Enterprise Strategy Group™ by TechTarget

WHITE PAPER

Future-proofing Your Proxy Architecture

By John Grady, Principal Analyst
Enterprise Strategy Group

August 2023

Contents

Executive Summary 3
The Evolution of the Web Proxy 3
The Shift to SASE and Its Impact on Proxies 4
Requirements for Web Proxies as Part of a Consolidated Platform 5
Conclusion 6

Executive Summary

Over the last two decades, web proxies have become a staple of the security stack for many organizations. Proxies do offer benefits, especially in certain scenarios where companies face specific compliance requirements. Yet many maintain their proxy simply because they have invested significant time and effort into building their security architecture around them. Regardless of the reason, many organizations will maintain a web proxy for at least the next few years.

Those that start their planning early and begin to migrate to consolidated platforms that can support a proxy architecture in the short and moderate term, as well as a broader SASE initiative over time, will enjoy consistent, integrated security; improved operational efficiency; and better user experiences.

However, enterprise environments have fundamentally changed, and every organization needs to begin planning for security convergence and how to continue to shift more controls to the cloud. This concept of secure access service edge (SASE) is sometimes oversimplified and broadly applied. It will be a longer-term process, especially among enterprise companies, and some organizations might choose not to pursue SASE initiatives. But those that start their planning early and begin to migrate to consolidated platforms that can support a proxy architecture in the short and moderate term, as well as a broader SASE initiative over time, will enjoy consistent, integrated security; improved operational efficiency; and better end-user experiences.

The Evolution of the Web Proxy

Web proxies were originally introduced primarily to help large organizations improve the performance and security of their internet connections. Proxies were used to cache frequently accessed web pages and protect individual machines by serving as an intermediary for web requests. Over time, security teams added more protective capabilities such as antimalware, sandboxing, and data loss prevention (DLP) to create secure web gateways (SWGs). Often, these capabilities were stitched together from a variety of vendors integrated via protocols such as the Internet Content Adaptation Protocol (ICAP).

Along the way, cloud proxies were introduced to support direct internet breakouts from branch offices, yet many organizations have retained their on-premises proxies for larger office locations. Today, many organizations continue to use a mix of on-premises and cloud web proxies as core components of their security stack. Some of the most common reasons for this include:

- **Supporting no default route architectures.** Security teams might not want workloads and applications communicating with the internet, except for in certain circumstances such as downloading OS updates or patches. Proxies can be used to ensure these systems do not have direct, unfettered access to the internet and instead are routed through an explicit proxy.
- **Supporting compliance requirements.** Some organizations operate under compliance requirements, with a web proxy serving as a core security tool. While the NIST 800-53 guidelines for security and privacy controls concern government organizations, regulated industries such as financial services and energy have adopted them as well.
- **Expected migration difficulties.** While some organizations continue to use a web proxy because they feel it provides the best security or helps them maintain compliance, others do so because changing their security strategy is too complex. Years of configuration and policies that have accumulated make it difficult for security teams to evaluate and understand what is important and what is outdated. Migration projects can seem overwhelming and can make continuing the status quo seem like the better option compared to rearchitecting

the network, at least in theory. Even when security teams migrate data from on premises to the cloud, they are often migrating existing cumbersome policies.

Yet there are notable drawbacks to these types of fragmented proxy deployments. To start, many organizations have bolted security capabilities from multiple vendors onto their core web proxies. Rather than fully reconfiguring their network architectures, some organizations connect on-premises and cloud services together via ICAP for advanced malware protection and DLP, as well as proxy chaining for remote browser isolation that might not be available or desired from the incumbent vendor.

While somewhat simple in the short term, ICAP adds unnecessary complexity from a management perspective. Navigating multiple consoles to create security policies is inefficient. Further, when aspects of a policy are duplicative across different services, the potential for human error can increase, creating a gap in the organization's security posture. With many vendors having added advanced features over time, such as their own sandboxing and DLP capabilities, the value of ICAP has deteriorated and has little relevance for today's SWG.

Additionally, legacy proxy architectures can impact the user experience. Having to backhaul traffic from remote users to a central on-premises proxy solution can result in latency issues. Any time the user has to navigate to the internet or applications differently based on where they are, there is the potential for frustration and for productivity to be impacted. Caching is a technique that helps in reducing bandwidth usage and was a relevant feature in the early days of the web. But with today's web traffic primarily consisting of dynamic content with more than 90% of the traffic being encrypted with the use of HTTPS, the value of caching has diminished. With liability issues and with alternatives like traffic prioritization available, the use of web caching is not relevant in today's proxy discussion.

