

The Challenge of SSL Decryption in Network Security

At its core, the role of a firewall is to segment and manage network traffic. By decrypting network traffic, organizations gain increased visibility, enabling security and networking teams to take informed actions such as blocking or filtering harmful traffic. However, the challenges of implementation, combined with the concerns over privacy and technical hurdles, make SSL decryption a sophisticated yet essential component of modern network security.

Common Challenges

Operational Constraints: Implementing SSL decryption is resource-intensive, consuming substantial memory on already resource-constrained firewalls. This often leads to operational bottlenecks, hindering the effectiveness and responsiveness of network security measures.

Privacy Concerns: While SSL decryption enhances security by allowing network teams to see and manage all traffic, it also raises privacy concerns. Business units frequently perceive this capability as invasive, leading to internal conflicts about the extent of monitoring. This tension between security enhancement and privacy expectations creates a delicate balance that organizations must navigate.

Technical Complexities: For security teams eager to implement SSL decryption, the technical challenges are significant. Determining which categories of traffic to decrypt and understanding the flow of this traffic within the organization can be daunting. Without clear insights into traffic categories and attacker behavior, effectively prioritizing decryption efforts becomes a complex task. Additionally, managing certificates for users targeted for SSL decryption adds another layer of complexity. Starting with a small group of risky users is a practical approach, as it allows for better control and oversight over certificate management while assessing the impact and effectiveness of decryption measures.

Solving the Challenge is within Reach

Reach implements a strategic approach to SSL decryption, enhancing network visibility and security by intelligently analyzing encrypted traffic. By prioritizing decryption for high-risk traffic and streamlining the deployment process, Reach ensures that network defenses are both effective and efficient. This method not only improves the detection and management of potential threats but also aligns with privacy and operational requirements, making it an indispensable tool for modern cybersecurity needs.

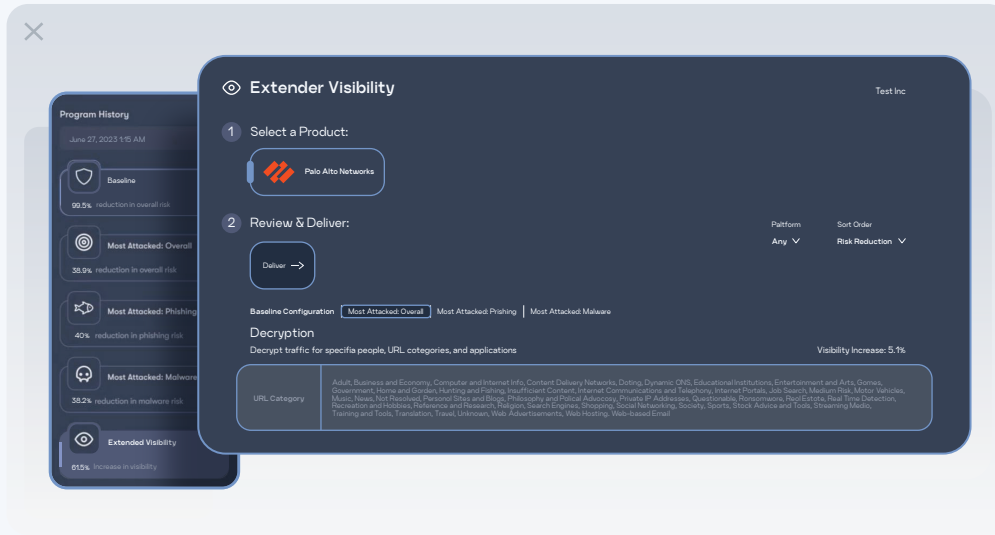
Drive Outcomes with Reach

Who to Decrypt: Reach provides a staggered approach to SSL decryption by identifying the minority of users that account for the majority of the risk. This helps to prioritize the rollout of SSL decryption.

What to Decrypt: Utilizing security and event data from across the security estate, Reach identifies key threats and informs which categories of traffic to decrypt, enhancing the effectiveness of firewall content filtering and ensuring that risky URL categories are addressed.

How to Decrypt: Reach provides configurators and detailed deployment guides, streamlining the rollout of SSL decryption and reducing the complexity and time required for implementation.

reach.security/connect
415.828.7475
sales@reach.security



Reach Capability

Description

Dynamic User Risk Profiling



Reach continuously updates and profiles users based on their exposure to attacks, applying these profiles to prioritize SSL decryption for users who are most frequently targeted by cyber threats.

Threat Analysis & Categorization



Utilizing advanced analytics, Reach examines security data from integrated products to categorize and prioritize traffic types for decryption, based on the prevalence and severity of incoming threats.

Automated Policy Configuration



Reach automates the configuration of SSL decryption settings on firewalls, guided by its analysis. It includes tools and templates that simplify the application of tailored decryption rules to enhance network security.

Get Started!



To join the community of customers enjoying the benefits of Reach and learn more about how it can transform your security posture, visit

Reach.Security/try-reach

Reach Security is revolutionizing the cybersecurity landscape by empowering organizations to maximize the ROI of their existing security products. With a focus on optimizing what organizations already own rather than adding complexity with new tools, Reach Security is committed to simplifying cybersecurity, reducing operational costs, and enhancing protection against evolving threats. Founded by cybersecurity experts with venture-backing from leading investors and cybersecurity luminaries, Reach Security is setting a new standard for cybersecurity efficiency and effectiveness. For more information, visit: **Reach.Security**.

reach.security/connect
415.828.7475
sales@reach.security