Attack Surface Management Coverage for Remote Workers with Prisma Access

Enable your IT and SOC teams to gain an attacker's view of your remote employee networks with integration between Cortex Xpanse and Prisma Access with GlobalProtect agents.

Introduction

Organizations have been forced to accelerate the migration to a remote workforce model despite very limited visibility into the security of their employees' remote networks. This means organizations have no way of knowing whether there are unknown exposures or critical issues open on remote employee devices or the network environments they are connected to.

What about your critical employees, like your CFO working with key financial information or your teams working with critical customer information? Do you know if they are connecting using routers with known vulnerabilities? Do you dynamically alter their access controls using policies based on where they are working? Or are they still under the same generous access policies as though they were on your office network?

Best practices include:

- Ensuring that insecure network configurations aren't exposing risky services on corporate devices.
- Gaining visibility to dynamically change policies and alter access controls based on employee location.
- Identifying endpoints connecting through known vulnerable routers and assessing the need to deploy enterprise-grade hardware to key employees.
- Measuring the organizational risk associated with key employees working from home or temporary networks.

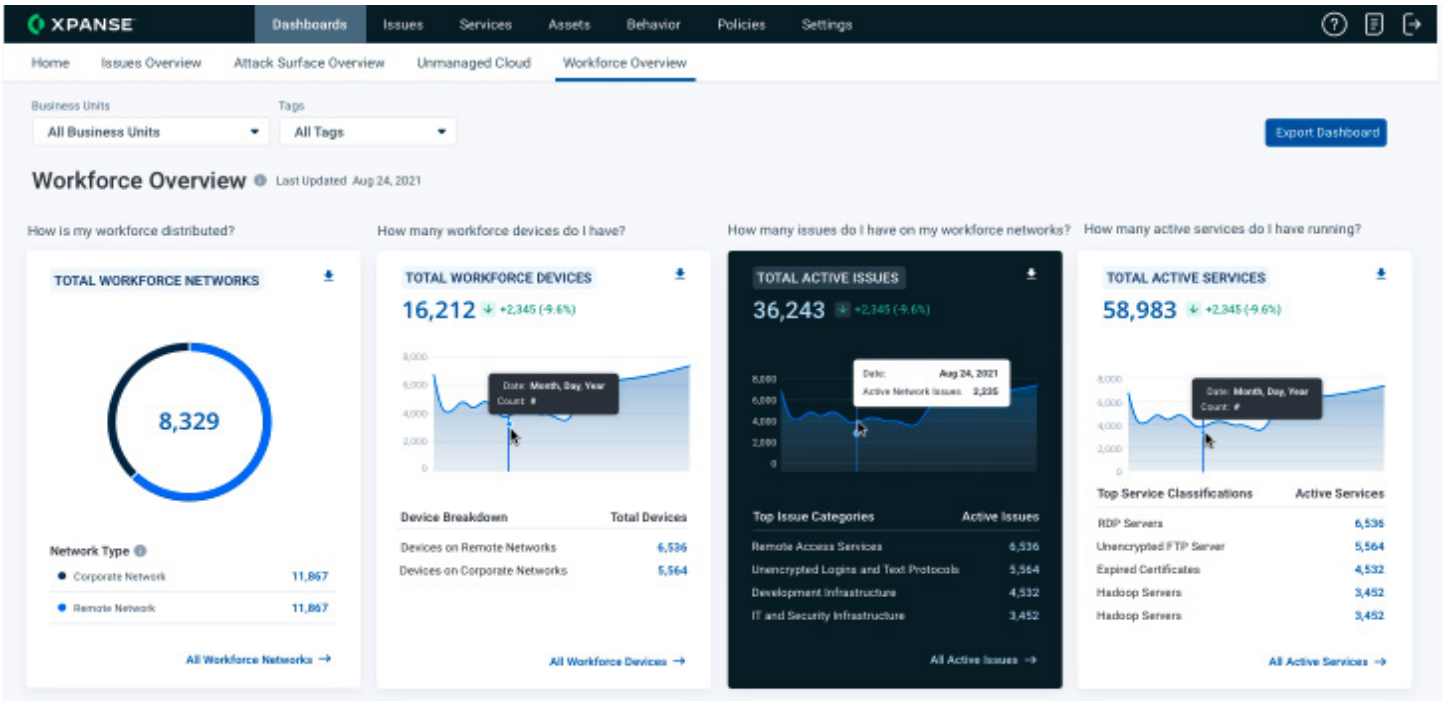

Figure 1: Gain an attacker's point of view into your employees' remote networks

Secure Your Remote Attack Surface

Using this API integration between Cortex® Xpanse™ and Prisma® Access with GlobalProtect™ agents. Organizations can effectively identify and get alerts on security issues on remote worker systems and network environments using public asset information discovered by Xpanse.

