Expander from Cortex Xpanse

Actively Discover and Automatically Respond to Your Unmanaged IT Infrastructure Risks—Without Manual Work

The move to hybrid work and expansions in the cloud have scattered your IT infrastructure and created new challenges for your security teams. More and more security teams struggle with limited attack surface visibility, which leads to an inability to respond quickly to zero days, an ever-growing backlog of repairs, and unclear risk prioritization due to the overwhelming volume of alerts.

At the same time, your scattered IT infrastructure offers attackers new opportunities. In 2022, attackers started scanning for vulnerabilities within minutes of most published remote code execution exploits,[1] while organizations take more than three weeks to find and fix their risky exposures, on average.[2] It's an unfair fight and the attackers have the edge.

> 69% of organizations experienced at least one cyberattack on unknown or unmanaged assets.[3]
>
> – **"ESG Security Hygiene and Posture Management Survey"**

However, your security teams can turn the odds in your favor with Cortex Xpanse. Expander, the flagship solution from Cortex Xpanse, is an active attack surface management solution that helps your organization actively discover, learn about, and respond to unknown risks in all connected systems and exposed services.

Current Methods of Defense Are Incomplete

Legacy vulnerability scanners scan infrequently. Security ratings and periodic pentesting focus only on your known assets. But what about the 30% or more assets that you're not monitoring?[4]

Table 1: Your SOC Can Use Xpanse to:

Fix Security Blind Spots	Automatically discover and eliminate risks from unmanaged IT infrastructure in your environments.
Prevent Ransomware	Actively shut the door on ransomware attacks with automation.
Eliminate Shadow Cloud	Eliminate unsanctioned, rogue cloud sprawl.
Improve Zero-Day Response	With just a click, assess and reduce your exposure to the latest CVEs.
Improve M&A Evaluation	Achieve better due diligence on security posture pre- and post-mergers and acquisitions.
Internet Operations Management	Actively discover risks on all your internet-connected systems and services.
Reduce Cyber Insurance	Eliminate unknown exposures to reduce insurance risk and premiums.

Fight Back with Active Attack Surface Management

Proactively manage your attack surface with Expander. Powered by several unique capabilities, Expander can help you not just find, but automatically fix, your risky exposures before your attackers can exploit them.

1. **Active discovery**: Automatically and continuously scan the entire internet. Actively discover and index your unknown risks in all connected systems and exposed services.

   Xpanse detects systems and services belonging to your organization across the global internet by delivering specialized payloads that target specific port-protocol pairs. In addition to discovering on-premises assets, Xpanse finds cloud assets belonging to your organization across all cloud providers—not just AWS, Azure, and GCP.

[1] 2022 *Cortex Xpanse Attack Surface Threat Report*, Palo Alto Networks, April 19, 2022.

[2] Ibid.

[3] Jon Oltsik, "ESG Security Hygiene and Posture Management Survey," ESG, January 27, 2022.

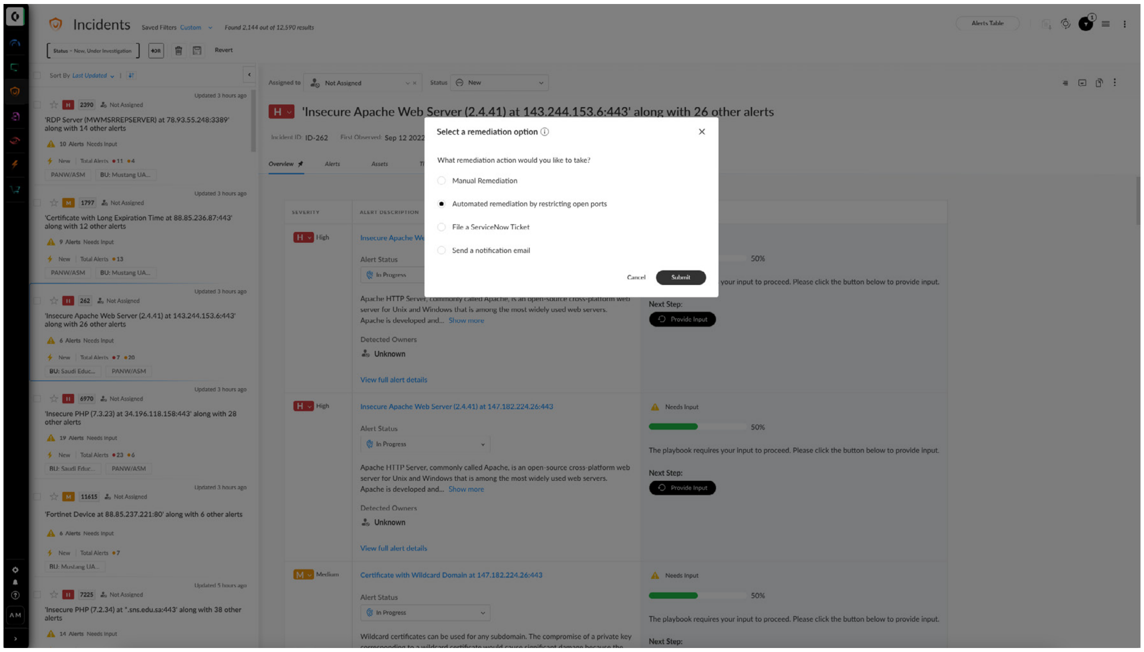
[4] 2022 *Cortex Xpanse Attack Surface Threat Report*, Palo Alto Networks.

