WHITE PAPER

SaaS Security Control Plane (SSCP) Covers Security Service Edge (SSE) Blind Spots

The rise of cloud computing and Software-as-a-Service (SaaS) has brought about new challenges in securing enterprise identities, applications, and data. Security service edge (SSE) is a model that has gained popularity as an effective solution to provide visibility and control to security teams as remote work has become more common, and the use of SaaS services has become more prolific in every company. SSE unifies a cloud access security broker (CASB), secure web gateway (SWG), and zero trust network access (ZTNA) to deliver the key capabilities of access control, threat protection, data security, security monitoring, and acceptable use control.

Zero trust security is the foundational capability of SSE that authorizes users to access critical data or resources. It follows a "never trust, always verify" principle, which means that every user and device must be authenticated before accessing a resource or data. This principle is dependent on a key assumption that the company controls the endpoint, network connection, or resource the user is trying to access. However, the reality is that more employees are working remotely on unmanaged devices and using unmanaged SaaS services, and a company's data and critical applications are increasingly beyond the enterprise perimeter. The result is that in many cases, the traditional SSE control points are no longer effective for these applications. Unless the company adopts a block first and approve as needed approach with integration into single sign on (SSO) product, most SaaS applications used in a company can be detected but not governed by SSE solutions.

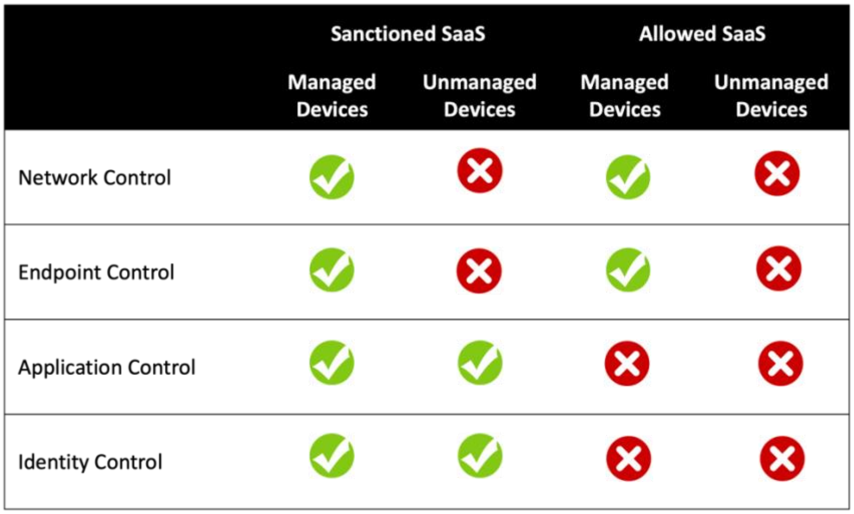
Legitimization of Shadow SaaS Erodes Value of SSE Controls

The explosion of SaaS has fundamentally changed how companies acquire and use technology, and every employee in a company can now find an application and start using it in minutes. They no longer must go through a lengthy purchasing process that requires business justification and a security review. The ease and convenience of being able to use any SaaS application has removed the stigma of shadow IT. Today, it is common for workers to search for an application to use for a project they have and then use that application immediately, often leveraging a free trial. Many companies allow this, creating a category of allowed SaaS, which is essentially shadow SaaS that IT is aware of but is unable govern effectively. The number of applications in this category is far higher than any other SaaS category and accounts for 90% of SaaS used in a company. Many applications have little security risk, but many do store and process sensitive, confidential, or regulated data that should fall under the governance of the company's risk and compliance program.

The reduced ability to govern the hundreds of allowed SaaS stems from the erosion of the security value of SSE control points. SSE relies on a key assumption that does not apply to most of the Internet SaaS applications that are used by employees. The assumption is that a company has control over the endpoint, network connection, or application and requires identity control to verify the user. However, with allowed SaaS, the company only controls the endpoint or network access but does not control the authentication, which means access control cannot be based on the zero trust framework. If the employee is using an unmanaged device, the company does not have any security controls that it can apply.

The table below highlights where SSE controls are effective, and where they are insufficient for comprehensive SaaS security. Some of the control points that are ineffective could be improved by implementing strict rules such as putting everything into an SSO application and not allowing access from unmanaged devices for sanctioned SaaS. The company could also enforce the policy that workers are not allowed to use any SaaS that is not officially sanctioned. However, these overly strict rules often have the effect of reducing productivity and are unrealistic due to licensing costs.

Table 1: Security Service Edge Control Points Summary



	Sanctioned SaaS		Allowed SaaS	
	Managed Devices	Unmanaged Devices	Managed Devices	Unmanaged Devices
Network Control	✓	✗	✓	✗
Endpoint Control	✓	✗	✓	✗
Application Control	✓	✓	✗	✗
Identity Control	✓	✓	✗	✗

What is notable is the lack of identity and application control for the allowed SaaS, which means zero trust access cannot be achieved. Allowed SaaS apps sit beyond the enterprise perimeter, and the company has zero control over the applications or resources. These apps are also more easily accessed through unmanaged devices, meaning there is greater risk of noncompliant application use. Furthermore, in the event a breach or other incident occurs, the security team is unable to gain access to the applications or secure any data stored there.

