Host Insights for Cortex XDR

Safeguarding endpoints starts with getting a clear picture of all your endpoint settings and contents to understand your risk. Once you've identified a threat, you need to stop it quickly and ensure it hasn't spread to multiple endpoints.

With Host Insights, an add-on module for Cortex XDR™, you get all these capabilities and more. Host Insights combines Vulnerability Management, Host Inventory, and a powerful Search and Destroy feature to help you identify and contain threats. Host Insights offers a holistic approach to endpoint visibility and attack containment, helping reduce your exposure to threats so you can avoid future breaches.

Benefits

- Find and eliminate active threats anywhere in your environment.
- Understand and prioritize risks with integrated vulnerability management.
- Get additional context for investigations and identify security gaps with unprecedented host and system visibility.
- Streamline operations with a unified platform for endpoint protection, extended detection, investigation, response, and vulnerability management.

Stopping Attacks Requires Speed and Visibility

Time is the enemy when you're responding to threats. Successful attacks must be contained quickly, before adversaries can steal your data. To reduce response times as well as quickly spot and diagnose issues, your analysts need rich, comprehensive data at their fingertips. They also need tools that can instantly scour your environment to find and eliminate active threats.

Often, the entry points for successful attacks are unpatched vulnerabilities. With thousands of new application and system vulnerabilities reported every year, security teams can struggle to find, assess, and prioritize vulnerabilities in their organization. If your team is like many others, they're also grappling with complex network architectures that include corporate campuses, branch offices, remote users, and cloud applications. These perimeterless, distributed networks are making traditional vulnerability scanners obsolete.

To effectively manage app and system vulnerabilities without burdening your team with endless reports or more tools to manage, you need a simple, scalable vulnerability management solution that integrates with your existing security infrastructure.

Host Insights for Cortex XDR

Host Insights, with the combination of Search and Destroy, Vulnerability Management, and Host Inventory, boosts the power of Cortex XDR to help your security team quickly and accurately identify and contain threats.

Figure 1: Host Insights Module

Search and Destroy

Search and Destroy lets you instantly find and eradicate threats anywhere in your environment. This powerful feature indexes all the files on your managed Microsoft Windows® endpoints so you can sweep across your organization to find and remove malicious files in real time. You can root out malicious files while avoiding burdensome and slow endpoint scans. Granular settings allow you to exclude files and directories on specific hosts.

Vulnerability Management

The Host Insights module offers you real-time visibility into vulnerability exposure and current patch levels across your endpoints to identify risk and prioritize mitigation. It reveals the vulnerabilities on your Linux and Windows endpoints, with up-to-date severity information provided by the NIST National Vulnerability Database and the Microsoft Security Response Center, including Common Vulnerabilities and Exposures (CVE) severity and metrics.

