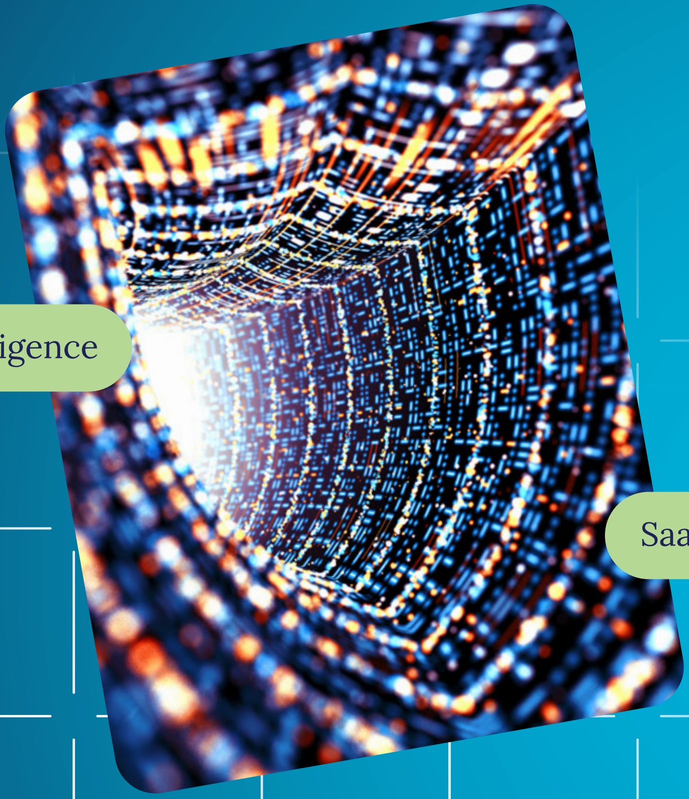
netskope

White Paper

Modern SaaS Security in an AI-driven World



Artificial Intelligence

SaaS Security

Table of Contents

Who should read this paper?

Network and security executive teams - VPs, directors, and managers, data security admins, compliance team, cloud infrastructure architects.

When to read this paper?

When you are evaluating your options for securing your SaaS applications and need a comprehensive understanding of the best practices and solutions available. This whitepaper is particularly useful if you are:

- Comparing different SaaS security solutions to find the best fit for your organization.
- Preparing to decide on a new security solution for SaaS security.
- Looking for in-depth insights and industry trends.

Why read this paper?

Securing SaaS today is more difficult than ever with exponential growth of SaaS risks, increased data exposure risks, stricter data privacy expectations and security gaps caused by diverse applications and data environments.

An understanding of some of these modern challenges of SaaS security will help you stay ahead of the curve and ensure your SaaS security posture is intact.

EXECUTIVE SUMMARY

SaaS remains popular among enterprises due to its accessibility, scalable usage, and rapid deployment. However, with exponential SaaS growth and increasing use of Shadow IT, securing SaaS was challenging before, and it is even more difficult now with the integration of GenAI applications. This situation is complicated further by the increased risk of data exposure owing to third-party SaaS apps being integrated with corporate SaaS apps, leading to complex interdependencies and the potential exposure of sensitive data. Enterprises are expected to not only adhere to regulations but also to prioritise data privacy to provide their customers with a better experience. The diverse range of applications across the enterprise and the constantly evolving data environment create security gaps and bring their own set complexity and management challenges.

Utilizing Cloud Access Security Brokers (CASB) and SaaS security Posture Management (SSPM) can help address the challenges associated with SaaS sprawl. Though the true value of any investment on SaaS security solutions will be realized when these solutions are seamlessly and natively integrated, with focus on detailed categorization of SaaS risks. Additionally, the solutions should address key areas like advanced data security, and risk prevention, along with simplicity in managing security operations and incident response

> Leverage Netskope's modern SaaS security capabilities, powered by GenAI, to stay ahead of the curve and secure SaaS, proactively.

MARKET CONTEXT

Cloud adoptions show no signs of slowing down. In fact, Gartner predicts they will become a business necessity by 2028, with global public cloud services spending projected to reach $679 billion by 2024. Enterprises are pursuing this trend, as investing in cloud technology presents undeniable advantages: It can drive market disruptions, enhance customer experience, and accelerate business initiatives.

Today, multiple cloud service models support diverse enterprise needs, mainly: Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS).

