

CHECK POINT + REDSEAL

APPLIED SECURE SEGMENTATION

Benefits

- Prevents unintended access
- Enables operational resilience
- Enables real-time, proactive protection
- Lowers incident response costs
- Continuous visibility across layers
- Understand your overall network security health and resilience

INSIGHTS

Network breaches aren't new, they've occurred for years – for sport, for profit, for ideology. But what has changed is businesses' reliance on their networks, the visibility and sophistication of breaches, and the level of management accountability. More is at stake.

Perimeter protection is no longer enough to protect the enterprise efficiently. Motivated attackers can use physical access, social engineering, compromises within the hardware and software supply chains or zero-day exploits to eventually breach corporate defensive mechanisms. Internal security controls are needed to provide visibility and protection over interactions within the enterprise network.

Compartmentalization is critical for the survival of an organization under attack. RedSeal and Check Point have partnered to implement network segmentation as a solution to provide organizations with access and agility while maintaining protection for their critical assets.

MODEL, TEST, PRIORITIZE, REMEDIATE WITH REDSEAL

RedSeal's advanced analytics engine creates functioning network **models**, **tests** networks to identify security risks, **prioritizes** needed actions, and provides critical information to quickly **remediate** issues.

As your network evolves RedSeal certifies you are secure by examining devices, scanner data, and vulnerability databases. We build an accurate model of your network through analysis of security rules, Access Control Lists (ACLs), and Network Address Translation (NAT) tables. Every allowed access path through the network is calculated to ensure that policies are operating as intended and networks are segmented securely. We prioritize the actions you need and provide you with information needed to quickly remediate issues. The result is reduced cybersecurity risk and lower incident response and maintenance costs.

DESIGN A SECURE ARCHITECTURE WITH CHECK POINT

In a world with evolving infrastructures, where perimeters are no longer well defined, and where threats grow more intelligent every day, we need to define the right way to protect enterprises. Software-Defined Protection (SDP) offers an infrastructure that is modular, agile and most importantly, SECURE.

Our architecture protects organizations of all sizes at any location: headquarters networks, branch offices, roaming through smartphones or mobile devices, or when using cloud environments. Protections must automatically adapt to the threat landscape without the need for security administrators to follow up manually on thousands of advisories and recommendations. These protections must integrate seamlessly into the larger IT environment, and the architecture must provide a defensive posture that collaboratively leverages both internal and external intelligent sources.

Software-Defined Protection partitions the security infrastructure into three interconnected layers:

- The Enforcement Layer Inspects traffic and enforces protection in well-defined segments
- The Control Layer Delivers real-time protections to the enforcement points
- The Management Layer integrates security with business process

The main principle behind the Enforcement Layer is segmentation. Segmentation is critical for the survival of an organization under attack because each attack that targets a single component of the network should not be able to undermine the entire enterprise security infrastructure. The role of segmentation in the SDP architecture is to prevent an attack from proliferating within the network, as well as to allow only authorized traffic to flow, according to the enterprise business processes

AN APPLIED, SECURE ENTERPRISE INFRASTRUCTURE

Security professionals can secure modern enterprise networks as they evolve while addressing necessary threat prevention by segmenting the network following the Check Point SDP architecture and using RedSeal to model and test this network design. RedSeal and Check Point enable business agility and continuous security posture assessment even as your organization evolves — whether through mergers or acquisitions, consolidation, outreach to partners and customers, or the addition of new applications and services.

The integration of RedSeal and Check Point provides an applied segmentation design through continued testing and remediation to ensure that your evolving network remains secure in the face of today's sophisticated attacks. By committing to segmentation programs, enterprises can vastly improve their ability to have a resilient design that mitigates network breaches before they become a data or property breach statistic.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyber-attacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

ABOUT REDSEAL

RedSeal provides a cybersecurity analytics platform to Global 2000 organizations that certifies their evolving networks are secure and accelerates compliance initiatives. RedSeal's advanced analytics engine creates functioning network models, tests networks to identify security risks, prioritizes needed actions, and provides critical information to quickly remediate issues. The result: reduced cybersecurity risk and lower incident response and maintenance costs. With operations in North America, Europe, and Asia, RedSeal customers include leaders in finance, retail, technology, utilities, service providers, and government, all served by RedSeal's channel partner network. Visit us at redseal.co

CONTACT US

RedSeal | 940 Stewart Drive, Sunnyvale, CA 94085 | Tel: 1 888 845 8169; 1 408 641 2200 | EMEA Tel: +44 20 7849 3020 | Email: info@redseal.co

Check Point World Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

Check Point U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233