Discovering Your Total Cloud Footprint

Cloud Transformation Demands a New Approach to Security

Today, most organizations have, or are building, substantial cloud footprints. Huge drivers of this are developers, marketing, and other non-IT functions creating (and abandoning) assets in the cloud. Many of these unknown and unauthorized cloud assets are in ephemeral IP space, making it even harder for organizations to get a holistic view of their cloud footprint for security and infrastructure management. Much of this development occurs outside approved corporate infrastructure as a service accounts.

What Customers Are Saying:

"We have centralized management for our Amazon accounts … but we are worried about what we don't know that is outside of our management view."

—CISO
Large Tech Company

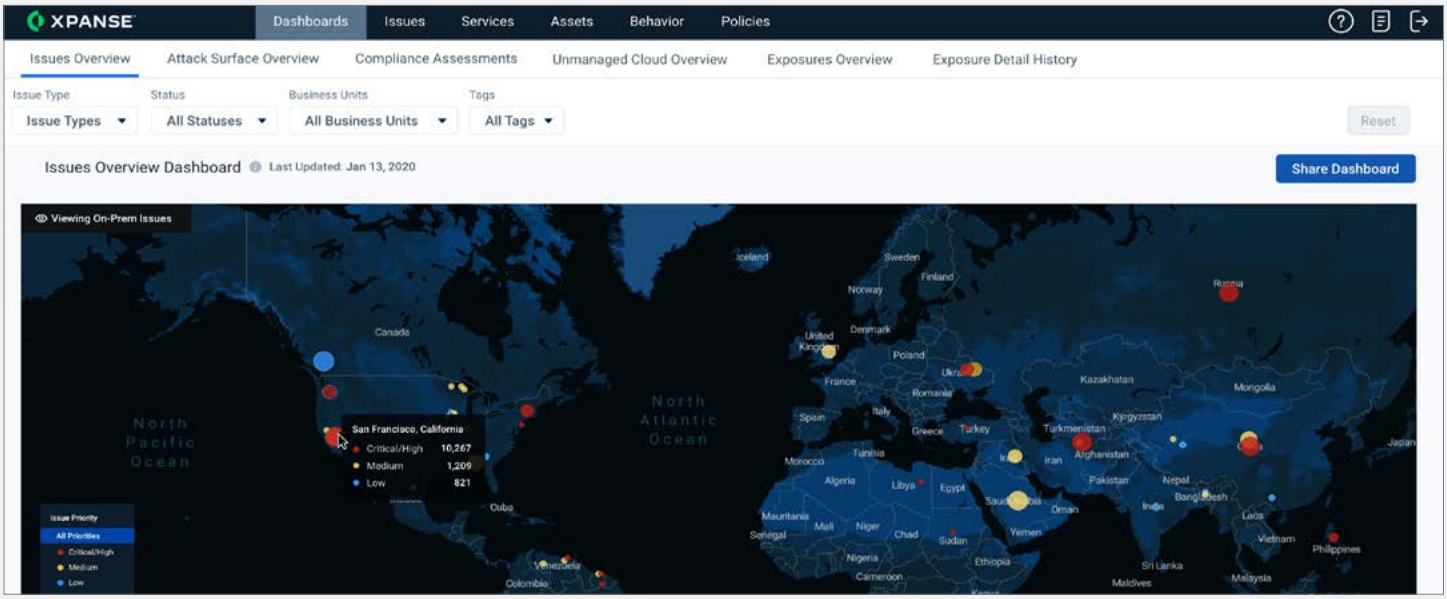

Figure 1: Discover managed and unmanaged cloud in one place

Global Cloud Adoption Brings Unaddressed Challenges

As global cloud adoption climbs, new challenges for IT and security teams emerge that current tools fail to address. While securing known assets is straightforward, it is not possible to secure what is not known—things like shadow infrastructure and rogue development, both of which abound in the cloud. Enterprise cloud footprints present unique challenges, including:

- **The failure of existing tools** to discover cloud assets across authorized and unauthorized providers in a current, reliable, and comprehensive manner.
- **The ease and speed** with which unknown and unauthorized cloud assets can be spun up and remain active and undiscovered.
- **The deficiency of existing tools** to reliably surface owned assets vs. other assets in multi-tenant or ephemeral environments.