The largest cloud services market is SaaS, with an estimated market value of approximately $244 billion in 2024 and a growth rate of 42% year over year. With over 31,000 SaaS companies globally, SaaS is expected to power 85% of all business applications by 2025, up from 70% in 2023.

WHAT MAKES SOFTWARE-AS-A-SERVICE (SAAS) SO POPULAR?

Even though SaaS applications have been around for a while, there are different factors that have contributed to widespread adoption of SaaS amidst organizations of every size today and will continue to do so in days to come. Following are a few:

1. **Lower Total Cost of Ownership and Scalable Usage:** A subscription-based pricing model allows enterprises and businesses to pay only for the resources and features they use and thus eliminates the need for upfront investment in hardware, software, management, and other infrastructure costs.

   Transitioning costs to a recurring operating expense allows many businesses to exercise better and more predictable budgeting.

   It also gives them the opportunity to scale their software stack up and down as per changing business requirements.

2. **Easier Accessibility, Availability, and Integration:** SaaS applications can be accessed via a browser or a device from anywhere in the world. This fosters remote work, collaboration among distributed teams, and better productivity.

   These applications are often customizable and offer built-in collaboration tools, integration with third-party services, and APIs that can enable seamless data exchange and interoperability with other systems and applications, thus offering organizations the granularity they seek in their day-to-day operations.

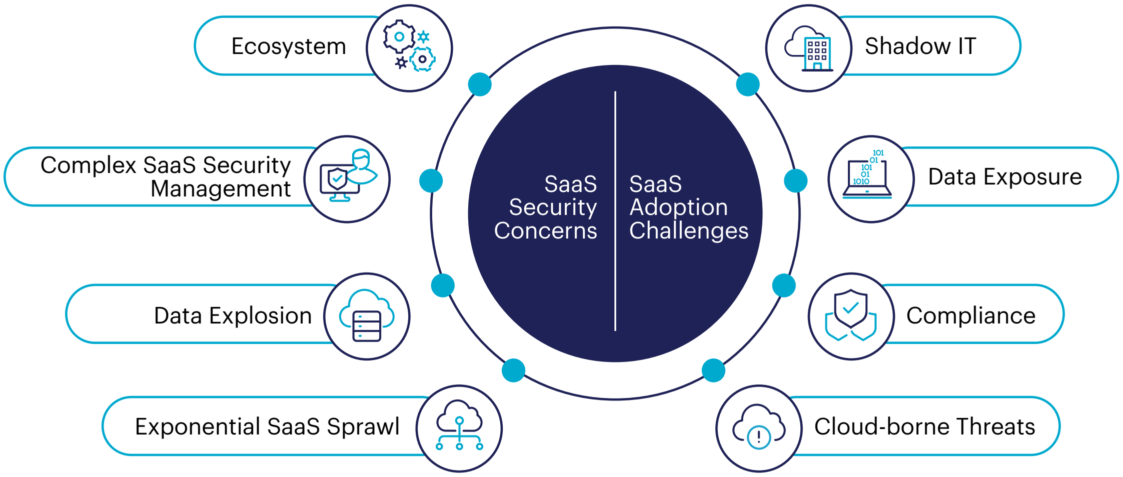
3. **Rapid Deployment and Continuous Updates:** SaaS applications can be deployed and provisioned quickly. This equips organizations to bring new products and services to market faster and capitalize on emerging opportunities.

   Organizations can rely on a SaaS provider to automatically deliver and perform updates and patch management, without any disruption to users. This further reduces the burden on in-house IT staff.

SAAS ADOPTION CHALLENGES AND NEWER CONCERNS FOR ORGANIZATIONS

While SaaS is the most popular cloud delivery model, it comes with its own set of security challenges and risks that organizations need to be aware of and control. Let’s evaluate a few challenges associated with SaaS adoption and how an evolving security landscape has posed a newer set of concerns for organizations to deal with.

SaaS Adoption Challenges and Newer Concerns for Organizations



Challenges associated with SaaS adoption

1. **Shadow IT:** Shadow IT refers to zero to poor visibility into unsanctioned SaaS applications being used within an organization. According to Gartner, by 2027, 75% of employees will acquire, modify, or create technology outside of IT's visibility.