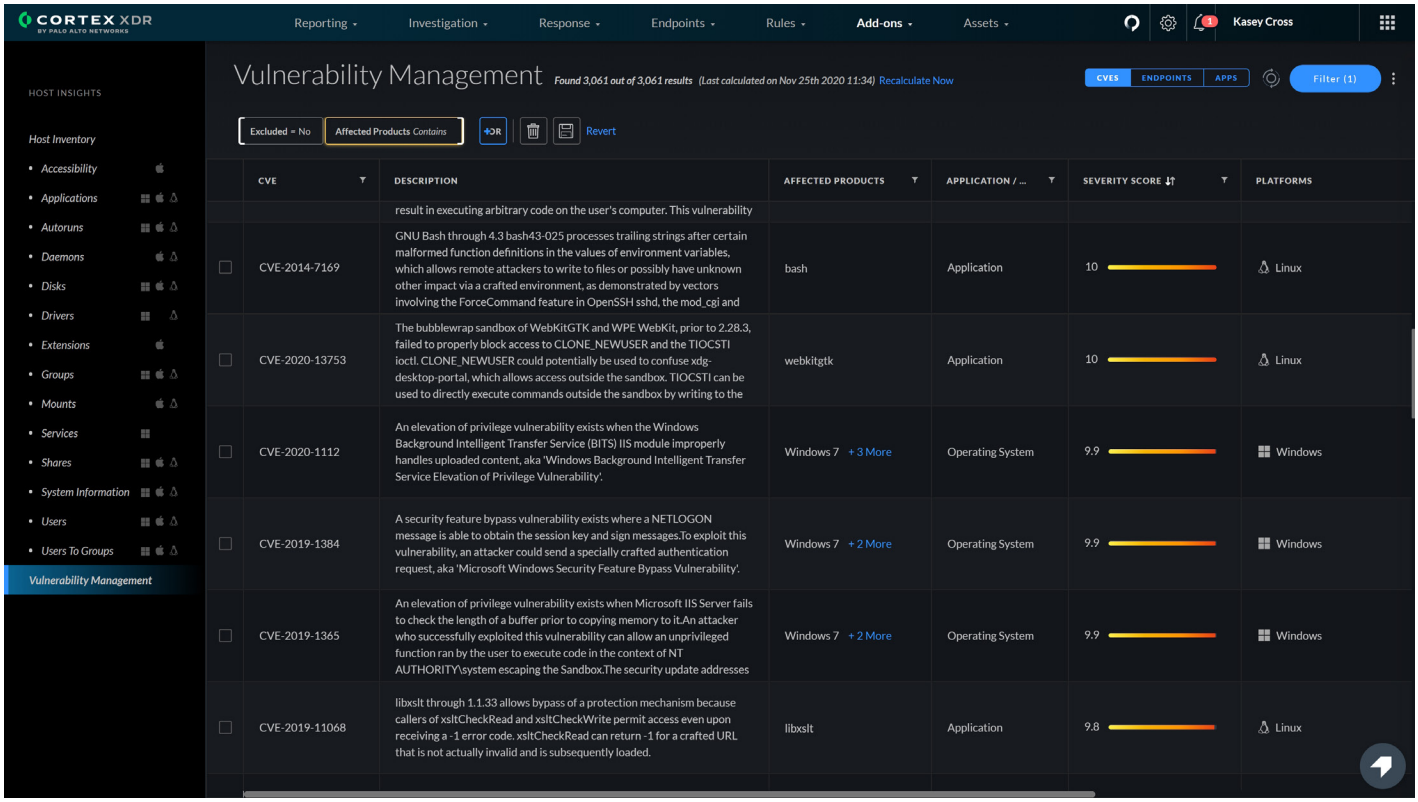

Figure 2: Vulnerability Management window with up-to-date CVE data from the NIST National Vulnerability Database and Microsoft Security Response Center

To help you better visualize findings, the Vulnerability Management features provide graphical dashboard and report widgets to reveal key insights, such as top vulnerable applications, top vulnerable hosts, and more. You can also exclude CVEs that are irrelevant to your environment so you can focus on the vulnerabilities that matter the most.

You can also view the Microsoft Knowledge Base (KB) updates installed on your endpoints.

Host Inventory

With Host Inventory, you can identify security gaps and improve your defensive posture by getting complete visibility into key Windows, macOS®, and Linux host settings and files.

You can view information about users, groups, applications, services, drivers, autoruns, shares, disks, and more. Host Inventory lets you filter, sort, and aggregate data to find the data you're looking for. By getting all your host details in one place, you can quickly identify security issues and speed up investigations with additional host context.

Test-Drive Host Insights

Do you want to see Host Insights in action? If you're a current Cortex XDR Pro per Endpoint customer, simply activate your 30-day trial license from the Cortex XDR License dialog window to get Host Insights today.