Benefits

- Identify risks for key remote employees and deploy enterprise-grade hardware selectively.
- Use visibility to dynamically change policies and alter access controls based on employee location.
- Improve mean time to respond by providing additional network data to a given incident.
- Find the internal and external IP mapping of your remote workforce.

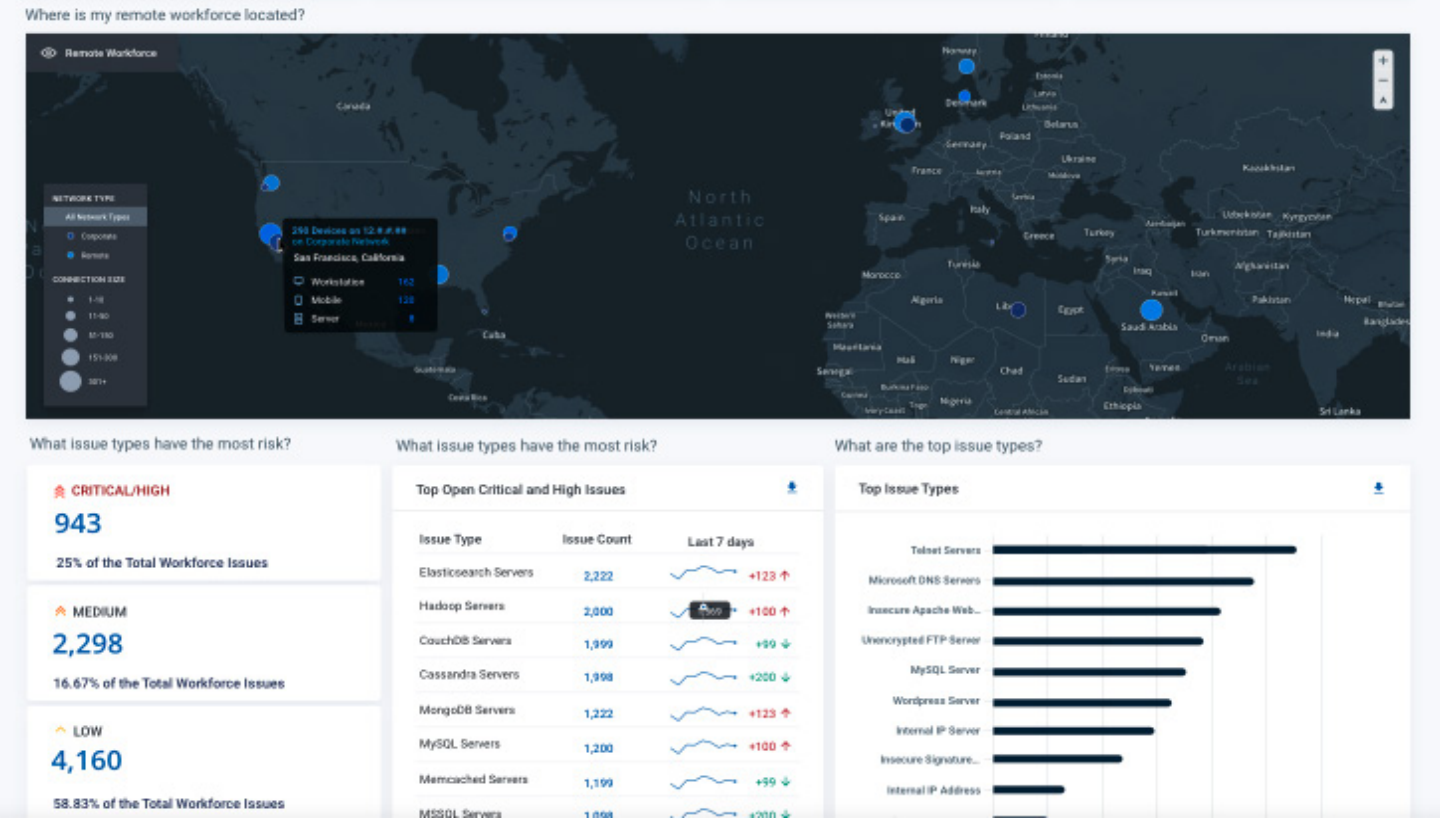

Figure 2: Automate issue prioritization of your remote employee networks

How It Works

This integration has four key capabilities:

- 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 (limited to clients that have successfully connected to GlobalProtect 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 the integration, organizations can more effectively prioritize issues for remediation and educate their users about the insecurities in their networks and how to secure them.
- Lastly, the integration allows you to remediate risky issues identified on remote networks—either directly on the device or via network configurations.

