paloalto NETWORKS | CORTEX XPANSE BY PALO ALTO NETWORKS

Cortex Xpanse Helps you

- **Discover cloud assets accurately:** Quickly identify all known and unknown domains and hostnames belonging to your organization.
- **Eliminate cloud sprawl:** Independently discover all cloud instances belonging to an organization and go beyond the big three (AWS®, GCP®, Azure®).
- **Improve your cloud VM program:** Enable cloud vulnerability management (VM) tools to resolve the hostname and domain data discovered by Xpanse into active cloud IPs to improve scanning accuracy.
- **Enforce cloud policy:** Complete and continuous view of cloud assets and their respective owners/business units across all known and unknown cloud assets.

Secure Your Known and Unknown Cloud Assets

Save Costs and Stay Secure While Accelerating Your Move to the Cloud

In an October 2020 report, Gartner wrote, "Worldwide, public cloud services will see modest growth of 6.1% in 2020, but will rebound with a four-year compound annual growth rate of 18.8% in 2021-2024. The proportion of IT spending that is shifting to cloud will accelerate in the aftermath of the COVID-19 crisis as CIOs invest in anticipation of returning growth." According to the same report, growth in cloud was 24.7% before COVID-19. Global circumstances have accelerated the move to the cloud.

Traditional Solutions Don't Work in the Cloud

Since cloud deployments can be done with as little as a credit card and an email address, rogue cloud instances are one of the most common inadvertent ways in which an organization's cloud attack surface grows rapidly.

Organizations have been forced to accelerate their digital transformation projects in light of recent demands on their networks. Cloud migration brings not only operating efficiencies but also cost savings. However, organizations will be unable to see these cost and efficiency improvements when they don't have a complete and continuous view into their attack surface. While teams are stressed and operating under pressure, attackers are constantly on the lookout for accidentally exposed vulnerabilities.

Deploying a cloud access security broker and instituting governance policies are good first steps, but they don't solve the problem of rogue cloud deployments.

While cloud workload protection platforms (CWPPs) are great at protecting data inside cloud-based software as a service (SaaS) tools, they are not helpful in identifying shadow IT infrastructures like a development instance spun up by a test engineer. The ability to track whether employees are adhering to policies is also critical. Cloud security posture management tools help manage policies, but they only do so for known cloud instances.

While organizations have developed cloud governance strategies to address some issues that this rapid cloud development has created, CISOs are often left with an incomplete picture when they ask their teams, "How are we ensuring our cloud policies are enforced?"

The cloud is growing every day. We have observed that:

On average, companies add
3.5 new
publicly accessible cloud services per day—nearly 1,300 per year.

At the high end, one customer added
693 new
publicly accessible cloud services in a single day.

Do you know your actual cloud instance inventory?

Do you know how many cloud instances in your organization are in unsanctioned cloud providers?

Cortex Xpanse can help you find out.

