailto:Tcasey@qualys.com)

 View original content to download multimedia: <http://www.prnewswire.com/news-releases/qualys-researchers-identify-7-million-vulnerabilities-associated-with-solarwindsfireeye-breach-by-analyzing-anonymized-vulnerabilities-across-worldwide-customer-base-301197812.html>

SOURCE Qualys, Inc.