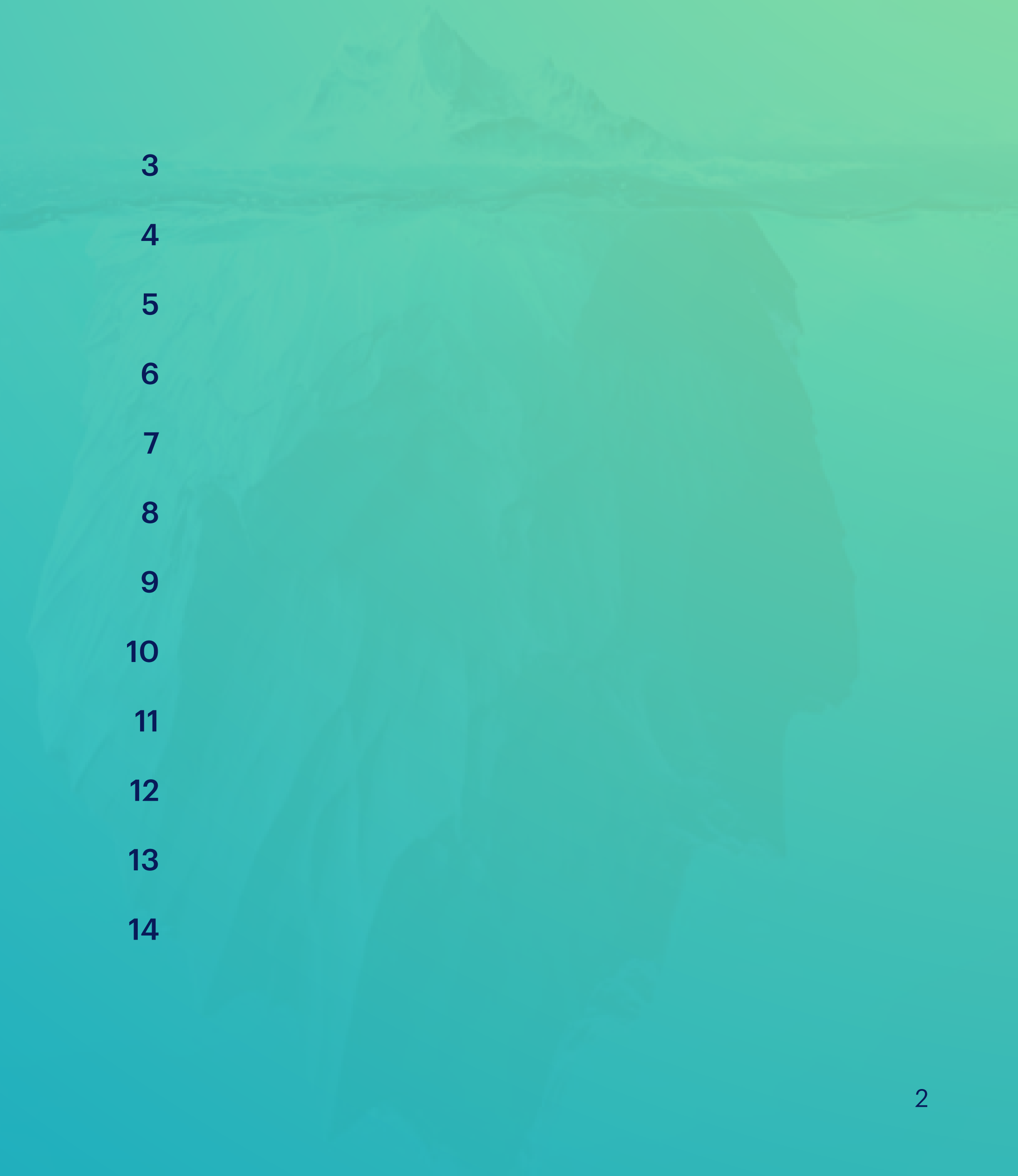
+ eBook

New Insights for Threat and Data Protection

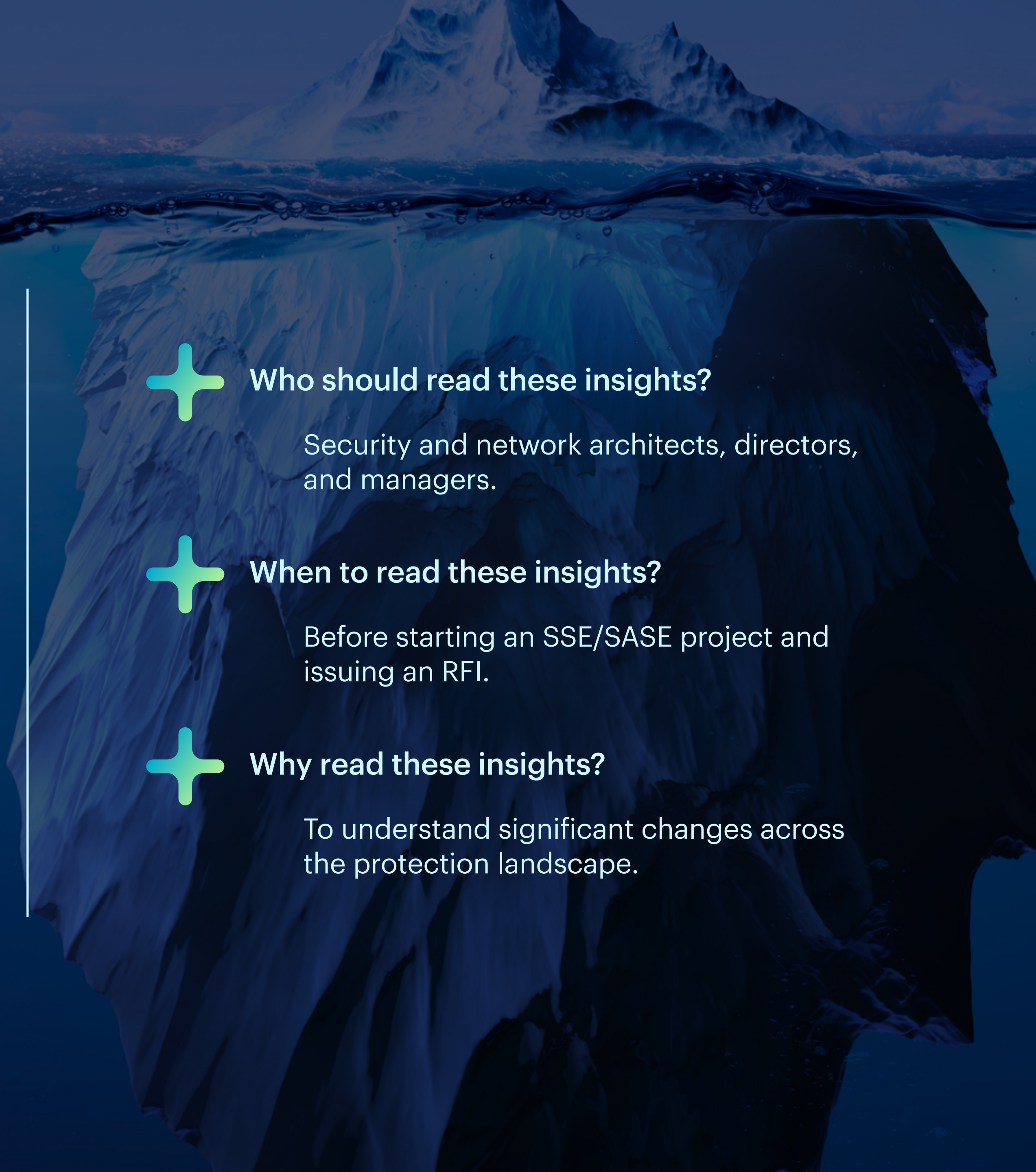
What Legacy Vendors Want to Hide

Table of Contents



Introduction

Threat and data protection legacy practices may be doing more harm than good. These age-old practices also enable security vendors to hide issues they do not want exposed. The pandemic accelerated SaaS and cloud adoption putting more users and data beyond fading perimeters and outside the scope of legacy security solutions. By working with enterprise and multinational companies on security service edge (SSE) deployments, we have compiled ten insights for policy controls, best practices, and how to uncover blind spots. We recommend updating your request for information (RFI) requirements when considering an SSE or secure access service edge (SASE) solution with these insights gained from the trenches.