   While the personal use of unsanctioned SaaS apps is not necessarily bad and can improve productivity, bring innovation, and enhance employee engagement, as well as adaptability and responsiveness, the usage of unprovisioned SaaS applications can leave the organization open to data breaches and noncompliance. It also leads to the SaaS stack evolving into distributed and unaligned systems.

   However, while tolerating the use of unsanctioned SaaS applications can have these benefits, it is essential for organizations to balance this flexibility with proper oversight and security measures to mitigate risks associated with data breaches and noncompliance. Implementing mechanisms to monitor and possibly integrate these tools can help maintain a secure and compliant environment while reaping the benefits of shadow IT.

2. **Data Exposure:** The use of SaaS applications can lead to sensitive data exposure in unprecedented ways, fundamentally changing the landscape of data security. Unlike traditional IT systems that are typically managed and secured within a company's internal infrastructure, SaaS applications operate on external platforms, often beyond the direct control of the organization. This decentralization results in fragmented data storage, where sensitive information is dispersed across multiple third-party services. This setup can inadvertently bypass established security protocols, making it easier for unauthorized individuals to gain access. Additionally, third-party SaaS apps integrated with corporate SaaS apps can create complex interdependencies and potential vulnerabilities, further exposing sensitive data. Thus, the proliferation of SaaS applications introduces novel and complex challenges for data protection, requiring organizations to adapt their security strategies to mitigate these emerging risks.

3. **Compliance and Data Privacy:** Funnelled by increased cloud adoption, AI/ML, and mobile applications, SaaS usage is going places, and with it, concern for compliance adherence as well. Organizations today must navigate a set of regulations that span across multiple jurisdictions, each with its own standard rules and requirements. The stakes are very high and any deference against these norms in day-to-day operations can attract fines, penalties, and loss of customers' trust. Moreover, a proactive approach to compliance, one that anticipates changes and adapts swiftly, never hurts; instead, it will help stay ahead of the curve. These regulations could revolve around international standards like the **General Data Protection Regulation (GDPR)** in the European Union and the California Consumer Privacy act (CCPA) in the United States for data handling practices.

   All in all, implementing SaaS compliance can be difficult, but it's necessary to ensure adherence with regulatory requirements. With the right strategies and practices in place, organizations can benefit from complying with regulatory requirements that will help keep them secure, while providing their customers with a better experience.

4. **Cloud-borne Threats and Malware:** This refers to security risks or malicious activities that target cloud computing environments. As more businesses and individuals migrate their data and services to SaaS, it's becoming a prime target for cyber threats. These threats can include data breaches, account hijacking, malware injections, and denial-of-services attacks, among others.

   To mitigate cloud-borne threats, it's essential to implement robust security measures such as encryption, access control, multi-factor authentication, and continuous monitoring. Additionally, staying informed about the latest security trends and vulnerabilities in cloud services can help organizations proactively address potential risks.

Newer set of SaaS security concerns for organizations to deal with

1. **Exponential SaaS Sprawl:** The explosive growth of SaaS apps has fundamentally reshaped the business technology landscape, with employees increasingly turning to these platforms, including emerging tools like generative AI applications, to meet their evolving needs. This surge in SaaS app adoption reflects a broader trend toward agile, cloud-based solutions that empower users to streamline workflows and drive productivity. However, the widespread use of these apps, without IT security oversight, introduces new complexities for organizations. Primarily they can pose significant security risks and challenge data management efforts. Despite these concerns, the allure of SaaS innovation continues to drive demand, underscoring the need for organizations to strike a balance between harnessing the benefits of these tools and implementing robust security measures to safeguard sensitive data. As quoted by BetterCloud, the net growth of SaaS applications used is up by 18% in 2023.

2. **Data Explosion:** "Data is growing." This statement would be underplaying the proclamation. As per IDC, by 2025, worldwide data will grow 61% to 175 zettabytes, with as much of the data residing in the cloud as in data centers. 49 percent of data will be stored in public cloud environments and nearly 30 percent of data generated will be consumed in real time.

   The exponential sprawl of data is transforming the digital landscape, with data growing in volume, variety, and velocity at an unprecedented rate. Organizations are grappling with an ever-increasing influx of data from diverse sources, spanning structured and unstructured formats, and arriving at staggering speeds.

