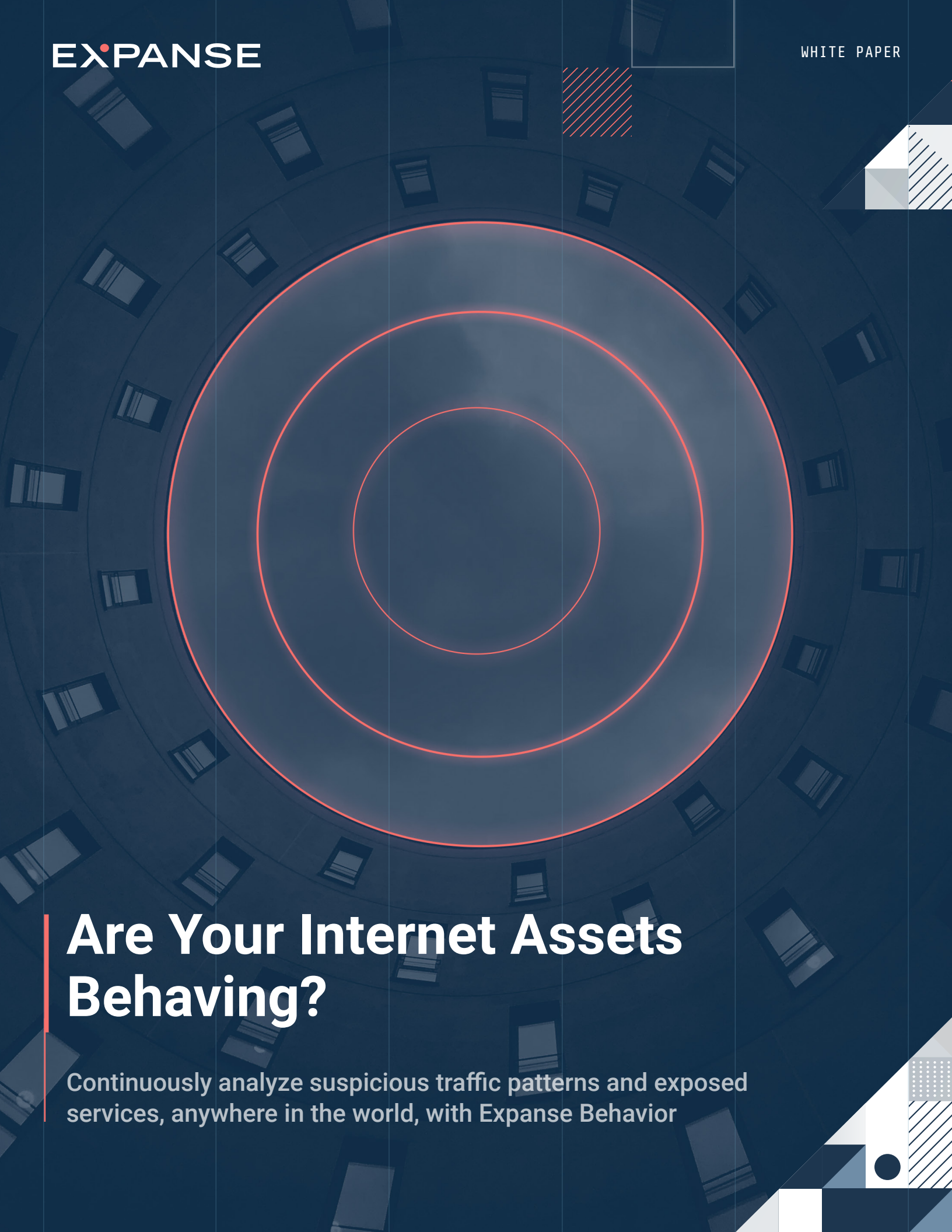
EXPANSE

WHITE PAPER



# Are Your Internet Assets Behaving?

Continuously analyze suspicious traffic patterns and exposed services, anywhere in the world, with Expanse Behavior

## What Is Keeping You From Applying and Enforcing Consistent Security Policies?

Protecting your enterprise requires the consistent application and continuous enforcement of security policies across your entire network. That network might include a large, diverse collection of Internet Assets such as IP addresses, domains, and certificates on-premise, in the cloud, and across the supply chain. You need to ensure that none of your Internet Assets communicate in a way that puts your enterprise at risk.

Your policies should reflect your specific needs and restrict the behaviors that you know could leave your network vulnerable. For example, you might set policies to:

- **Prevent assets from sending or receiving data using specific protocols, such as Server Message Block (SMB) Protocol or File Transfer Protocol (FTP)**
- **Ban the use of Remote Desktop Protocol (RDP) servers for employee remote access**
- **Refuse traffic to and from prohibited vendors (such as Kaspersky) or countries (such as those banned by the government)**
- **Prohibit cryptocurrency mining, peer-to-peer (P2P) sharing applications (such as BitTorrent), or anonymity services (such as Tor)**
- **Block known command-and-control traffic and communications with device types that are commonly compromised**

Making sure that policies are applied and enforced as they should be across your entire network can be difficult, especially since networks change on a daily or even hourly basis, with new Internet Assets being created by local teams that are not necessarily known to central IT and security organizations. These continuous changes mean very few large enterprises have a complete and centralized inventory of all of their digital infrastructure, including all Internet Assets. In addition, many also have no processes for discovering or continuously updating their Internet Asset inventory to account for mergers, acquisitions, or other business changes that can alter the enterprise network.

