CONCEAL

WHITEPAPER

Unpacking the Two Stack Problem

How Organizations Can Optimize Their Resources by Understanding and Consolidating Their Connectivity and SSE Stacks

CONCEAL

WHITEPAPER

Unpacking the Two Stack Problem

How Organizations Can Optimize Their Resources by Understanding and Consolidating Their Connectivity and SSE Stacks

INTRODUCTION

Enterprises today are under constant pressure to ensure seamless, secure access for employees, contractors, and partners operating from anywhere. In pursuit of this, most organizations have built their digital foundations around two distinct but interconnected domains: a connectivity stack and a security stack. The connectivity stack is responsible for enabling users to reach the applications and data they need by leveraging tools like VPNs, SD-WAN, firewalls, and virtual desktops. The security stack, typically composed of SSE or SASE components such as secure web gateways, CASB, ZTNA, and DLP, ensures that connections remain trusted and compliant. While both are essential, their separate evolution has created duplication, inefficiency, and friction. This is the essence of what we call the Two Stack Problem.

This whitepaper explores the nature of this problem, the costs and trade-offs it imposes, and the growing alternatives available to modern IT and security teams. We will examine the steps organizations can take to transition from two separate stacks to a unified model, as well as the measurable benefits of doing so. Finally, we will introduce the Conceal Browser-Native SSE platform, designed to merge connectivity and security into a single, efficient, and inherently zero-trust model.

CONCEAL

WHITEPAPER

Unpacking the Two Stack Problem

How Organizations Can Optimize Their Resources by Understanding and Consolidating Their Connectivity and SSE Stacks

1. WHAT IS THE TWO STACK PROBLEM

The Two Stack Problem arises from the historical separation of connectivity and security functions within enterprise networks. Connectivity tools like VPNs and SD-WANs were initially designed to ensure reliable user access to corporate resources. In contrast, security tools like SWGs, CASB, and ZTNA were built to inspect, control, and protect that access. Over time, both layers have grown more complex and feature-rich, but in doing so, they have begun to overlap. Each maintains its own agents, policies, and management consoles, leading to operational redundancy and increased risk. This duplication creates longer traffic paths, higher latency, and multiple points of failure. For instance, a remote user connecting to a private app through a VPN and then being inspected by a separate proxy may experience performance degradation and inconsistent policy enforcement. The result is architecture that is both expensive to maintain and challenging to secure end-to-end.

More importantly, this separation introduces blind spots. Because the two stacks are unaware of each other's full context, a malicious action within a browser session or a compromised credential may pass unnoticed until after a breach occurs. In short, while each stack performs well individually, their coexistence often undermines the very goals of Zero Trust—contextual awareness and continuous validation.

2. PROS AND CONS OF MAINTAINING SEPARATE CONNECTIVITY AND SSE STACKS

For years, many enterprises have accepted the coexistence of two separate stacks as a practical necessity. There are undeniable benefits to this model. Specialized tools can deliver deep capabilities in their respective domains, such as high-performance routing in SD-WAN, granular inspection in SSE platforms, and precise control in dedicated firewalls. This separation also allows IT and security teams to select best-of-breed vendors and independently evolve from each stack over time.

However, the disadvantages increasingly outweigh the advantages. Separate stacks require multiple deployment workflows, agent installations, and overlapping maintenance. This not only increases the operational burden but also inflates costs through redundant licensing and infrastructure. Performance is another casualty; when traffic must travel through multiple inspection points, often across vendor-operated data centers, it introduces latency and potential service interruptions. Furthermore, fragmented visibility makes it difficult to enforce uniform Zero Trust policies, and incident response often involves multiple teams working across disconnected systems. In short, while specialization has its virtues, fragmentation has become a costly obstacle to agility and efficiency.

3. ALTERNATIVES TO MAINTAINING SEPARATE STACKS

The industry has begun to respond to the Two Stack Problem by converging connectivity and security capabilities into unified frameworks. Cloud-native SASE platforms were the first step in this direction, combining SD-WAN and SSE into a single cloud-delivered model. While this reduces architectural sprawl, it still relies heavily on vendor-operated data centers and proxy-based routing, creating new dependencies and potential points of latency.