What versions of Prisma Access and GlobalProtect are required?
In order 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.

New Asset Types in Xpanse

There are three new asset types in Xpanse:

- **Networks**: Networks are the grouping of remote devices observed sharing a public IP address. Networks can be remote or corporate if they overlap with the customer's asset map.
- **Devices on remote networks (remote workforce devices)**: This asset type will be extended in the future to support data from additional remote workforce sources.
- **Devices on corporate networks**: These are the devices found on networks that overlap with Xpanse's asset map of an organization.

New Asset Page in Expander

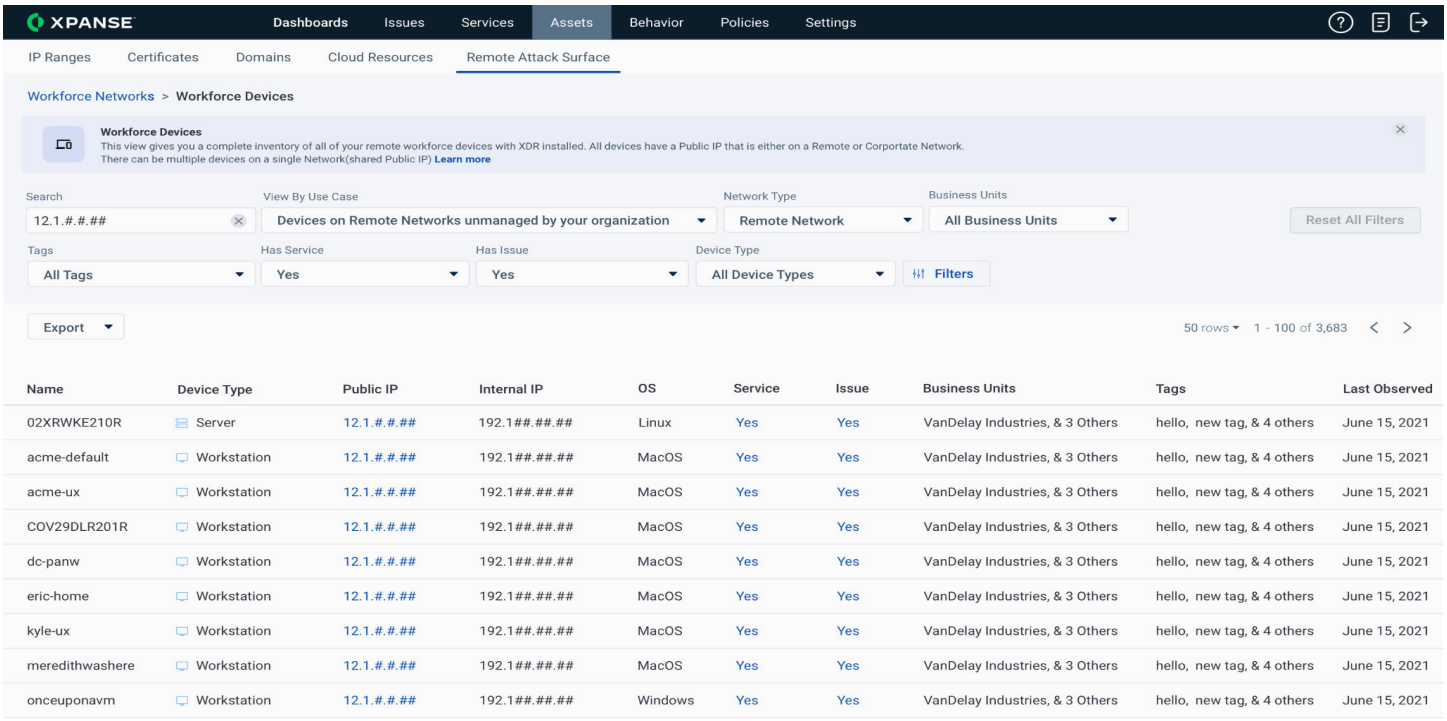

Figure 3: New assets inside Expander based on details from Prisma Access and GlobalProtect

New Features

New features on the Expander asset page include:

- A central repository of all your devices on remote networks.
- The ability to identify the type of device on your network to streamline investigation and remediation.
- Identifying the exact mapping of the external IP to internal IP to better track your devices across networks.

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