Who should read these insights?

Security and network architects, directors, and managers.

When to read these insights?

Before starting an SSE/SASE project and issuing an RFI.

Why read these insights?

To understand significant changes across the protection landscape.

Insight 1

Bypassing Microsoft 365 traffic inspection is a blind spot

Best in class SSE solutions now remove the performance versus security trade-off to bypass Microsoft 365 (M365) traffic inspection, in addition this threat and data protection blind spot has grown too large to ignore. Question any inline security vendor that bypasses M365 traffic in your environment.

Key Points

- **More than one-third of cloud-delivered threats are from OneDrive and SharePoint.** This trend has been consistent over the past few years and can be seen in the Netskope Threat Labs 2024 Report where these applications rank first and third in popularity, respectively.
- **More than half of encrypted web traffic is cloud-related, and M365 can be the largest portion.** We have passed a tipping point with more SaaS and cloud service traffic than legacy web traffic. M365 applications can represent 35-40% of cloud related SaaS traffic as IT users spend their workdays within these applications creating and managing content.
- **Inspecting M365 traffic with legacy security solutions impacts user experience.** Backhauling remote and hybrid user traffic to data center on-premises security appliances can impact user experience. On the other hand, direct access by users bypassing these security gateways creates a blind spot for threat and data protection. SSE solutions are replacing these security appliances and legacy VPNs with a more secure, granular, and faster user experience.
- **Microsoft partner certifications require a bypass with a default of no inspection.** Looking back the certification had its justifications given the point above about legacy security solutions impacting user experience. However, today SSE solutions provide an array of global on-ramps with a performant user experience with no trade-off between security and performance. The default needs to change to inspecting M365 traffic as a leading source for cloud-delivered threats and potential data theft.
- **View your web browser secure connection certificate to validate inspection.** Click on the icon in front of the URL when working within an M365 application to view the web browser secure connection and its certificate. If you see a Microsoft certificate for the TLS tunnel, then you are bypassing inspection and have a blind spot. An SSE solution provides inspection and uses its certificate (or a customer CA signed certificate) for the secure TLS tunnel from the user to the SSE cloud platform. So, you should see the SSE solution certificate for the secure connection, not the Microsoft certificate.

Insight 2

The frontline is now real-time at T+0 for threats versus the herd

Real-time threat protection at T+0 hours is the frontline; avoid being misled by higher detection rates hours or days later from shared threat intelligence across the herd. This is an area you must press inline security vendors to provide T+0 threat detection efficacy rates with a low false positive percentage.