This proliferation is fueled by a multitude of factors, including the digitization of processes and the widespread adoption of cloud-based services. As data continues to expand in both scale and complexity, organizations are confronted with the challenge of managing a diverse array of data types, ranging from traditional relational databases to image formats, compressed files, multimedia content, and streaming data streams. Moreover, the proliferation of data-sharing practices, both within organizations and across ecosystems, further exacerbates the challenge, as data flows freely between systems, departments, and external partners.

3. **Complex SaaS Security Management:** In today's expanding SaaS landscape, organizations seek comprehensive security solutions. This includes an overarching risk management strategy for evaluating and monitoring SaaS usage, and flexible governance frameworks to ensure compliance and security. These elements are vital for optimizing SaaS security management.

   SaaS security management poses a significant challenge due to the proliferation of diverse security tools and platforms. With organizations utilizing a multitude of SaaS applications across various departments and functions, each app may come with its own risks and compliance requirements, leading to fragmentation and gaps in security coverage. This complexity is further compounded by the disparate nature of security alerts generated by traditional SaaS security tools, making it challenging for security teams to effectively prioritize and respond to threats. Incident management fatigue sets in as teams grapple with the overwhelming volume of alerts coming from different sources. Moreover, managing security across multiple consoles and enforcing complex policies adds another layer of complexity, often resulting in confusion and inefficiency. To address these challenges, organizations need to streamline their security infrastructure, consolidate tools where possible, and invest in centralized management solutions that provide unified visibility and control over the entire SaaS security landscape.

4. **Ecosystem:** The main reasons for popularity of SaaS applications today are the scale, flexibility, customization, and quick turnaround that they offer. If equated right, deploying the right applications as a part of the SaaS stack can greatly impact an organization's time to market while giving a competitive edge. However, for this to happen it is imperative that data sharing amidst an organization’s systems, at times disparate, is without any data manipulation and transformation steps. Amalgamation of SaaS applications with existing organizational set-up, on-premises systems, cloud assets, and third-party platforms can present significant challenges, involving visibility, compliance, and governance. Even with careful planning and implementation, it is crucial to ensure secure data exchange between disparate systems, all while maintaining data integrity.

SECURITY CONSIDERATIONS FOR AN ENTERPRISE-READY ORGANIZATION

Increased cloud adoption has led to accelerated SaaS implementation. However, managing these applications has become challenging due to their diverse nature, the highly distributed workforce accessing them, and the dissolving corporate network perimeters. Despite these challenges, securing SaaS environments is crucial for protecting sensitive data, maintaining customer trust, and complying with regulatory requirements.

Every organization should adhere to the following basic tenets of enterprise readiness when securing SaaS applications:

1. **Data Protection:** SaaS applications often store and process sensitive data, including customer information, financial records, and intellectual property. Implementing robust security measures is essential to prevent unauthorized access, data breaches, and data loss. Both accidental insider errors and malicious insider actions can expose sensitive data to significant risks, including theft and loss.

2. **Compliance Requirements:** Regulators keep a close eye on organizations' security practices to ensure compliance with applicable laws and regulations such as PCI DSS, SOC 2, ISO 27001, GDPR, etc. Organizations must demonstrate adherence to these security practices to avoid regulatory fines and penalties.

3. **Customers' Trust and Privacy:** Data breaches can damage a SaaS provider's reputation and erode customers' trust. Investing in robust security measures helps build confidence among customers and stakeholders, demonstrating a commitment to protecting their data and maintaining a secure environment.

   Protecting customers' privacy is also important to comply with various regulations – GDPR, CCPA, and HIPAA.

4. **Malware Protection and Zero Trust:** In a SaaS-enabled enterprise, the risk of attacks is significant due to the interconnected nature of cloud applications and the high level of user interactions. Implementing advanced threat protection strategies is crucial to detect and mitigate malware and zero days. Additionally, adopting a zero-trust security model ensures that all user interactions are continuously secured and that no entity is inherently trusted when accessing corporate resources.

CHANGING PARADIGM

Investing in and exploring new technologies can help organizations gain momentum and a competitive edge. Among emerging technologies, generative AI (GenAI) stands out for its profound influence on SaaS. According to Gartner, by 2026, generative AI will significantly impact 70% of the design and development efforts for new applications. SaaS companies are already recognizing the potential benefits of this technology, with 35% of them currently integrating AI in some capacity.

One method of integration involves leveraging large language models (LLMs), which enhance the system's ability to understand user intent and provide appropriate responses. For example, in the banking industry, chatbots use LLMs to address initial queries and provide guidance effectively.

