Attack Surface Management Coverage for Remote Workers

Enable Your IT and SOC Teams to Gain an Attacker's View of Your Remote Employee Networks

In the past few years, remote work has become the norm in every organization. Unfortunately, it's not just organizations and their employees that see great benefits from remote work—attackers see opportunities as well.

When employees work from remote networks that are vulnerable or suboptimal, they expose critical data and open the organization to a potential breach. So, employees working from cafes, homes, or coworking locations should be considered to be operating from hostile locations.

The Problem

Remote employees, by definition, can be anywhere, connected to any network, making the job of security far more difficult. Several commercially available routers have known vulnerabilities and key employees (VPs, CXOs, payroll, etc.) connecting through these devices are at the risk of exposing potentially sensitive information.

Getting visibility into the security posture of remote workers is hard, and traditional tools do not help organizations:

- Understand the behavior of remote employees.
- Measure the organizational risk associated with employees working from their homes or temporary networks.
- Ensure that insecure network configurations aren't exposing risky services on corporate devices.

The Solution

Cortex® Xpanse™ provides the visibility needed to protect remote employees and their networks by integrating its leading attack surface management (ASM) platform with Cortex XDR and Prisma® Access GlobalProtect™ VPN service. Once an issue has been identified, customers can remediate them via Cortex XDR response actions, host firewall rules, changing access policies, or by isolating that employee's device.

Table 1: Multiple Ways to Secure Your Remote Workers

Xpanse + XDR	
Capabilities	The Xpanse + XDR integration helps bring Cortex XDR endpoint data together with Xpanse's internet scanning capabilities to: • Identify exposed risky services from where employees are connecting. • Confirm Cortex XDR agent deployment coverage across customer's key networks.
Use Cases	• Monitor your remote employees' network environments to identify operational risks. • Ensure full coverage of Cortex XDR deployment by identifying all externally facing assets that do not have an XDR client installed on them. • Improve response and remediation time by adding full context data of the network from Xpanse to endpoint incidents detected by Cortex XDR.
FAQ	**What version of Cortex XDR is required?** • Customers must have Cortex XDR 3.0 or newer to implement the integration. **Do customers need special licenses?** • No. Customers only need an active Cortex Xpanse and Cortex XDR license with endpoints deployed. **How do I activate the integration?** • Input the Cortex XDR API key into the Expander API connectors page, and it's done. **How frequent are the data refreshes?** • We will refresh existing networks and assets with relevant data daily. There will be a timestamp of the latest update in Xpanse.
Xpanse + Prisma Access	
Capabilities	The Xpanse + Prisma Access integration helps bring Prisma Access' GlobalProtect client data together with Xpanse's internet scanning capabilities to: • Identify exposed risky services from where employees are connecting. • Better understand employee VPN usage and geographic distribution.
Use Cases	• Monitor your remote employees' network environments to identify operational risks. • Ensure full coverage of Cortex XDR deployment by identifying all externally facing assets that do not have an XDR client installed on them. • Improve response and remediation time by adding full context data of the network from Xpanse to endpoint incidents detected by Cortex XDR. • Monitor your remote employees' network environments to identify operational risks. • Utilize remote worker risk posture information to inform security policies.
FAQ	**What versions of Prisma Access and GlobalProtect are required?** • To utilize the new integration, customers must be using Prisma Access with GlobalProtect agents (i.e., mobile users). The integration will also support customers who have deployed GlobalProtect via NGFW or Panorama. This latter qualifier also requires that they have an active Cortex Data Lake (CDL) subscription and are forwarding GlobalProtect logs to CDL. **How do I activate the integration?** • Once customers have both products, they can work with their Customer Success team to enable the integration. **How frequent are the data refreshes?** • We will refresh existing networks and assets with relevant data daily. There will be a timestamp of the latest update in Xpanse.

Benefits of extending ASM coverage to your remote workers:

- Identify risks for key remote employees and deploy enterprise-grade hardware selectively.
- Discover the gaps in coverage of Cortex XDR agents in your organization.
- Use visibility to dynamically change policies and alter access controls based on employee location.
- Ensure employees are using an approved VPN service.
- Improve MTTR by providing additional network data to a given incident identified by Cortex XDR.
- Identify employees working from unapproved locations and employees not using VPNs.
- Find the internal and external IP mapping of your remote workforce.