Ultimately, those companies that have relied on web proxies have invested a significant amount of time and resources refining the routing paths and security policies around these controls. This has made it difficult for organizations to contemplate migrating to a proxyless security architecture.

The Shift to SASE and Its Impact on Proxies

As organizations have become more distributed, the need for consistent, location-agnostic security has only increased. Employees are increasingly remote, and the resources they rely on to do their jobs are often cloud-resident. Specifically, research from TechTarget's Enterprise Strategy Group has found that 63% of employees currently work in a remote or hybrid manner.[1]

As a result, many organizations are beginning to plan for and implement converged cloud-centric architectures. Specifically, SASE and security service edge provide a unified architecture to secure user access to private applications, public applications, and the internet. Some of the most common drivers of interest in SASE include:

- **Improving security effectiveness (43%).** The traditional approach of adding new tools to defend against emerging threats and protect new parts of the environment has reached a point of diminishing returns. It is incredibly difficult to properly configure and manage so many tools, opening the organization to unnecessary risk.
- **Simplifying infrastructure and processes (32%).** Cloud-delivered, as-a-service models are desirable because they relieve security and network teams of infrastructure management responsibilities. Not all organizations are ready to fully migrate to the cloud, but a unified hybrid architecture can help bridge the gap.
- **Delivering better employee experiences (29%).** Security teams are increasingly judged not only on their ability to protect corporate users and resources, but also on whether they enable the business to be more

[1] Source: Enterprise Strategy Group Research Report, *SASE Trends*, December 2021. All research references and charts in this white paper are from this research report.

productive and agile. A large part of this is ensuring that users have access to the resources necessary to do their job with as little friction, interruption, or impact to performance as possible.

However, while many organizations will ultimately move toward a SASE architecture, not all will migrate at the same pace. Enterprise organizations, especially, will be thoughtful and diligent in their planning and adoption of SASE solutions for a variety of reasons—including that enterprise environments are more complex with a variety of locations and services, there are more individual security tools in use (many of which have been patched together over time), and those existing controls often necessitate specific network architectures and routing paths (such as web proxies) that can make migration difficult.

That said, even organizations that do not plan to migrate toward SASE in the short term can benefit from beginning to think about how consolidated platforms that provide the flexibility to support short-term requirements, as well as a longer-term path toward a SASE architecture, can help their organization.

While a SASE architecture will ultimately serve a number of use cases, more than one-third (34%) of survey respondents said SWGs are a starting point for SASE, with an additional 35% noting that SWGs are a secondary consideration for SASE. This makes it critical for organizations using web proxies to begin planning for how they will migrate toward a SASE implementation that supports their architecture both now and in the future.