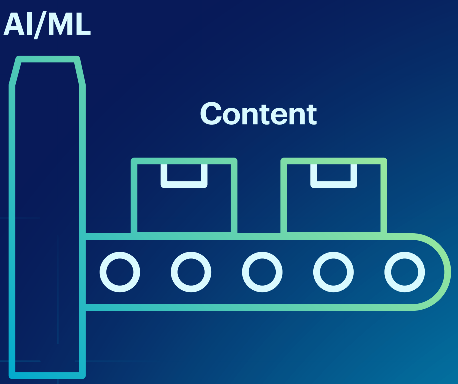
Key Points

- **Attacks have faster life cycles, may be targeted, and use trusted apps/domains.** Patient zero is the first person infected by a new threat and with targeted attacks they may be the only one. Given attacks are using trusted application and cloud services for hosting and delivery, these domains are often allowed, and as noted above often bypassed.
- **Validate real-time T+0 threat protection efficacy versus T+4-hours or longer.** When viewing lab reports for inline threat protection efficacy, review the T+0 real-time results, and if not provided, request them. Many reports will report on the highest efficacy rates hours or days later when shared threat intelligence from the herd makes everyone look good.
- **Pay attention to the false positive (FP) rate in test reports, a lower percentage is better.** A known trick when testing threat protection is to dial-up detection capabilities at the expense of false positive detections. While a solution may get 98% and 99% ratings for efficacy over several hours of retests, see if the FP rate is 2.0% or higher. You are unlikely to get the same high detection results when threat protection is dialed down to lower the FP rate to an acceptable level below 1.0% for customers.
- **Demand a recent threat efficacy test report for inline defenses.** Attacks change and not every threat is an executable file, as file-less attacks increase, plus fake forms and phishing attacks focus on access credential compromise. Hosted fake login forms in trusted cloud services for applications that users access every workday require real-time protection to protect patient zero and others with first exposure. Test reports should cover PE files (executables), non-PE attacks (file-less), and phishing attacks. Most endpoint testing does not cover all three, so look to SSE solutions to cover the gaps. Optionally, consider best in class pen-test tools if no test report can be provided.
- **T+0 is the front line; everyone looks good hours later with shared threat intel.** Avoid the quick glance or scan of threat protection lab test reports and understand the details for T+0 real-time results versus hours or days later. Also make sure the FP rate is acceptable for the testing and matches your expectations. Threat protection in real-time at T+0 and how fast solutions can learn new attacks within an hour is key.

+ Insight 3

Content visibility enables AI/ML defenses for real-time protection

Generative AI is now widespread with expectations to transform many parts of our daily lives including at work and home. For AI and machine-learning (ML) to work in real-time it requires content, and this is where SSE solutions differ for threat and data protection.



Key Points

- **Real-time AI/ML defenses only work if they have the content.** Assuming attacks are file-based ignores the fake login forms and other tactics hosted in cloud services used within attacks. Real-time phishing detection with AI/ML defenses is possible given the content can be exposed inline during the business transaction to protect the user. AI/ML defenses only used in the background do not protect in real-time.
- **Inline defenses need to provide content visibility for SaaS applications.** Not every inline SSE security solution can expose content for managed and unmanaged SaaS applications and cloud services, so inventory what content can be inspected. Also, consider most threats come from non-company tenants and personal instances of popular SaaS applications where inline inspection is your first line of defense, as endpoints and email security lack the ability to decode SaaS application content in real-time for AI/ML analysis.
- **Both data and threat protection utilize AI/ML-based defenses inline.** Portable executable (PE) files can be detected inline with ML classifiers where 6 out 10 malicious PE files do not have a known signature at the time of detection, according to Netskope threat research. Phishing attacks can also be detected where AI/ML analyzes fake forms to protect in real-time long before phishing URLs are shared in threat intelligence feeds. Here are some examples of phishing attacks detected using real-time AI/ML defenses.
- **Source code is the most popular content used in ChatGPT.** As the most popular Generative AI application to date, ChatGPT is mainly being used to optimize source code. AI/ML data classifiers from Netskope can detect more than 20 types of source code inline without traditional data classification, registration, or data identifiers of DLP. This enables SSE solutions with GenAI app connectors to immediately provide data protection of company source code and to coach users in real-time to use company approved GenAI applications and tenants.
- **AI/ML defenses need to be inline, not just in the background.** AI/ML capabilities have been used for years in the background for detection, optimization, classification, and even operations. The explosive focus on GenAI apps has resulted in the overuse of AI in marketing messages and content. Focus on what SSE solutions are providing inline with real-time AI/ML capabilities versus the background.

Insight 4

Phishing is moving beyond email and into all communications

Widespread communication channels to users are enabling phishing, fraud, and business compromise beyond traditional email. Leveraging SaaS and cloud hosting services, phishing attacks can ride on these popular domains and evade detection by legacy security defenses unable to decode and analyze SaaS content with real-time defenses. Going forward content visibility is a key requirement for SSE solutions to enable real-time defenses.

