paloalto® NETWORKS | CORTEX® XPANSE BY PALO ALTO NETWORKS

Discover and Monitor Your Internet Assets

Your Attack Surface is Constantly Changing

Organizations are managing more internet-connected assets than ever before. But with the rise of the cloud, remote workers, and the decentralization of IT, it's challenging to keep track of all of these assets and their communications.

Existing solutions fall short when it comes to discovering and monitoring unsanctioned, unknown, or misconfigured assets. Organizations need a foundational system of record for their internet-facing assets that includes continuous global discovery and monitoring to assess, manage, and reduce their attack surface. That's where Cortex® Xpanse™ comes in.

Xpanse Use Cases

- **Attack Surface Reduction:** Understand how your organization looks to attackers, find previously unknown assets, and remediate exposures before they're taken advantage of.
- **Cloud Asset Discovery:** Manage your cloud footprint and discover shadow infrastructure as a service so you can bring unknown assets under management.
- **Inventory Management:** Get an automatically populated, continuously updated list of all of your internet-connected assets so you can manage them effectively.
- **Third-Party and Supply Chain Risk:** Assess a third party's cyber risk to identify exposures and improve the security posture of everyone involved.
- **Mergers and Acquisitions:** Ensure digital assets and their exposures are cataloged and known before, during, and after the transaction is finalized.
- **Audit and Compliance:** Identify all of your internet-facing assets to ensure you aren't caught off guard during a compliance audit.

Get a New Perspective

Managing your internet assets and monitoring your attack surface go hand-in-hand. Attackers will evaluate your organization from the outside as they look for gaps, exposures, or other indicators that an asset is out-of-date or not a part of regular monitoring.

IT operations groups are tasked with maintaining an ongoing, up-to-date inventory of all assets. This inventory then feeds into security processes, providing the foundation for what is protected by the security tools they implement.

Xpanse provides the only internet-wide platform to discover and monitor all of your internet-connected assets to:

- Maintain a complete, continuously updated inventory of all the internet-facing assets that belong to your organization, including assets on-premises and across all cloud providers
- Continuously discover unknown assets and bring them under management
- Develop processes and service-level agreements (SLAs) to drive the deviation between what is known and unknown tozero, and to ensure that all assets are well configured
- Continuously monitor assets for indicators of compromise and unusual behavior to prioritize high-risk and high-impact problems

How Xpanse Works

Xpanse indexes the entire internet to collect data about every device connected to it. From there, we build out a comprehensive inventory all internet-connected assets and domains belonging to an organization. Our indexing also surfaces any exposures present on each of those assets that could be attacked or exploited.

With this knowledge, Xpanse can provide you with a comprehensive, continuously updated inventory of all of your internet-connected assets and their details, including associated exposures, non-compliant configurations, and risky communication behaviors.

What Sets Xpanse Apart

A single source of truth for internet-connected assets and their potential exposure to attacks, on-prem, and across all cloud providers

Automatic, continuously updated inventory of assets that belong to an organization, including all business unit and subsidiaries

Visibility into risky and out-of-policy communications between your assets and other assets on the public internet

No installation or instrumentation required

White-glove implementation and ongoing support from IT and security operations experts

Our Products

Expander

- Discover, monitor, and track internet assets automatically, anywhere in the world, and reduce your risks and exposures
- Quantify risks and prioritize internet assets that need remediation
- Bring unknown internet assets under IT control for improved IT hygiene
- Maintain cloud governance with visibility into internet assets across all of your cloud providers

Behavior

Continuously analyze suspicious traffic patterns and exposed services, anywhere in the world, including connections to:

- Tor
- Kaspersky
- Known command-and-control infrastructure
- Prohibited geographies

Link

- Improve the operational security of your strategic suppliers, fix exposed internet assets, and discover suspicious network traffic in your supply chain that no one else can find—anywhere in the world
- Monitor suppliers' internet assets for risky or out-of-policy communications
- Implement a shared governance model to reduce suppliers risk
- Hold suppliers accountable for their security lapses

Where Xpanse Fits into the Security Stack

Xpanse helps enterprise security teams reduce their attack surface by discovering and monitoring the risks and exposures of their global internet attack surface.

Xpanse asset, exposure, and behavior data can be integrated into your existing SIEM and vulnerability management tools to ensure that new exposures, configuration changes, and risky and out-of-policy communications can be flagged for inspection and remediation.

APIs and Integrations

Integrate data about internet assets into existing IT and security platforms like Splunk, QRadar, and ServiceNow.

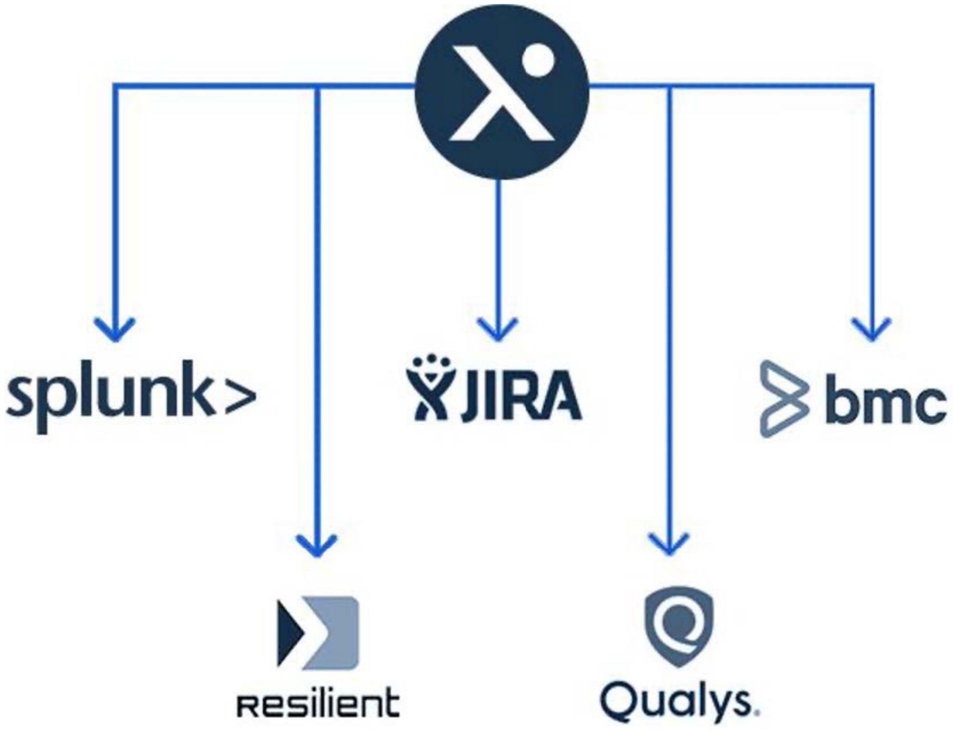

Figure 1: Integrated internet assets

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