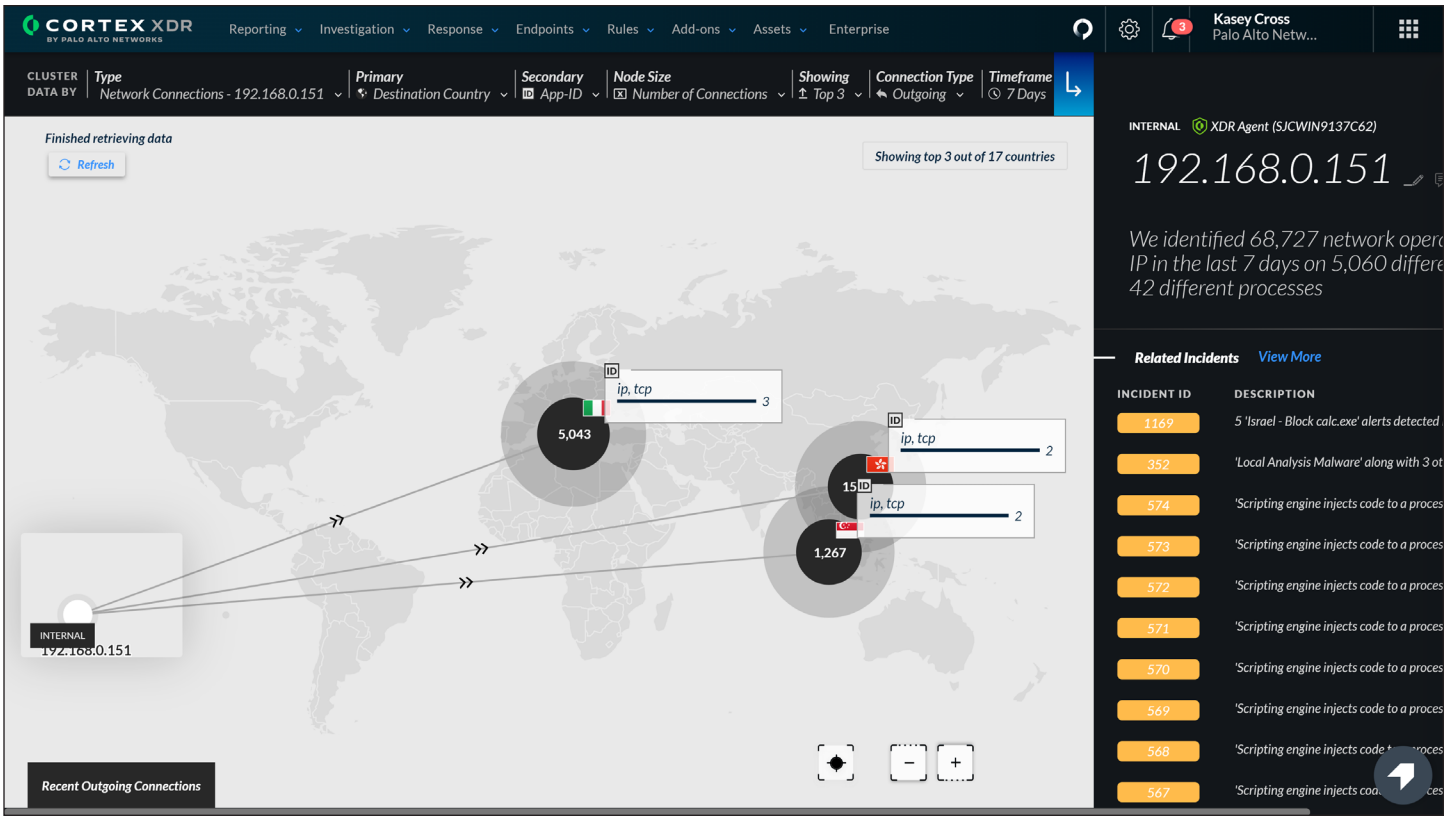

Figure 3: Host Insights includes a unique Asset View to simplify investigations

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

host-insights-for-cortex-xdr-ds-120220