Key Points

- **Phishing is a primary entry point for ransomware.** Weekly news stories continue to expose the impact of ransomware where research reports note key entry points of phishing including software packages and patches, access compromise, drive-by downloads, malvertising, and file-less attacks. Across the kill chain for ransomware attacks, content visibility enables threat and data protection including anomaly detection, access compromise, and data exfiltration.

- **Social, IM, Chat, and personal communications are phished.** Financial institutions have been the leading target of phishing attacks, however, social media has grown to almost equal the leader in a close second place ranking within one percentage point, followed by SaaS/webmail in third place based on the latest trends.

- **Users expect a work/life balance and access to personal apps.** Hybrid and remote work have put new demands on managed devices for users accessing personal communications. Even returning to offices, users expect a work/life balance for access. Work to limit access to high-risk apps, control app activities to protect data, and consider remote browser isolation (RBI) of personal SaaS and webmail to protect managed devices. Blocking access only frustrates users and keeping high value IT workers is a competitive advantage.

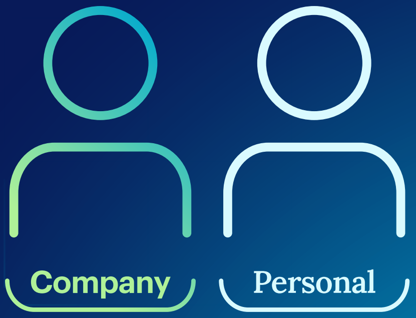
- **SaaS apps host fake login forms in trusted domains to users.** SaaS adoption continues to increase year over year at a 20%+ growth rate where more than 98% of new SaaS applications are adopted by business units and users, not IT administration. Look beyond managed SaaS applications into unmanaged tenants and personal instances for applications as blind spots for phishing attacks hosting fake login forms.

- **Attack entry has expanded beyond traditional email, inspect SaaS inline.** The hidden 800-pound gorilla between legacy secure web gateway (SWG) and cloud access security broker (CASB) solutions is the inline inspection of SaaS applications and cloud services numbering in the thousands for many companies and organizations. Avoid the stereotypes of CASB as DLP for managed SaaS and legacy SWG for all things web and cloud.

Insight 5

Focus on personal app instances for threats and data exfiltration

The new high-risk zone for threat delivery and data theft resides in the blind spot of SaaS personal (vs company) instances. While you may provide managed SaaS office productivity applications to your users, they can also have their own personal instance version. This enables data exfiltration from company to personal instances in applications all too easy, and under the same domain you allow and may not inspect inline.



Key Points

- **Data theft increases 300% in the last 30 days of employment for departing users.** In the first two years of the pandemic, Netskope research on data movement and sprawl found an interesting trait. For users that terminated employment, researchers looked back at the past 30 days of data activity and found an increase of more than 300% in data exfiltration compared to active users. Working remotely, users were collecting data and information they viewed as valuable for their next job a few weeks before departing.
- **For those 30 days, 74% of data theft goes into personal cloud storage apps.** No surprise, users collected the data into personal cloud storage during the last 30 days of employment, where the leading application was Google Drive. Applications and cloud services providing free file storage lead for both data exfiltration and threat delivery given how easy they are to use and access.
- **Monitor and control data movement between company and personal instances.** Well over 480 applications have both company and personal instances where data movement and activity should be monitored, controlled, and assessed for behavior anomalies. And for applications without instance awareness, your SSE solution should be able map user identities for logins for policy controls per application tenant.
- **The overwhelming majority of cloud-delivered threats are from personal instances.** The first key point in this eBook noted OneDrive and SharePoint delivering over one-third of cloud-delivered malware. The qualifier to this key point is the threats are mainly from personal and rogue instances, not your company managed instances. Attackers easily create and use rogue public free applications, or compromised accounts to deliver threats and exfiltrate data, inspecting SaaS traffic inline with real-time defenses is required.
- **Avoid blocking and tenant restrictions and enable SaaS app instance-awareness**. SSE solutions without instance awareness for hundreds of applications will suggest blocking unmanaged tenants and thus only allowing managed SaaS access inline. This frustrates business units and users where more than 98% of applications in use are not IT managed, and you remove a viable resilience and fail over option if your managed apps go offline for any reason.

