Expanse Behavior

A complete, outside-in view of the behavior of your perimeter, its responsive assets, and their communications outside your organization

Attackers Will Hide in the Shadows

Most organizations lack complete visibility of what's going into or out of their networks from the Internet. And this lack of visibility provides attackers an easy path into your organization. The sheer number of devices connected to the Internet makes monitoring every network egress point increasingly difficult. Adding to that complexity are cloud infrastructure, remote workers, and devices that don't allow you to install traditional monitoring equipment.

Expanse Behavior solves this visibility gap by looking at the problem from the outside. Using global Internet flow data, Behavior surfaces communications between your Internet-connected assets and others on the Internet. This perspective removes the traditional challenges of traffic monitoring without the need for installation of agents or configuration of monitoring tools. The result is an accurate way to detect and stop risky and out-of-policy communications.

Expanse Behavior Helps You:

Passively uncover suspicious or risky activity to and from assets on your network

Validate whether security and access policies are being followed

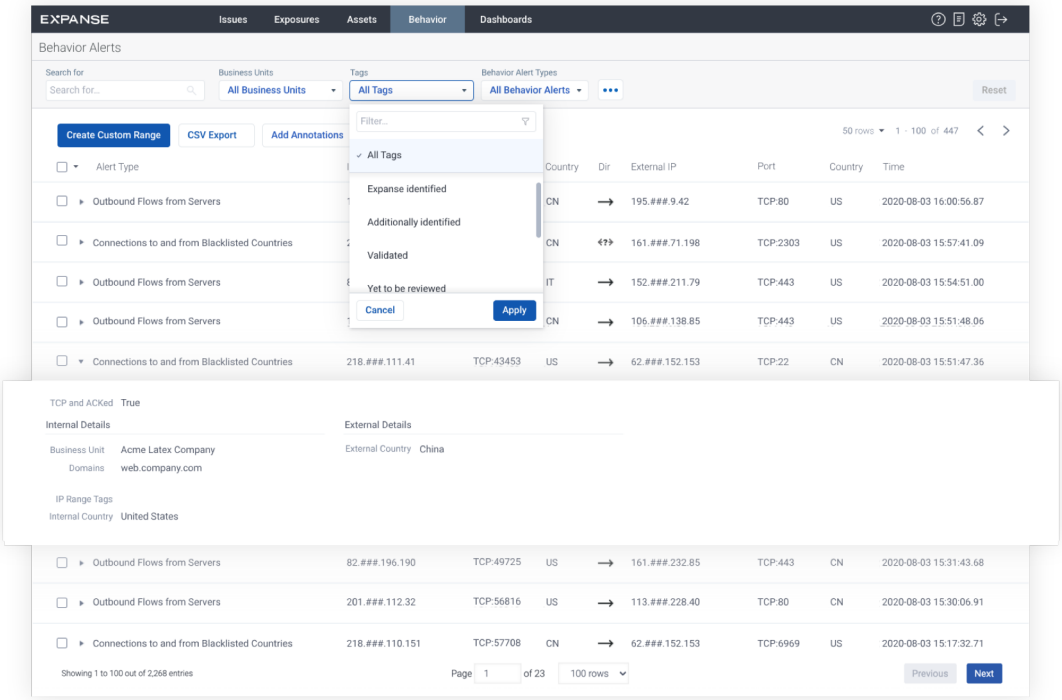
Identify assets communicating with Tor networks, command-and-control servers, and geographies that may be prohibited

Understand Communications Outside Your Perimeter

Historically, in order to understand network and Internet communications, you needed to deploy sensors, gather logs, and install agents on any device that you needed to monitor. While those methods are adequate for monitoring assets that you know about and can install agents on, they don't scale alongside digital transformation trends like BYOD, cloud infrastructure, and IoT devices.

Coupled with your complete Internet-connected asset inventory from Expander, **Behavior** provides global context about communications between those assets and others which may indicate that you have a compromised asset within your organization. The outside-in perspective offered by Expanse products provides insights about both assets and communications that are not be available via traditional monitoring systems.

Gaps in visibility and policy can and will be exploited by an attacker, leading to data breaches, ransomware attacks, or other business-crippling events.



The Solution

Expanse has developed a new way to approach these problems by partnering with global Internet service providers to join observed Internet traffic data associated with your networks with our active sensing data. By unifying these types of data, our platform helps you have a comprehensive view of your assets and what they are talking to. This is a fundamental shift from traditional approaches that rely on humans to scrutinize network traffic wherever local sensors were dropped.

Behavior discovers, tracks, and notifies you of risky and policy-violating activities on your network, all without agents or instrumentation.

Key Use Cases

Behavior detects communications to and from your Internet-connected assets that may indicate policy violations or the potential compromise of an asset, including:

- Connections to risky services like Tor or BitTorrent
- Connections to risky or prohibited geographies or countries, like those prohibited by the OFAC
- Use of problematic, risky, or prohibited software, like P2P sharing applications
- Communications with device types that are commonly compromised or used as command-and-control servers

Behavior delivers contextualized notifications so you can take immediate action and remediate identified issues. Easily see where you may have policy gaps and ensure that changes in your infrastructure and assets are managed in a secure, compliant way.

3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.expanse.co