However, the use of GenAI brings data privacy and compliance challenges. Sharing sensitive corporate information with AI models can inadvertently expose confidential data, as accurate AI responses often require precise prompts. Chatbots like ChatGPT and Gemini, which utilize natural language processing (NLP) to create detailed conversational dialogue, exemplify these risks.

Additionally, the integration of GenAI contributes to the ever-increasing data landscape. Techniques like data synthesis (augmenting real data to train AI models more efficiently) and data stories (using augmented analytics to blend data analysis with compelling narratives for better decision-making) are becoming prevalent.

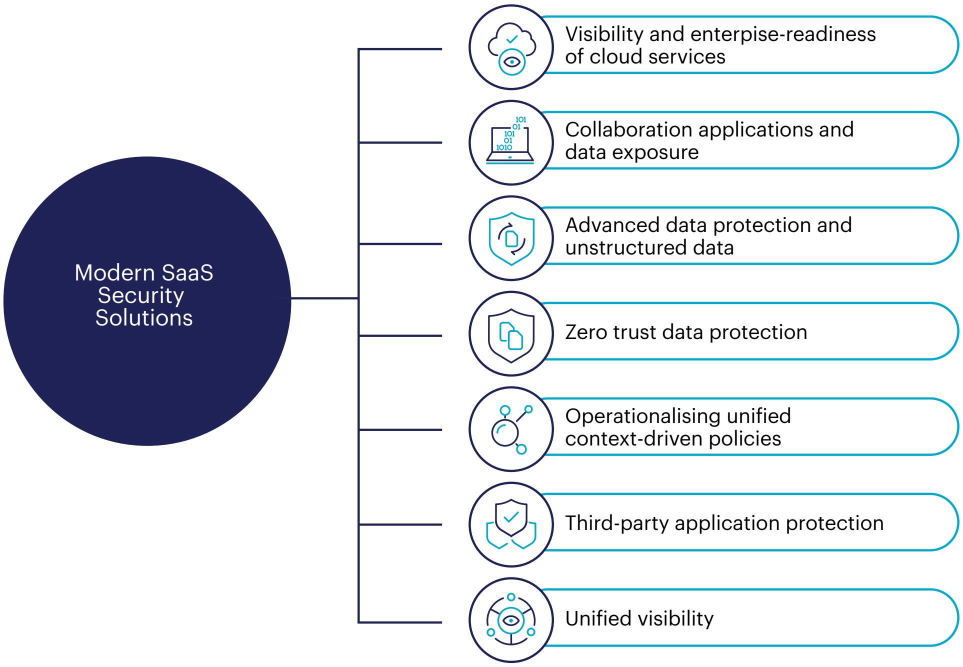
While GDPR, Interim Administrative Measures for Generative AI (China), and Artificial Intelligence and Data Act (Canada) have already established predefined norms and recommendations on the usage of GenAI, it's only a matter of time until we will see evolved compliance norms from other global regulations—EU AI ACT, U.S. Algorithmic Accountability Act, Model Artificial Intelligence Governance Framework, AI Ethics Framework, etc.—targeting specifically the use of GenAI technology in any form within an organization.

A MODERN SAAS SECURITY SOLUTION HAS DISTINCTIVE CHARACTERISTICS

The use cases for SaaS security today are much more sophisticated than merely discovering "shadow IT" and stopping sensitive data uploads to SaaS, and are increasingly focused on granular categorization of SaaS risks, automation, advanced data security, and risk prevention, along with simplicity in managing security operations and incident response.

Let's look at a few of them:

Distinctive Characteristics of a Modern SaaS Security Solution


Modern SaaS Security Solutions
Visibility and enterpise-readiness of cloud services
Collaboration applications and data exposure
Advanced data protection and unstructured data
Zero trust data protection
Operationalising unified context-driven policies
Third-party application protection
Unified visibility

Visibility and enterprise readiness of cloud services

There are tens of thousands of SaaS companies operating worldwide, and this number is expected to increase fivefold by the end of 2024 driven also by advancements in AI technology.

Needless to say, visibility into new SaaS applications, both from established SaaS vendors and emerging ones, is crucial for security teams within any organization. As these applications gain popularity and become integral to daily operations across departments, accepting and tolerating these applications without assessing potential vulnerabilities can compromise the organization's security posture, while excluding them without scrutiny can adversely affect productivity and trust. The need for swift action in this context is paramount.