+ Insight 6

Users need real-time coaching and guidance, not transparency

Security training programs may meet compliance regulations once per year, however the knowledge is quickly forgotten, and old practices prevail. While the long-held security practice of transparency for defenses remains, we are now in a growing SaaS and cloud services environment where users need guidance in real-time during business transactions to protect data. Imagine a drive in the dark of night into a new city without GPS navigation to find your destination.

Key Points

- **Real-time coaching and guidance help users during business transactions.** Assist users during business transactions about risky applications and recommend safer alternatives. Or warn about risky activities within applications when sharing data outside the company. Real-time coaching, like GPS navigation while driving, is here and should be leveraged quickly in new SSE deployments to guide users.

- **More than 95% of the time users do the right thing when coached and avoid risks.** When users are prompted with a real-time alert during a business transaction concerning a risky application or activity, our findings and customer feedback is that more than 95% of the time they cancel the business transaction to avoid the risky activity.

- **For the other 5%, collect justifications to learn and refine access policy controls**. For users warned about a risky activity with real-time coaching, you can collect a justification reason for continuing with the business transaction. This allows you to further refine your granular policy controls with a better understanding of more use cases and scenarios.

- **Blocking activity frustrates users, raises help desk tickets, and reduces business agility**. Coarse-grain policy controls that block business transactions should be replaced with real-time coaching and to collect justifications. This enables a win-win-win scenario where most users cancel the risky transaction, the few that need to complete the transaction inform you why, and you increase your business agility.

- **Avoid blocking when real-time coaching is an option and educate on risky activity.** Feedback from customer CIOs and CISOs shows that leveraging real-time coaching also results in fewer helpdesk tickets related to blocking policies. User experience, fast access, and transparency remain important, however, like GPS navigation, users appreciate guidance to protect data and the company.

Insight 7

Data protection versus formal DLP, know the difference

If you work in networking or security and data loss protection (DLP) comes up in a meeting, you are probably thinking it is time to exit or check your messages. Reducing the attack surface with data protection before formal DLP is of high value for networking and security teams. Policy controls and access work like a funnel for data protection, so when DLP is invoked, you have the most efficient and focused policy effort.

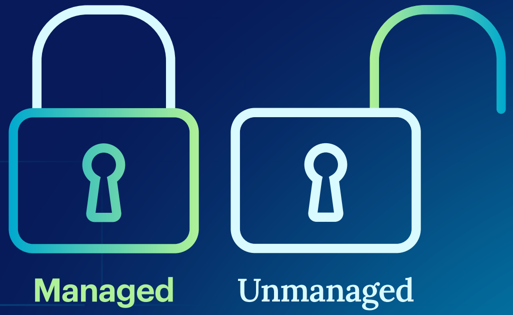
Key Points

- **Formal DLP often requires data classification and registration, it takes time**. For structured data formal DLP is the answer and for all channels of data activity across web, SaaS, cloud, email, and endpoint. Yes, it takes time to find sensitive data sources, classify data, and register the data for exact data matching or fingerprinting where performance and scale is vital for millions, or even billions, of records.
- **Data protection monitors and controls data movement by application and instance.** Before formal DLP you should be implementing data protection policy controls including access to risky apps, app activities, and data movement by application and instance. Put up guard rails with SSE network security around data movement for users to reduce the surface area for risks and data exposure.
- **Recommend safer alternatives for risky apps and activities, plus real-time coaching**. Part of data protection before DLP is the use of real-time coaching during business transactions. Like GPS guidance and awareness about a traffic accident ahead, you can provide safer alternatives to protect users, data, and your company.
- **Collect justifications to advance and refine policies controls for data movement.** Learn new use cases and scenarios from users in their justifications to refine policy controls for data protection that may or may not require formal DLP policies and rules. An SSE solution provides visibility and control for content beyond legacy security solutions, set aside the time to learn these new capabilities.
- **Reduce the attack surface with a funnel approach for data protection controls.** As you work through your RFI requirements and a proof of concept, there should be a funnel structure for policy controls that keeps reducing the attack surface area long before DLP policies and rules are invoked. An entire set of policy controls should focus on data movement and activity, coaching, justifications, and safer alternatives.