2. **Active learning**: Use supervised machine learning models to continuously map your attack surface and prioritize remediation efforts. Reduce mean time to detect (MTTD) and mean time to respond (MTTR) without additional analysts.

   Our proprietary attribution engine then analyzes ownership signatures and relationships between different systems to dynamically attribute your internet assets back to you. We do all of this without requiring any agents or instrumentation on the customer side. Your Expander instance also comes with clear, out-of-the-box policies to help you identify the issues that need your attention the most.

3. **Active response**: Immediately reduce your attack surface risks with built-in automated playbooks instead of merely raising IT tickets.

One persistent challenge for many organizations when remediating attack surface risks is the highly manual and time-consuming task of determining the ownership and business context of unknown assets. Unlike attack surface visibility tools, the Active Response Module in Expander solves this challenge and automatically resolves exposures to reduce your risks.


Incidents
'Insecure Apache Web Server (2.4.41) at 143.244.153.6:443' along with 26 other alerts
Status New

Select a remediation option ⓘ

What remediation action would you like to take?

○ Manual Remediation
● Automated remediation by restricting open ports
○ File a ServiceNow Ticket
○ Send a notification email

Cancel | Submit

Figure 1: Empower your analysts with automated playbooks to resolve exposures faster

With user-friendly workflows, seamless integrations, and cybersecurity experts on call to support your account, Expander helps you take action to mitigate any risky systems or services and protect your organization.

Hear from Xpanse customers through Gartner Peer Insights:

“Great team of architects that had the wisdom to look further out than we did.” – CTO, Finance

“Special armor kit for SOC.” – Manager, Finance

”Overall experience has been outstanding. This product has allowed us to discover assets that we were not monitoring.” – Security and Risk Management, Finance

Not Just a Solution—Your Attack Surface Management Partner of Choice

White Glove Support

Every Expander customer gets an expert support team, including a dedicated technical engagement manager, cyber research analysts, and field engineers. Our team does the heavy lifting for you to help you get the maximum value from your Expander implementation.

Consolidate and Integrate

Expander has several out-of-the-box integrations with the Palo Alto Networks suite of security solutions to help you consolidate your SOC workflow on one platform.

Expander can serve as a system of record for your global external attack surface and help you get the maximum possible value from your existing tool set.

Rapid Response to New Security Concerns

Xpanse can rapidly deploy new policies to monitor specific internet-exposed systems and services. When new zero-day exploits and CVEs are announced, Xpanse can quickly turn around discovery for that system in Expander. This empowers your team to stay nimble in responding to the ever-changing security landscape.

Some of the world's largest and most demanding organizations use Xpanse to secure their attack surface by reducing their risky exposures. Xpanse protects the U.S. Department of Defense, all six branches of the U.S. military, several federal agencies, and large enterprises like Accenture, AT&T, American Express, AIG, Pfizer, and over 200 others. Learn more about how organizations are funding their ASM initiatives: Value Drivers for an Attack Surface Management Program.

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