This is where leveraging detailed reports generated by cloud access security broker (CASB) vendors can be a game-changer. These reports offer granular insights into the risks and even the "enterprise readiness" of SaaS applications, covering aspects such as SaaS usage across the enterprise, risk attribution based on the apps' readiness, potential data exposures, compliance risks, and granular controls to limit risky user activities. They also specifically help manage sanctioned/managed apps and restrict certain data movement to unsanctioned/unmanaged apps.

Let's consider the process. Customer security teams require risk categorization of new applications they intend to monitor or use. CASB providers traditionally employ a manual process, where researchers assess a SaaS app, compare its risk profile against a database, and assign a risk score. If the app is new, extensive research is conducted to determine its risk score and categorization.

Integrating generative AI (GenAI) can transform this process significantly. By automating parts of the assessment, turnaround times can be drastically reduced. With GenAI, CASB vendors can quickly score and map emerging applications, additionally enabling customers to self-serve and obtain rapid categorizations and more granular risk insights via natural language queries. This process can reduce the time taken from days or weeks or months to mere minutes.

Furthermore, incorporating advanced analytics can generate custom reports specific to the customer's needs. When conducted within compliance norms and under proper supervision, this approach enhances the organization's security posture. It also provides peace of mind by ensuring that new applications are thoroughly vetted for enterprise readiness, allowing for timely implementation or consideration of alternative options.

Collaboration applications and data exposure

As quoted by Statista, the collaboration software market (SaaS apps like Slack and Teams) is projected to reach US$15 billion in 2024. The increasing adoption of cloud-based services, the normalization of hybrid workforces, and the need for integrated collaboration tools accessible anytime, anywhere are driving the demand for secure collaboration tools. These tools are essential for facilitating teamwork across geographically dispersed teams. By leveraging social and collaboration tools, organizations enable real-time communications and content sharing, which are particularly beneficial for hybrid workforces.

However, while the rise of collaboration tools meets a critical need, it is imperative that organizations prioritize data privacy and security. Sensitive or confidential information often flows through these platforms, increasing the risk of unintentional data exposure. This is especially true when third parties such as contractors, analysts, collaborators, agencies, customers, and vendors are involved. Collaboration platforms facilitate communication and can simplify the sharing of sensitive information, but this also heightens the risk of security breaches. Sensitive data can extend beyond passwords and structured files to include images, screenshots, and other unstructured documents.

The EA Games security breach is one such example, wherein the process was initiated by purchase of a stolen cookie that was sold online for $10 and the same was used to gain access to a Slack channel used by EA. This stolen Slack authentication cookie enabled bad actors to infiltrate the EA Games' network, stealing 780 Gb worth of data, including source codes, to two of the company's multibillion dollar franchises.

The sheer volume of data transferred via collaboration tools is also a concern. This data often includes proprietary information that must be protected. A significant risk arises when collaboration team channels are created including external third parties, and are then used unwittingly by employees to share sensitive data such as financial documents or unreleased plans.

Modern SaaS security solutions must account for various contextual factors to automatically secure data against exposure. These factors include the type of data being shared, the sensitivity of the data, the identities of the sharers and recipients, and who can access the data within specific channels. Preventing data exposure requires mechanisms to intercept and secure messages before they are posted in channels that include external parties.

In summary, while individual security measures can safeguard collaboration tools and platforms to some extent, maximizing the benefits of these tools without compromising productivity requires comprehensive solutions. A modern SaaS security tool should be based on a zero-trust framework and provide real-time visibility and prevention capabilities leveraging rich risk context. This can be achieved by natively integrating inline SaaS security with API and SaaS security posture management (SSPM), and by leveraging shared risk intelligence to inform and mitigate potential risks dynamically.

Advanced data protection and unstructured data

By 2024, modern privacy regulations will blanket the majority of consumer data, but less than 10% of organizations will have successfully weaponized privacy as a competitive advantage.

Data is growing in leaps and bounds, with unstructured data a big part of the mix, making such sensitive data harder to detect and protect.

The evolving pace of business communication and new data sharing behaviors today demand a new approach to data loss and prevention (DLP) methods, an upgrade from the tried and tested data identification methods that DLP mainly rely on. Frequent data sharing in the form of images captured via smartphone screenshots is one such example. And this is where a contextual understanding of the data being shared, especially specific sensitive data from the sea of information within a corporate environment, will help tremendously.