+ Insight 8

Managed versus unmanaged apps redefines inline defenses

The security department silo is fading alongside the IT perspective of managing only what they adopt and access. Digital transformation is moving ahead and driving business units and users to adopt SaaS and cloud services without IT involvement. While IT may manage 40-60 SaaS applications and cloud services, there are likely thousands of applications in use within a company or organization. If unknown, the first step should be a cloud risk assessment.



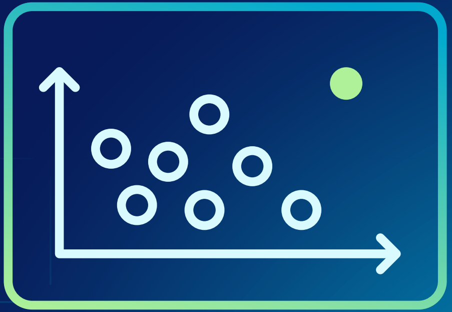
Key Points

- **More than 97% of applications in use are not IT adopted and managed.** This is the speed of adoption driving SaaS at more than 20% growth year over year. As companies adopt a cloud-first strategy, they look for SaaS apps to replace what they use in their data centers. Some countries even have a cloud first strategy as seen with Australia.
- **Business units and users are the primary adopter of unmanaged apps.** Business units and users have goals and timelines driving towards digital transformation, and it is a matter of survival for some companies. They are the primary adopters of unmanaged SaaS applications and cloud services outside of IT administration. An SSE solution can safely enable unmanaged tenants and personal instances with inline policy controls and coaching.
- **API inspection only applies to managed apps and cloud services.** Better together is the mindset given that API inspection is limited to managed applications and cloud services and the previously mentioned 800-pound gorilla for inline inspection covers both managed, unmanaged, and personal application instances. Want to control file sharing then look at API inspection? Want to limit risky apps and coach users? Then look to inline inspection with real-time policy controls.
- **Your cloud storage is likely clean, the rest of it hosts malicious threats.** No issues here, your company managed cloud storage is likely clean and closely protected. This is why attackers use free cloud hosting with roque accounts and compromised personal instances to deliver cloud-hosted threats and phishing. Here the 800-pound gorilla shows up again beyond what can be seen for managed tenants and instances.
- **Inspect unmanaged apps and personal instances inline.** Your RFI should cover the ability to provide inline inspection for thousands of unmanaged apps and hundreds of applications for instance awareness. The ability to inspect this content inline is key for threat and data protection, enabling behavior anomaly detection, and using analytics to uncover unknown risks and data movement.

+ Insight 9

Behavior anomaly detection is no longer optional

For years user and entity behavior anomaly (UEBA) detection struggled with optimal events and logs for the desired use cases of insiders, access compromise, and data exfiltration. The addition of SSE logs and events providing insight to users, apps, and data activity opened the flood gates to support these use cases with high efficacy.