Managing and securing assets in ephemeral IP space requires a view of assets that is current and accurate. Incumbent tools fail because they track cloud IP addresses to an organization simply because that IP address was seen hosting a company asset at one time—information that quickly gets stale and isn't useful or actionable for securing rogue cloud assets. In this key way, security paradigms designed for static networks don't work in the cloud, and relying on this ineffective approach can cause IT and security practitioners to scan, penetration test, and waste time investigating assets that aren't even theirs—all while missing critical unknown cloud assets that create risk.

Organizations cannot use these tools to build a holistic view of their cloud assets. Without a better strategy, organizations are left with an incomplete view of their internet assets and no way to monitor critical business applications hosted in the cloud.

The "Whole-of-Internet" Approach to Discovering and Securing Cloud Assets

Today, an organization's cloud assets can reside in any provider in the world—including in residential/commercial cloud providers. To fully solve the problem, organizations must take a discovery-first, "whole-of-internet" approach to cloud security.

Once cloud assets are discovered and any misconfigurations are exposed, organizations may leverage a myriad of cloud security tools on the market to manage asset permissions and other configuration items—but cloud asset discovery must be a continuous process to maintain a clear and accurate picture of the organizational cloud footprint.

Cortex® Xpanse™ Expander gives you a powerful, streamlined web interface that provides detailed information about attributed cloud IP addresses.

CORTEX
BY PALO ALTO NETWORKS

A "whole-of-internet" approach relies on the collection, correlation, and attribution of internet data to discover and present an organization's total cloud footprint.

Table 1: The "whole-of-internet" approach defines every public-facing asset

	What It Does	Why It's Important
Complete global internet coverage	Records details of all publicly routable assets, services, and their configuration details across the entire global internet.	If this isn't comprehensive, the discovery process will miss assets that should be attributed.
Comprehensive service classification intelligence	Maintains an accurate rule set that uses combinations of ports, protocols, and response details to classify specific service types. It must index every IP across multiple ports and protocols and then apply these rules to the responses in order to parse and record every routable service.	Inaccurate or incomplete service classification intelligence will lead to undiscovered or misclassified cloud services.
Frequent indexing of global internet	Maintains a current snapshot of publicly routable assets.	Infrequent indexing will lead to stale or undiscovered cloud assets.
Detailed organizational fingerprints compilation	Maintains an accurate set of an organization's fingerprints on which to search the global internet dataset for attributable cloud assets.	Inaccurate or incomplete lists will lead to undiscovered or misattributed cloud assets.

What Customers Are Saying:

"My biggest shadow infrastructure problems is in cloud providers we don't even recognize."

–Director of Cloud Security Operations
Large Tech Company

"Marketing is my worst problem … They spin up commerce sites in the cloud that nobody in it knows about and then they just forget them … "

–Director of Security Architecture and Vulnerability Management
Large Tech Company

"We discovered assets in three cloud providers when we only knew about one … "

–SOC Lead
State Government Organization

The Value of Complete Cloud Discovery

Well-executed "whole-of-internet" cloud discovery provides substantial business value to organizations through:

Identification of shadow infrastructure or rogue development noncompliant with company policy.

"We discovered assets in three cloud providers when we only knew about one…"

–Head of Incident Response
Fortune 100 Healthcare Company

Consolidation of all previously unknown cloud assets into a sanctioned management console for centralized control and visibility.

"All of our cloud assets should be in our central AWS account; anything else should be moved to it and consolidated."

–CISO
F100 Services Organization

Confirmation that asset permissions are configured correctly by comparing against the system's view of that asset from the internet.

"Xpanse policy management dashboard was helpful in enforcing policies centrally across our organization."

–VP of Security Infrastructure and Vulnerability Management
Large Financial Services Organization

Risk mitigation of exposures on cloud assets not previously under management or those exposed unintentionally through configurations and permissions.

"We discovered an engineer accidentally left up a dev environment in AWS. We had him take it down."

–CISO
Large Tech Company

Trend analysis of the organization's cloud footprint by provider to better understand cost and consolidate contracts.

"A third party manages our cloud assets, but I want to verify that they are managing our assets according to our policies."

–Head of Vulnerability Management
Healthcare

Let's Talk.

Visit https://go.expanse.co/demo-request.html to set up a demo.

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