Enterprises have tried to adapt to constant network change by acquiring tool after tool in an attempt to maintain compliance across all Internet Assets. Some of the tools are vendor-specific, while others are from legacy vendors that have not adapted to the scale and velocity of enterprise growth. The reality is that, despite record spending on tools of every type, the problem persists. The modern enterprise requires a platform that moves as fast as the business, and a way to monitor communications across a heterogeneous network to make sure Internet Assets are adhering to policies and reducing potential risks.

### Behavior Helps a Global Bank Comply With Strict Government Regulations

Banks and other financial services organizations must diligently monitor Internet traffic to ensure they are complying with sanction requirements from the U.S. Office of Foreign Assets Control (OFAC).

Security professionals at one large bank thought they were successfully blocking all outbound traffic to OFAC-prohibited countries. But after implementing Expanse Behavior, the team learned that some traffic matched the profile for communications with Iran — a country sanctioned by the United States. After a subsequent internal investigation, the team discovered that not all corporate firewalls were configured correctly.

The team used the insight from Behavior to close the gap, applying policies more consistently across the network and preventing compliance issues going forward.

## Gain Clear Visibility Into Internet Communications

Expanse Behavior™ automatically identifies risky connections to and from your Internet Assets so you can maintain consistent policies across your network. Providing a complete, outside-in view of Internet Asset communications, Behavior gives you the insights you need to determine whether or not policies are being followed — all without requiring any software deployment or configuration.

### Know Your Unknowns With the Expanse Internet Operations Management Platform

The Expanse Internet Operations Management Platform continuously indexes the entire public Internet, producing over one petabyte a day of data about all Internet-accessible systems and services, including detailed information about the software configurations and risky communications of every connected asset. Fusing together this planetary-scale data allows the Expanse Internet Operations Management Platform to determine which Internet Assets are owned by your enterprise and create a single, comprehensive system of record of those assets. This system of record is continuously updated, capturing information about all Internet Assets on your quickly changing global networks. This means you get visibility into any potential exposures as they happen, anywhere in the world.

### Scrutinize Suspicious Communication Activity

Once you have a complete, current, and accurate inventory of all of your Internet Assets, the next step is to monitor those assets for suspicious or risky communications activities. Behavior analyzes traffic to and from your inventory of Internet Assets, using samples from 90% of the world's Internet traffic in partnership with global Internet service providers.

These sampled data (netflow) provide information on communications — including source, destination, and port information — without transmitting the content of those communications.

By applying out-of-the-box and custom filters to netflow data, Behavior identifies communications that violate your enterprise policies. For example, Behavior might discover:

- **Outbound web connections are not flowing through a secure web gateway (SWG), in violation of your company policy**
- **Not all inbound communications are flowing through a web application firewall (WAF), as you require**

Insights and alerts about policy violations from Behavior can be leveraged in several ways. For example, the Expanse Technical Add-on for Splunk sends information directly to Splunk from Behavior or Expander. Similarly, the Behavior API integrates information from Behavior into other security and asset management tools. Or you can use the Expanse web interface to view policy violations surfaced by Behavior or generate time-based email alerts.

With insights from Behavior, it's possible to check network logs and pinpoint the Internet Assets that are causing problems so that you can remediate issues and achieve the consistent application of policies across your network.

## A Comprehensive, Continuously Updated, Outside-in Perspective

Behavior provides deep, comprehensive visibility into Internet Asset communications by monitoring traffic from the outside in. Capitalizing on Expanse's extensive Internet service provider partnerships, Behavior collects and analyzes a full range of communications flowing into and out of your network, including networks where local sensors may not be deployed. In contrast, on-premise network monitoring solutions and manual, in-house processes are unable to track all of your asset communications beyond your perimeter.

**Behavior provides a comprehensive view into how your network is communicating and alerts you when Internet Assets are violating your security policies.**

The outside-in approach simplifies administration. With Behavior, there is no system that you need to deploy, configure, or manage internally. You gain unparalleled insight without adding complexity.

## Conclusion

As your network continues to evolve, it will become increasingly difficult to track all of your Internet Assets, monitor their behavior, and make sure they are adhering to your security policies. Behavior provides a comprehensive view into how your network is communicating and alerts you when Internet Assets are violating your security policies. With new insights into the behavior of Internet Assets, you can remediate problems and ensure all of your network devices are working together to protect your business.

## Ready to Learn More?

Visit Expanse.co to learn more about Expanse Behavior and set up a demo.





WP_Behavior_102_EN