# Expander

## A Better Way to Manage Your Attack Surface



Organizations today have more complex and difficult-to manage attack surfaces than ever before. Whether you're working to secure an on-premises network, unknown cloud infrastructure, critical supplier networks, or remote employee workstations, it can be nearly impossible to get visibility into and manage your complete external attack surface. That's where Expander, Expanse's flagship solution, comes in. Expander helps you discover, evaluate, and mitigate your global external attack surface to secure your organization.

## Industry-Leading Discovery

Expanse 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. In addition to discovering on-prem assets, Expanse 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.

By looking at both assets with clear ownership indicators and any assets related to them, Expanse provides you with the most complete, current, and accurate inventory of your global Internet attack surface with Expander.

## Expander Helps You:

**Reduce mean time to detect (MTTD):** Quickly identify any risky assets and services belonging to your organization that are exposed on the public Internet.

**Reduce mean time to remediate (MTTR):** Remove exposed assets or put measures in place to protect risky exposures before bad actors find them.

**Boost security team productivity:** Improve productivity by reducing manual processes and providing a system of record for Internet assets across other IT and security systems.

**Prevent a costly breach:** The cost of a security breach can easily stretch into the millions. Prevent a breach with Expander by identifying threat vectors before attackers do.

# How It Works

## 1. Discover

Expanse indexes every system and service on the global Internet every day. 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.

## 2. Evaluate

Your Expander instance comes with clear, out-of-the-box policies to help you identify the Issues that need your attention the most. Prioritize and triage the Issues that are most important to you. You can also deploy custom policies to help you evaluate risks according to the unique needs of your organization.

**Attack Surface Management**
In Expander

## 3. Mitigate

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.

# Additional Benefits

## 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.

## Robust Integration Ecosystem

Expander integrates with the most popular SIEM, SOAR, ITSM, VRM, CSP, and other solutions that are core to your ecosystem. This means 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 toolset.

## Rapid Response to New Security Concerns

Expanse is able to rapidly deploy new policies to monitor for specific Internet-exposed systems and services. When new zero-day exploits and CVEs are announced, Expanse 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.