To get desired outcomes and with utmost accuracy and urgency, leveraging machine learning (ML) and deep learning can be a game changer. For context, ML programs are designed to learn from examples. File classification through machine learning can ensure a rapid and effective means of identifying sensitive information. ML classifiers excel at accurately categorizing documents and images, based on similarities, into specific categories. Image classification doesn't always have to replace textual analysis, but it must complement textual analysis to enhance sensitive data detection.

ML-based image and document classification in a modern DLP solution provides higher efficiency, more accuracy, and better data security.

Zero-trust data protection

Data resilience is among the top three infosec priorities for 2024, and nearly 49% of the surveyed leaders on Gartner Peer Insights survey indicate data security as the top priority in their organizations' 2024 cybersecurity strategy.

This is mainly because of the potential of facing a data breach and/or cyber-physical security incident. In the year 2023, the estimated cybercrime cost was US$10.5 trillion annually and the average cost of a data breach was expected to be US$4.4 million. About 74% of data breaches had a human element at its center.

Data breaches continue to expose personally identifiable information (PII), intellectual property (IP), and other sensitive data at an alarming rate. Both intentional and unintentional data loss by employees, whether malicious or well-meaning, are predominant causes of breaches, along with malicious data exfiltration by external cybercriminals. The consequences of a breach affecting PII and IP can be severe, including direct loss of revenue, diminished reputation, and noncompliance fines.

As engagement models have evolved and settled into a "hybrid" mode, a balanced yet modern approach to tracking, monitoring, and data processing is essential for any organization. Accelerated cloud adoption and increased usage of collaboration apps have broadened the attack surface, necessitating the evolution of data protection methods.

While data loss prevention (DLP) solutions, along with cloud access security brokers (CASB), were originally conceptualized to control users' access to data and meet compliance requirements, traditional DLP solutions were designed to protect data, not the identity of data users. Moreover, if a DLP solution cannot scale and provide additional security across the tech stack, it triggers false positives and increases the load on security practitioners.

In keeping with the theme of consolidated controls, it makes sense to develop capabilities that overlap between user behavior-focused controls and data loss prevention. This could mean that security teams can create and implement a single policy for dual use in data security and insider risk mitigation. User behavior-focused controls can be effective when they work in tandem with DLP, but they will not be sustainable if DLP becomes increasingly inaccurate and its gaps larger.

Another important theme is the adoption of zero-trust security paradigms. By 2026, 10% of large enterprises are expected to have a comprehensive, mature, and measurable zero-trust program in place. Zero-trust security identifies users and devices and grants them just the right amount of access, allowing the organization to function with minimal friction while mitigating risks. A properly deployed zero-trust program demands integration and seamless configuration of different components. Zero trust at its core brings security controls back to the data itself.

Data protection technology today can benefit from an adaptive zero-trust approach that leverages security context and automatically enables proper protection based on changing conditions. DLP must integrate with a wide range of security control points, continually ingest their logs, and leverage them dynamically. A zero-trust-ready DLP must consider organizational risks from users, devices, data, networks, and applications to gain rich risk awareness and provide the right remediation actions.

Every organization has specific data protection needs, and data protection programs are never the same for all. That is why a DLP technology needs to be adaptive, rich in functionalities, and broad in coverage to be shaped around each specific data protection program.

Operationalizing unified context-driven policies

Thales Cloud Security Study 2023 reflects upon the operational complexity of multi-cloud environments, wherein 55% of the respondents find it difficult to manage data in the cloud. Human error was identified as the leading cause of data breaches, along with exploitation of vulnerabilities due to poor security posture as the other cause of concern.

The cloud landscape, as it stands today, is vast, with numerous SaaS applications, each of them presenting different risks, as a part of the picture that must be managed day in and day out, and more are getting added to the overall spectrum daily. Here is where policy management comes into play as a guiding principle that sets the basis for decision-making across the organization, and ensures governance, compliance, and risk management are all duly in place.

Though it is important to note that there are different dimensions for policy management to consider with assets—data, applications, technologies, devices, third-party tools, etc.—involved as a part of the equation. The ever-evolving and expanding attack surface and the constant alerts that are being generated, are further add-ons to the equation.

