Cortex Xpanse Third-Party Attack Surface Assessment for Partners

Differentiate Your Services for Your Clients by Incorporating Critical Attack Surface Assessments

Organizations today have more complex and difficult-to-manage attack surfaces than ever before. Whether they're working to secure an on-premises network, unknown cloud infrastructure, globally distributed business units, or remote employee workstations, it can be nearly impossible to get visibility into and manage their complete external attack surface.

Partners can leverage the Cortex® Xpanse™ Third-Party Assessment product to provide visibility into their end clients' attack surfaces, including their internet-facing assets and any misconfigurations that introduce risk into their network. Partners can incorporate the findings from these assessments into their existing services, such as vulnerability management, pentesting, cloud security, and incident response, to provide a heightened and differentiated level of protection for their clients.

How the Xpanse Third-Party Assessment for Partners Works

Discovery

The Xpanse Third-Party Assessment discovers your end clients' internet-facing assets by scanning the entire internet across all 4.3 billion IP addresses, categorizing the responses, correlating them with several other public and proprietary datasets, and using machine learning to attribute relevant assets back to your end client's organization with unmatched accuracy. Assets are categorized and organized by hosting environment (on-premises or in the cloud) in the Xpanse Third-Party Assessment platform to offer you and your clients a complete asset inventory.

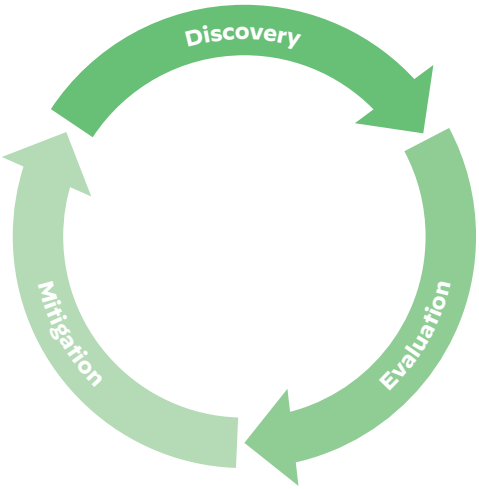

Figure 1: Third-Party Assessment cycle

Evaluation

Once an end clients' assets are discovered, the Xpanse Third-Party Assessment product scans those assets across more than a hundred ports and protocols to identify services that are running and any misconfigurations that introduce risk to the organization. These findings are managed as out-of-the-box policies in the platform with a default prioritization level that you or your end client can customize. Examples include:

- Remote access servers like RDP
- Database exposures like MySQL
- Insecure or expired SSL certificates
- Web application risks such as unencrypted logins and exposed development environments

Mitigation

You or your end client can take action on any misconfigurations with in-product workflows such as deeper issue investigation, assignment to the point of contact, and progress tracking. Xpanse's Third-Party Assessment platform also supports multiple workflow integrations such as those with ticketing systems, SIEMs, and SOARs to help you reduce MTTR of internet exposures on behalf of your clients.

The Third-Party Assessment platform can be configured to be solely accessible to the partner or co-deployed where both the partner and the end client can interact with the insights in the product.

Partner Benefits

Differentiated services
Use the visibility to enhance the existing service/offer being delivered.

Net new services
Deliver new services that provide attack surface visibility, evaluate risks identified, and mitigate risks to improve enterprise security posture.

Improved efficiency
Replace manual ways to comprehensively discover attacks.

Partners can use Xpanse's Third-Party Assessments to differentiate the following services:

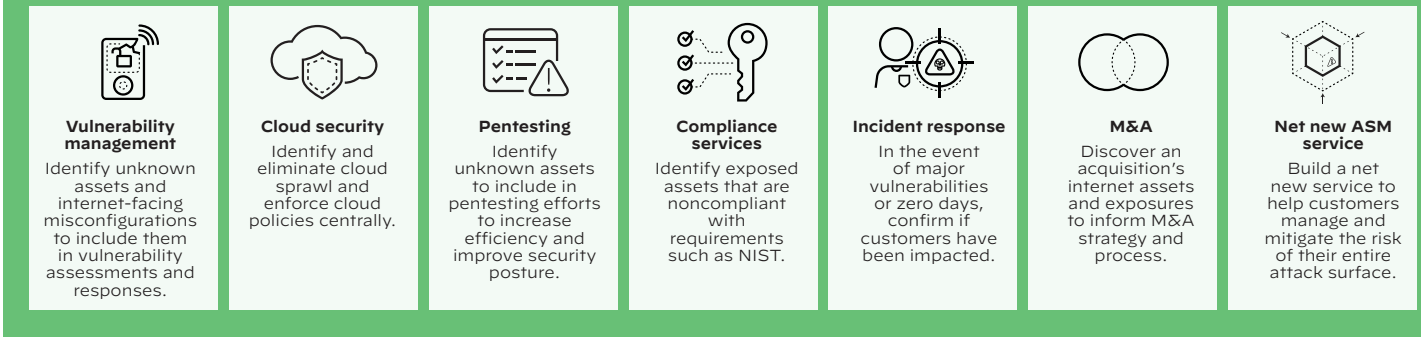

Figure 2: Partner services to incorporate with Third-Party Assessments

Xpanse's Third-Party Assessment Platform Is Built for Partners

Xpanse's Third-Party Assessment platform comes with capabilities critical to support and enable partners, such as:

- **No deployment:** No configuration is needed to discover the attack surface, reducing partner onboarding complexity and time to revenue and increasing client time to value.
- **Multitenancy:** The ability for partners to easily switch between Expander instances for their tenants using the same login.
- **Customizable:** Separate tenants for each client allow partners to tune policies according to client needs and reduce noise in alerts for their analysts.
- **Enriched context:** Internet asset informs prioritization of Xpanse incidents and can enrich and inform prioritization of other partner alerts.
- **Operational platform:** An extensive APIs and ecosystem of out-of-the-box integrations. The issue management capability allows partners to track incident status and analyst comments.

End Client Benefits

MTTD
Faster time to discover internet-facing assets and their misconfigurations

MTTR
More effective and efficient remediation of internet-facing misconfigurations

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_ds_xpanse-third-party-assessment-for-partners_030922