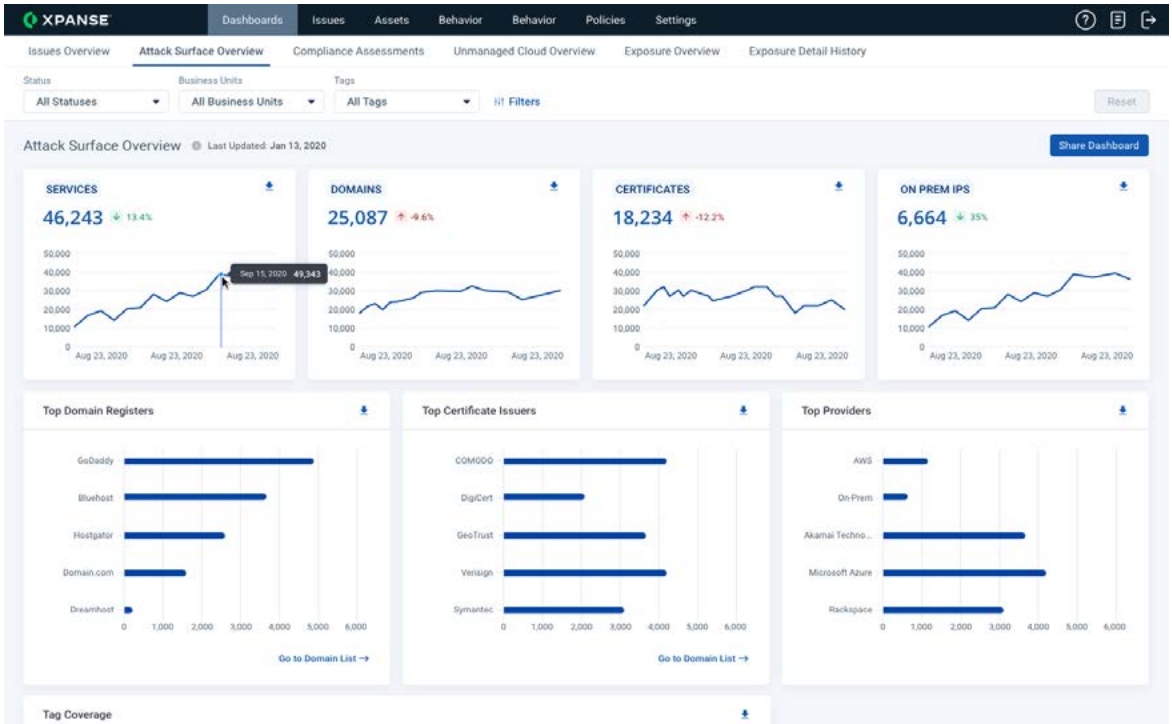

Figure 1: Cortex Xpanse Attack Surface Overview

Traditional Solutions Don't Work in the Cloud

Cortex® Xpanse™ overcomes the limitations of traditional solutions and goes further in locating all cloud exposures to enforce an organization's cloud policy. With Xpanse, organizations can monitor and remediate a wide range of critical issues that arise during cloud migration projects.

Xpanse detects systems and services belonging to your organization across the global internet by delivering specialized payloads that target specific port-protocol pairs. By fusing this information with a number of public and proprietary datasets, we are able to match the full and correct set of internet-facing systems and services back to your organization. Xpanse finds cloud assets belonging to your organization across all cloud providers, not just AWS, Azure, and GCP. We deliver this data in Expander with high confidence and industry-best accuracy.

Example of Risks Uncovered

A Fortune 100 information technology company had corporate policies around only hosting company assets in three approved providers. The Xpanse cloud module discovered assets across more than 10 providers and their account owners.

What Sets Xpanse Apart

- Highly accurate discovery and attribution of all internet assets
- A single source of truth for assets on-premises and across all cloud providers
- Automatic, continuously updated inventory of assets
- No installation required—we can work solely off your company name and information on the public IPv4 space