Another response has been the rise of secure enterprise browsers, which embed security controls directly into the browsing experience. However, these typically require users to abandon their preferred browsers and adopt a proprietary one, which is a challenge in environments with diverse user preferences or strict application compatibility requirements.

A newer, more seamless approach is the Browser-Native SSE model. Rather than routing traffic through distant inspection nodes or enforcing the use of a specific browser, this model delivers connectivity and security directly within the user's existing browser. It combines the key elements of ZTNA, DLP, and advanced threat detection at the point of interaction, which eliminates the inefficiencies of legacy architectures while maintaining a native user experience.

4. HOW TO GO FROM TWO STACKS TO A CONSOLIDATED STACK

Transitioning from dual-stack complexity to a consolidated architecture begins with an honest assessment of your current environment. Organizations should start by mapping all existing connectivity and security components, noting areas where functionality overlaps. Common redundancies often include access control enforcement, traffic routing, and content inspection, which may be handled by both connectivity and security tools today.

Once these overlaps are identified, it becomes easier to define a target state aligned with Zero Trust principles. This target state focuses on direct, identity-based connections to applications without the need for intermediaries. Pilot programs are an effective way to test consolidated solutions in controlled environments, such as replacing VPN and SWG functions for specific user groups. Metrics such as latency, user satisfaction, and incident response time provide valuable insight into the benefits and potential challenges of a broader rollout.

As the organization gains confidence, it can gradually decommission redundant systems and consolidate management under a unified platform. This process not only reduces infrastructure but also streamlines policy administration, creating a more agile and secure operating model.

5. EXPECTED BENEFITS OF MAKING THE CHANGE

The advantages of consolidating connectivity and security stacks are both immediate and long-term. From a financial perspective, organizations can significantly reduce costs by eliminating redundant licenses, maintenance contracts, and hardware appliances. Operationally, a single management plane means fewer agents to deploy and maintain, and a unified policy framework ensures consistent enforcement across all users and devices.

Performance improvements are equally notable. By removing unnecessary proxy hops and data center detours, users experience faster connections and fewer disruptions. Security is also enhanced; when enforcement occurs at the browser level, visibility extends to the most common attack surface where modern phishing, credential theft, and malicious code execution typically happen.

Ultimately, consolidation drives simplicity. IT and security teams can shift focus from managing infrastructure to enabling productivity, while end users benefit from a seamless experience that doesn’t require extra logins or client installations.

Unpacking the Two Stack Problem

How Organizations Can Optimize Their Resources by Understanding and Consolidating Their Connectivity and SSE Stacks

CONCLUSION: THE CONCEAL BROWSER-NATIVE SSE PLATFORM

No VPN. No Proxy. No VDI. No Data Center.
Just the security you want, whenever and wherever you need it.

The Conceal Browser-Native SSE platform represents a fundamental rethinking of how secure connectivity should be delivered. Instead of relying on proxies, VPNs, or dedicated enterprise browsers, Conceal provides a lightweight, in-browser solution that unifies Zero Trust access and real-time threat protection within a single framework. By operating natively within the browser, Conceal eliminates the need for traffic redirection, ensuring line-speed performance while continuously enforcing security policies.

Conceal connects users directly to SaaS, web-based, or private applications intermediaries. Its unique ability to analyze and act on browser activity at the Document Object Model (DOM) level allows it to stop malicious actions before they cause harm. Integrated data loss prevention ensures sensitive information stays protected, while seamless interoperability with identity providers and SIEM/XDR/SOAR solutions makes Conceal easy to deploy and manage.

The result is a consolidated platform that simplifies IT operations, enhances user experience, and reduces the total cost of ownership. For organizations ready to eliminate the inefficiencies of the Two Stack Problem and achieve Zero Trust at line speed, Conceal offers a clear, practical path forward.

Schedule a personalized demonstration today at https://conceal.io/demo and experience how Browser-Native SSE can transform your approach to security and connectivity.