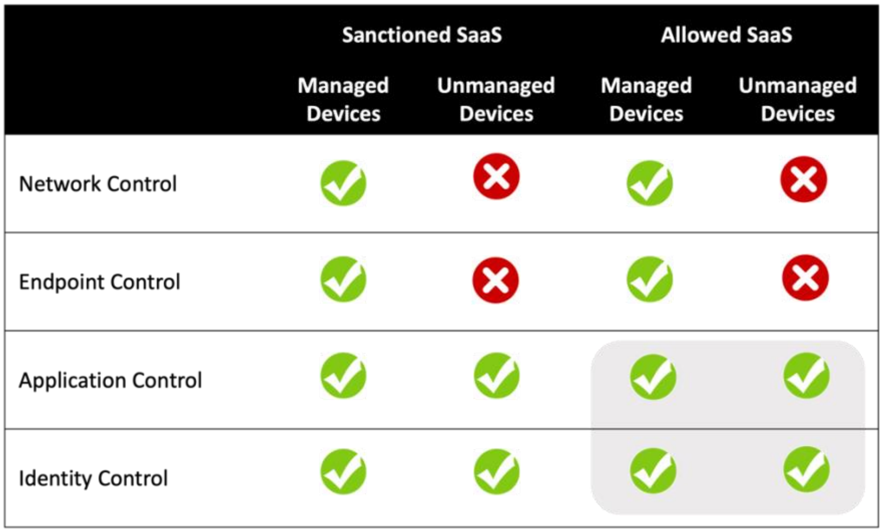
SaaS Security Control Plane Addresses SSE Shortcomings

Companies who want to realize the productivity and enterprise agility value of SaaS applications are designing security architectures that include a SaaS security control plane (SSCP). The SSCP provides a complete view of identity security risk for both sanctioned and allowed SaaS. It provides security teams the ability to extend identity control to SaaS applications they do not govern and is the foundation of a complete SaaS risk management program. Companies are finding that allowing business owners the flexibility to use the applications they want to use results in a closer partnership with IT and security teams that improves compliance. To do this securely requires an SSCP.

In a world where data, resources, and employees are outside the enterprise perimeter, identity security is emerging as the most critical control point. Strong identity security is the foundation for zero trust, but to achieve this requires the unification of identity security silos and a consolidated view of user authentication and authorization that extends to SaaS that is not officially sanctioned. Where SSE is unable to do this, the SSCP was designed specifically to address this gap in SaaS governance.

SSCP achieves this by creating an identity fabric that extends to allowed, but ungoverned, SaaS applications. This allows security teams to control user accounts on SaaS applications without any integrations with security products and enables zero trust access. The following table shows the control points the Grip SSCP can provide that an SSE solution cannot highlighted in gray. The primary control benefits come from extending identity and application control to allowed SaaS, or those that the company allows employees to use but does not govern explicitly.

Table 2: SSCP with SSE Control Points Summary



	Sanctioned SaaS		Allowed SaaS	
	Managed Devices	Unmanaged Devices	Managed Devices	Unmanaged Devices
Network Control	✓	✗	✓	✗
Endpoint Control	✓	✗	✓	✗
Application Control	✓	✓	✓	✓
Identity Control	✓	✓	✓	✓

By extending application and identity controls to allowed SaaS for managed and unmanaged devices, Grip SSCP helps companies implement a more comprehensive SaaS security program and extend zero trust security to these applications.

Additional Benefits of Grip SSCP Solution

In addition to helping to secure SaaS applications, the Grip SSCP delivers numerous other benefits that can help companies.

Digital Supply Chain Vulnerability

Digital products are increasingly relying on SaaS services as key building blocks. This creates a network of systems that are connected through various networks and interfaces that can be extremely complex and requires a high level of trust. However, in a digital supply chain, it may not always be feasible to authenticate and authorize every entity involved in the supply chain due to the large number of participants and the dynamic nature of the interactions. For example, a manufacturer may have to rely on a third-party supplier for certain components, and this supplier may have its own set of suppliers and partners. Grip SSCP can detect the creation of accounts on new development services and automatically require developers to justify the use of these apps. If the reasons provided are not sufficient, the account is locked, and control is provided to the security team.

Single Source of Truth for Identity Risk

Understanding identity risk is critical to zero trust security, and not having a single source of truth can be a challenge because it can lead to inconsistencies and conflicts in assessments across different systems and departments. Today, identity risk is assessed from multiple viewpoints such as endpoint, network, user, application, etc., and there is no single source of truth. This can lead to conflicting risk assessments and result in users being granted access to resources they should not have access to or being denied access to resources they should have access to. Grip SSCP can consolidate dashboards and security personnel can have a single source of truth to understand identity risks and empower teams to orchestrate their actions across multiple systems from one place.

Integrating Identity Security Silos

Modern identity security is extremely complex, and companies are constantly adding new products to address new threats. This has created an environment where most products operate in silos, where different teams or departments within an organization are responsible for their own security product and policies, and they may not share information or collaborate with other teams. This can create security product overlaps and gaps in security, as well as lead to inconsistencies in policies and procedures that creates barriers to implementing zero trust security. Grip SSCP can help all teams involved in identity security collaborate and coordinate their policies and actions.

SSCP Helps Companies Realize the Full Benefits of SSE

SSE is a powerful approach to cybersecurity that can help organizations protect their sensitive data, networks, and resources from advanced threats. However, implementing it does not cover the entirety of risks created by the proliferation of SaaS use in a company. To overcome these risks with traditional SSE solutions will result in an inflexible architecture that requires each SaaS application to be individually vetted and integrated into a security application for governance.

A better way to achieve the security outcome desired is to add an SSCP to the architecture to reinforce the identity security gaps SSE is unable to cover. SSE provides many advantages with its ability to provide security services wherever users and applications at the edge where end-users and their devices are located. However, it was never designed for a world where workers provisioned their own applications on demand without going through a central purchasing process. By adding an SSCP, companies can achieve a robust and effective zero trust security model that can withstand even the most sophisticated cyber threats.