Requirements for Web Proxies as Part of a Consolidated Platform

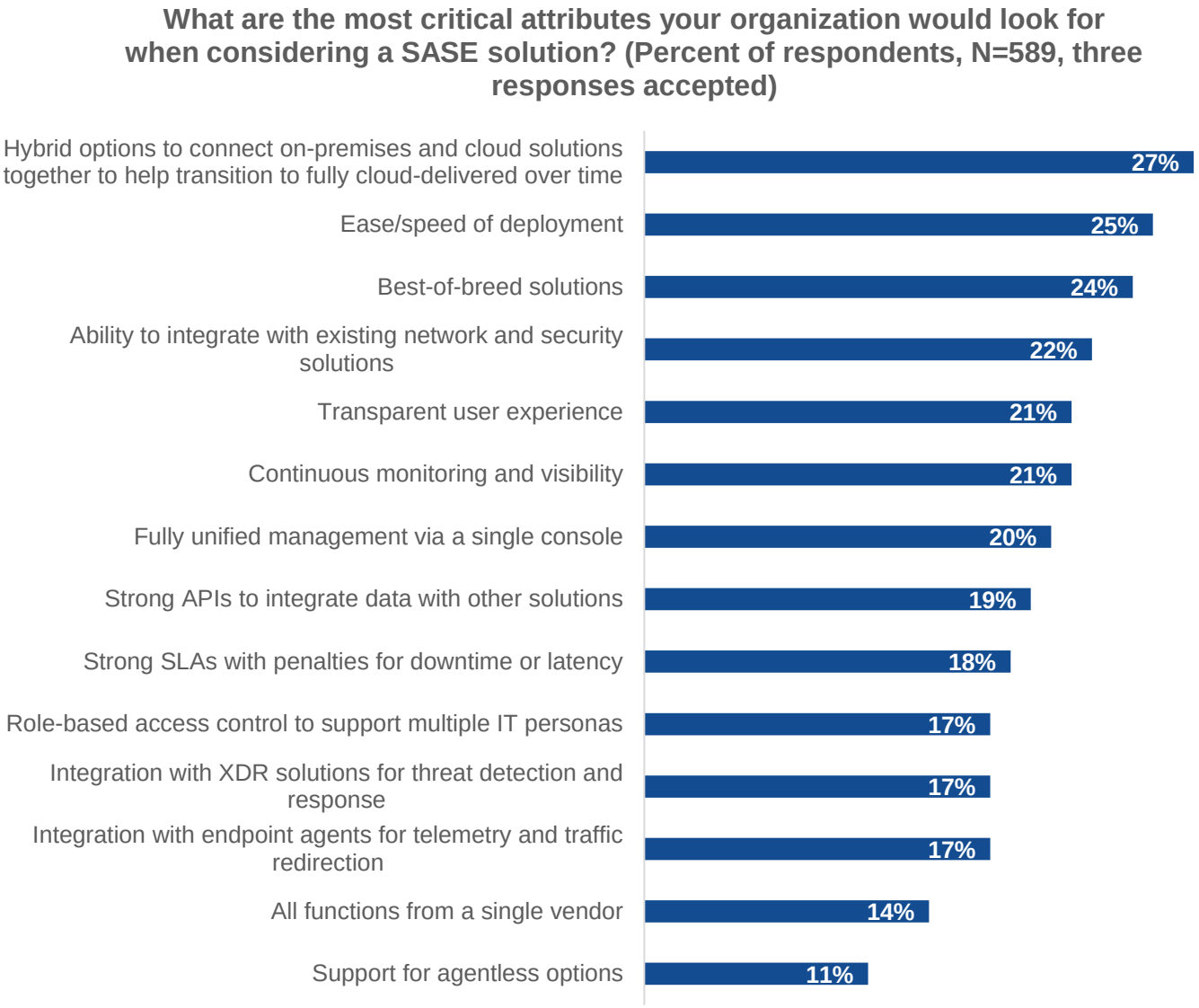
As security teams begin to think about the type of architecture they will support in the future and how to begin to bridge the gap over the short and moderate term, a few capabilities stand out. Obviously, any consolidated platform must have core proxy capabilities. It must support explicit proxy deployments where no default routes are required, along with transparent proxy deployments to support user and device traffic regardless of where they are located—which could be on premises at either a headquarters office or data center, or a remote office. Further, consolidated platforms should provide flexible authentication methods to help organizations that plan to modernize their identity stack over time. For example, while the Kerberos protocol might be currently used on premises, SAML support will be necessary if the organization moves to a cloud identity provider in the future.

Beyond specific proxy functionality, the list of critical attributes for SASE solutions begins to shed light on other important aspects of what a modern consolidated platform supporting a web proxy should include (see Figure 1). Some of the most commonly cited critical attributes are:

- **Hybrid options.** As noted, few, if any, enterprises will fully migrate to the cloud overnight, with most retaining a combination of on-premises and cloud-delivered security tools. Platforms that provide consistent web proxy capabilities on premises and in the cloud can help security teams navigate this transition at their own pace.
- **Ease/speed of deployment.** Security teams have expended time and energy building their networks to support web proxies. Consolidated platforms that provide proxy capabilities, easily plug into existing architectures, and offer simple policy migration from existing proxies make the transition from legacy solutions much simpler.
- **Best-of-breed security.** No organization is willing to sacrifice effectiveness for efficiency. A proven track record for defending the largest organizations from the most sophisticated threats and a history of security detection innovation are critical aspects of a consolidated network security platform.
- **A seamless user experience.** As mentioned earlier, a core goal of security modernization is providing consistency for users regardless of where they are. Access to corporate resources should be the same whether users are in the office or working remotely, and the security protections they enjoy must be consistently applied at the same time. A consolidated platform is the only way to achieve this.

- **Fully unified management.** Finally, these platforms should not just pay lip service to consolidation but should offer true convergence and migration toward a unified console. This includes consolidated management for both next-generation firewall and proxy capabilities, as well as "write once, apply everywhere" security policies.

Figure 1. Critical Attributes for SASE



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Conclusion

Ultimately, security teams currently using web proxies should be seeking flexibility to help them more effectively navigate security modernization. Consolidated platforms supporting web proxies that also pave the way for SASE in the future can bridge the gap between current architectures and what will be needed in future years. Through these platforms, organizations can achieve consistent, integrated security; improved operational efficiency; and better user experiences. With consolidated platforms, organizations will have a simplified roadmap toward proxy replacement at their own pace, with the option of retaining a proxy architecture if they so choose. This flexibility will

help security teams be more agile in responding to unforeseen changes, as well as more effective in enabling the business.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com