REDSEAL

Keeping an eye on IPv6 in your hybrid network

The IPv6 wave is here. Are you ready?

With the proliferation of connected devices, organizations everywhere are making the transition to Internet Protocol version 6 (IPv6). For some, it's a strategically planned, even mandated, migration from IPv4. But for most, the unplanned growth of IPv6 infrastructure in their networks is a long-anticipated problem that has finally come home to roost.

Cloud adoption—whether sanctioned or through shadow IT—has fueled IPv6 use, and unexpected IPv6 connectivity is now pervasive. IPv6 has crept into hybrid networks, creating unintended access points and pathways rife with risk. In the worst cases, differences between old IPv4 and new IPv6 fabric result in firewall bypasses that go unnoticed until a breach occurs.

The pressure is now on to get an eye on all things IPv6 in your network.

Reduce risk with RedSeal

RedSeal is a network exposure analytics platform that identifies business assets in a hybrid network that are exposed to risks and delivers the contextual information needed to manage those risks efficiently. Without installing agents, RedSeal collects and analyzes data from disparate network infrastructure—from on-premises firewalls, switches, and vulnerability scanners to private and public cloud resources—to build a complete network model with all devices, connections, and exposure points identified. These can be IPv4 or IPv6, previously known or unknown.

RedSeal helps answer critical questions about IPV6 in your network:

- Where and how is IPv6 being used in my network?
- What percentage of my total network assets are in IPv6-only environments?
- Which specific devices need to be upgraded to IPv6?
- Has my IPv6 migration created gaps in my network security?
- How do I verify the security controls put in place for my IPv6 network?

For IPv6, its powerful inventory and attack path mapping capabilities patrol your network, looking for all kinds of defensive gaps, including unexpected or unplanned growth of IPv6 infrastructure. RedSeal maps your network, identifies IPv6 resources, and then thinks like an attacker and finds whatever pathways have been left open, now including IPv6 pathways.

IPv6 intelligence for your network

RedSeal delivers the network context you need to answer critical questions about IPv6 in your network, from big-picture assessments to detailed queries.

Gain comprehensive visibility
Get a detailed inventory of all IPv4 and IPv6 connected assets, along with a vendor-agnostic visualization of IPv4/IPv6 interfaces in one connected model.

Reveal vulnerable attack paths
Run detailed path queries to understand potential traffic flows through IPv6 subnets. A hop-by-hop analysis provides detailed insights into possible attack paths and reveals potential firewall bypasses.

Mitigate security and compliance risks
As IPv6 spreads across your network, verify that a protocol change won't result in unintended access or risk. Easily pinpoint devices in which discrepancies have come up during an IPv6 rollout to ensure compliance with IPv6 adoption mandates and timelines.

To support our customers at every phase of IPv6 adoption, RedSeal will maintain support for IPv4 and continue to expand support for IPv6—from foundational visibility and attack path analysis to risk prioritization. Currently, RedSeal integrates with 125+ networking and security products to deliver the most comprehensive and accurate model of your network, and we are working to add IPv6 support to each plugin in priority order.

Contact us for more details about license requirements and supported devices.

Learn more

For more information about how RedSeal can help you minimize risk and maximize resilience in your IPv6 and dual-stack networks, **schedule a demo** with one of our product experts today.

redseal.net | info@redseal.net | +1 408-641-2200 | 888-845-8169