Table 1: Cloud Security with Cortex Xpanse		
	Xpanse Platform	**Legacy Solutions**
1. Discover Cloud Assets Accurately	Customers can ingest Xpanse-identified fully qualified domain names into their VM tools for accurate cloud scanning.	Traditional IP scanners don't work for the cloud since the IP addresses are always changing. They also don't have a complete list of target accounts to scan.
2. Eliminate Cloud Sprawl	We independently discover all cloud instances belonging to an organization, and go beyond the big three (AWS, GCP, Azure).	Need to be manually deployed across each account and are limited to the big three.
3. Identify and Remediate Shadow Cloud	Our platform can identify and attribute all cloud instances that belong to your organization, which will help you bring services hosted on other providers into your sanctioned provider list.	CWPPs can only protect data inside your SaaS applications and cannot identify all instances that belong to your organization.
4. Discover Cloud Dev Environments	Xpanse can identify and alert on any dev environments that are accidentally exposed to the public internet.	No comparable solution exists.
5. Enforce Cloud Policy	Set up alerts when cloud assets from unsanctioned providers show up on your network.	Only work on known providers and need to be manually installed on every provider.
6. Identify Insecure Certificates	Discover public-facing certificates and alert based on certificate misconfigurations, including expired certificates, long validity, etc.	Can only track known certificates that have been manually added or imported into a certificate management solution.
7. Identify and Patch Web App Services	Our data enrichment process helps to ensure that all web server software versions are approved and are not using end-of-life software versions, etc.	Incomplete since they can only scan known assets.
8. Identify Colocated Cloud	Discover and remediate some of the most commonly exposed co-located cloud services, like SSH, FTP, and POP3, to prevent potential breaches.	No comparable solution exists.
9. Audit Your M&A Cloud Assets	Independently assess security risks of potential acquisitions and drastically reduce the amount of time it takes to discover and integrate an acquired company's assets.	No comparable solution exists.
10. Enable Seamless Integrations	Leverage Xpanse engineering support to build custom integrations to seamlessly integrate our platform in your workflow.	Limited documentation support and do not support development of custom integrations to find issues with dangling DNS.

CORTEX
BY PALO ALTO NETWORKS

Save Costs on Cloud Migration with Cortex Xpanse

Help Your Team Discover Unknowns

While most cloud migration projects result in cost savings, a suboptimal digital transformation project could actually end up costing you more in the long term. For security teams, maintaining full visibility into colocated cloud infrastructure is extremely difficult since they don't have a complete view of unknown/unsanctioned cloud instances, and their known cloud assets are ephemeral and not linked to static IP addresses.

How is a central IT team going to manage this cloud sprawl, especially if it's due to using multiple clouds? It's hard enough to manage internal systems with asset inventories and configuration management databases that are often out of date and may not represent the entirety of the environment. How can you enforce policy on moving targets or those that you don't even know about?

Xpanse provides an automatically updated system of record for cloud assets through continuous agentless discovery, attribution, and monitoring across all of your sanctioned and unsanctioned cloud environments for security risks and noncompliance. Xpanse will discover all of your public cloud assets and enrich them with metadata, making it easy to prioritize actions and potential remediation.

You can also identify coloted cloud exposures (e.g., an exposed database server hosted on the same IP as one of your web applications). This helps your team with an accurate picture of your cloud and on-premises assets to accelerate digital transformation initiatives. You can also save costs by getting more out of your existing InfoSec tools since the Xpanse platform complements them to improve operational efficiency of an organization's workforce by reducing mean time to detect and mean time to response.

Xpanse Cloud Security Success Stories

A large financial services organization used Xpanse to identify more than double the number of assets that they were already tracking in their known AWS accounts.

A Fortune 500 commercial real estate company used the Xpanse cloud module to identify a development database server publicly exposed in cloud IP space, outside of the corporate cloud. This development environment was running multiple services, including critical remote access protocols. They remediated the service as soon as it was discovered. This was not on the organization's known IP space and outside the organization's visibility without the Xpanse cloud module.

Conclusion

While organizations are moving into the cloud to save costs and be agile in their operations, improper implementation will result in more expenses. Xpanse provides IT operations, DevOps, and security teams with the confidence that their cloud governance and digital transformation projects are being pursued and implemented securely, according to policy, and that they stay that way over time.

About Xpanse

Xpanse protects the world's most important organizations by discovering risks on the internet that no one else can find. Xpanse customers comprise more than 10% of the routable internet and rely on Xpanse to discover, evaluate, and mitigate their global internet attack surface. Using patented data collection, processing, and analysis technology, Xpanse reduces risks associated with internet assets and enables a secure digital transformation for the world's largest organizations.

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

cortex-xpanse-Secure-Your-Known-And-Unknown-Cloud-Assets-wp-05122021