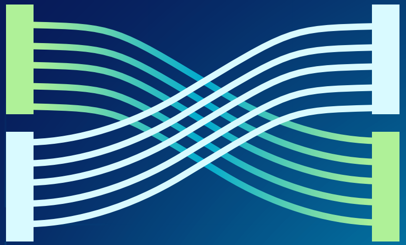
Key Points

- **Users are more assertive with data working remote or hybrid.** A few months into the pandemic and the trends were very clear, remote users take more risks accessing websites, content, and sharing managed devices. Users also found paths out of known swim lanes for data sharing and activity when working remotely with multiple SaaS applications and cloud services, including their own personal instances. As the pandemic matured, users also increased productivity, perhaps lacking water cooler conversations and office distractions.
- **Compromised access is an underground economy on its own.** Increasing SaaS adoption with direct access from remote and hybrid work locations also opened the door for access compromise attacks and an underground economy to sell these credentials. To fight back, your SSE solution should provide dedicated egress IP addresses for managed SaaS access unique to your company or organization. This prevents compromised credential use and prevents reputation issues with shared IP address pools.
- **Use inline inspection to create user and peer group activity baselines.** SSE solutions inspecting thousands of SaaS applications and for hundreds of instances provide excellent event and log data. This enables highly desired UEBA user and peer group activity baselines for anomaly detection going beyond what sequential anomaly rules and queries can detect with accuracy. Also, peer groups flush out any pre-existing anomalous behaviors within a single user baseline.
- **Leverage machine learning (ML) based UEBA to detect anomalies.** Given the granular policy controls of an SSE solution, the alerts, logs, and events enable multiple machine learning (ML) models and unique detectors. An SSE solution should have more than 50 ML models and 100+ detectors for anomaly detection for a desired degree of maturity and experience.
- **Score and monitor users for risky behaviors and data exfiltration.** SSE solutions open the door for user confidence index (UCI) scoring for use in adaptive access policy controls and to signal investigations into event correlation timelines for risky activity and data movement. Review our blog on how to operationalize UEBA for more details.

Insight 10

Monitor to uncover the unknowns in analytics and visualizations

Comparable to using AI/ML for defenses is the use of advanced analytics and visualizations to understand application trends, behaviors, plus known or unknown anomalies. A cloud risk assessment can set a baseline to then begin implementing policy controls and to monitor changes in behavior and activities to achieve the desired results. Real-time coaching and collecting justifications can be shown in graphic visualizations, as well as word clouds. Think beyond legacy SWG and web filtering reporting with new SSE visibility for apps, users, and data activity.



Key Points

- **Visibility is key for users, applications, and data activity to find unknowns.** How many cloud storage applications are in use across your company and organization? How many are managed versus unmanaged and is there data sharing with third parties, partners, and consultants? The same holds true for generative AI apps, plus the wider array of applications used in marketing, sales, and human resource departments working with sensitive data.
- **Remove blind spots for M365, instances, and unmanaged applications.** SSE solutions remove the blind spot of not inspecting M365 traffic and the hidden personal instances or unmanaged partner tenants often related to threat delivery and data exfiltration. The days of filtering by domain and web category for the primary applications and cloud services most frequently used are gone. Now the details are within instances, activity, and data movement.
- **Leverage dashboards and graphic visualizations (i.e., Sankey charts).** Humans are very effective with visualizations to detect anomalies and areas of interest for further details and drill downs. SSE solutions should provide a wide array of dashboards and visualizations beyond traditional reporting, plus the ability to store events and logs for 3, 6, or 13 months, thus enabling year-over-year analysis. Near real-time log streaming off SSE platforms is also preferred, however, the destination may not have advanced analytic visuals and dashboard ready to use.
- **Monitor data exfiltration flows for users, applications, and instances.** Data is the zero trust component that connects users, devices, applications, and networks together. Data flows between these components and is at the heart of what to protect. SSE solutions with granular visibility and control enable least privilege access and continuous monitoring to further refine and mature policy controls to support zero trust principles. Providing zero trust access with a blind spot for users, apps, data activity misses the strategy and objectives of zero trust.
- **Uncover unknowns with analytics from context and visualizations.** Users adopt and find new paths for unknown and unapproved data movement every day. Analytics can uncover these unknowns in graphic visualizations quickly and efficiently. Unless the new data activity triggers alerts, it could remain hidden for an insider, risky users, or departing employee collecting sensitive information for their next job.

Summary

These 10 insights bring out new capabilities and requirements for an SSE or SASE RFI and future projects. Insights from customers recommend an SSE transformation from existing capabilities of legacy security solutions first. Then the SSE journey begins developing new skills, adding new defenses like dedicated egress IP addresses, assisting users with real-time coaching, removing blind spots and trade-offs, adding guard rails and data protection before DLP, leveraging real-time (T+0) defenses including AI/ML-based detection, and monitoring for behavior anomalies while using analytics to graphically expose the unknown.

- **Learn more about Netskope Security Service Edge**
- **Customer Case Studies**
- **Gartner Critical Capabilities for SSE**