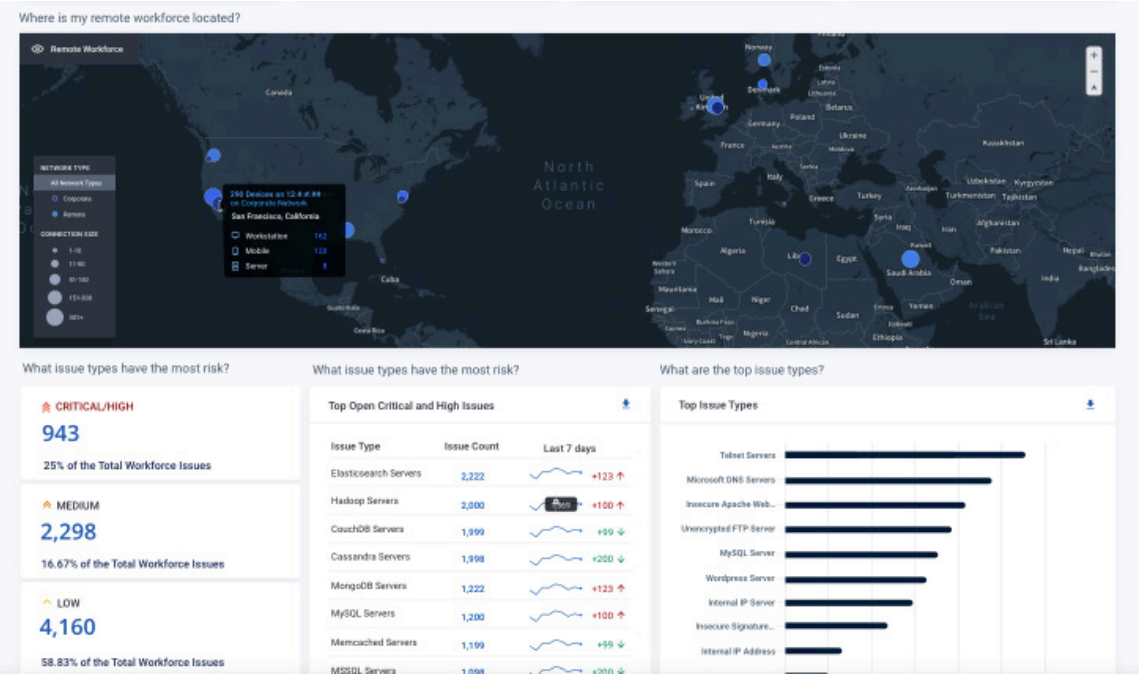

Figure 1: Automate issue prioritization of your remote employee networks

How It Works

Xpanse + Cortex XDR

The integration gathers endpoint data from Cortex XDR (only assets that have a public IP address and have been seen in the last 24 hours) to identify remote workforce devices associated with your organization. It then combines this data with Xpanse's global scan data to identify risky issues and services running on the networks where your employees are located, giving you a complete picture of your remote workforce.

Cortex XDR® gives you internal insight into what's running on those devices, while Xpanse gives you the external perspective and identifies what's exposed to the internet. Teams can remediate risky issues identified on remote networks—either directly on the device via Cortex XDR or via network configurations.

Xpanse + Prisma Access and GlobalProtect

The integration gathers GlobalProtect VPN client data/device data, which could come either through a Prisma Access deployment using GlobalProtect, or from a GlobalProtect instance installed on an NGFW (only assets that have a public IP address and have been seen in the last 24 hours) to identify remote workforce devices associated with your organization. It then combines this data with Xpanse's global scan data to identify risky issues and services running on the networks where your employees are located, giving you a complete picture of your remote workforce.

With the visibility provided by these integrations, organizations can prioritize these issues for remediation and also educate its users about the insecurities in their networks and how to secure them.

To learn more about how you can secure your attack surface, visit Cortex Xpanse.

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