Organizations deal with operational struggles in their security environments when they have alert fatigue.

When it comes to alerts, only a portion of security incidents can typically be addressed by an incident response team, while false positives waste valuable time and effort in diagnosis. Amidst the plethora of wasted alerts, there could be potential indicators of significant forthcoming incidents. One way to manage the constant flow of alerts would be to "block" everything, but this approach is both counterintuitive and impractical.

A more effective approach is for security practitioners to receive actionable recommendations based on data points like alert criticality, related resources, users, and activities—in other words, context behind the alerts. This would tremendously reduce complexity for security practitioners and provide them with valuable guidance. If security policies could become more automatic and leverage all relevant context for prioritizing posture findings, quickly remediating the most important issues from a policy enforcement standpoint, it would be highly beneficial.

This can be achieved by natively integrating all SaaS security components, including inline controls, APIs, and SSPM, and by leveraging security policies that are no longer disjointed but based on the context of aggregated risk intelligence from the source of action to the destination. This enables automatic, precise responses to violations. Additionally, integrating a SaaS security solution within an overall security service edge (SSE) platform powered by zero-trust principles and collecting risk intelligence across a broader security ecosystem—from users and endpoints to applications and data—can further enhance security policies and response efficacy.

By leveraging additional context, a SaaS security solution can define and set more granular controls, allowing security teams to enable more automated workflows without compromising on risk. Ideally, not only should the policy framework be common across products, but the policies themselves should be unified across critical control points to work in tandem with data in motion, data at rest, and SSPM solutions for maximum visibility.

The true value of context-driven policies lies in empowering organizations to facilitate frictionless collaboration, minimize risks in real time, reduce alert fatigue, and provide valuable guidance. This approach benefits end-users by allowing them to work with fewer inhibitions and security practitioners by reducing the number of alerts they need to process.

Third-party application protection

As reported by Gartner, in the year 2023, 45% of organizations experienced third-party-related business interruptions during the past two years.

For context, every other organization today, large or small, gets a third-party application on board to help with routine tasks. A third-party application is created by a developer to be hosted by some other vendor. Third party here is also cross-referenced as supply chain, vendor-supplied, or outsourced software and can be associated with or consist of code, configurations, libraries, plugins, and other tools like code analyzers, repositories, monitoring, as well as other processes involved in software development.

The third-party software support market was predicted to cross US$1 billion in 2023. While digital transformation and cloud adoption had made the dependency on third parties indivisible, reality today is more and more applications are being created out of house. Not only do these applications enhance productivity, but they are also easy to onboard. The increasing support cost for legacy software is another root cause why organizations are looking for lower-cost third-party options. In other cases, benefits like customization and interconnectivity offered by third parties in marketplaces make it too sweet a deal to pass by.

While an organization can take all the possible measures to keep its security posture intact, it is difficult to assume that third-party software has been properly secured. In fact, software products, as they are created today, are an amalgamation of proprietary and open-source code. Third-party software is no exception; any software vulnerabilities or a gap between software development and release can be exploited by hackers or malicious programs.

There is more to the story. The SaaS landscape is vast, as we know, with multiple levels underneath. The same theory applies to third-party applications as well. We do have third-party applications connected to other managed applications; examples here could be MS Teams or Google Drive, also referred to as open authorization (OAuth) applications. In principle, they act as an intermediary on behalf of the end-user, sharing end-users account information with third parties without exposing the credentials, thus granting them access to certain resources associated with a user on another service.

That said, OAuth applications are flexible by design. What this means is when it comes to configuration settings and built-in security features, there are few mandatory details required for each grant type but for the most part they are optional. And this leaves room for authentication vulnerabilities and plenty of options for data ex-filtration. In fact, one of the most talked about data breaches of the year 2024 was based on OAuth applications, wherein bad actors leveraged OAuth applications as part of the attack against the organization's corporate environment.

Needless to say, an organization should assess the security measures implemented by the third-party vendor, monitor their security practices, and have contingency plans in place in the event of a data breach or other security incident, including an offboarding strategy involving timely revocation of access. Apart from taking proactive steps to invest in tools like SaaS security posture management, which can provide end-to-end visibility and control across applications—in-house, commercial, open source, third-party, or OAuth.

With a full view of third-party application inventory, security practitioners can draw conclusions on the health of the third-party portfolio, and other potential third parties involved. This could also give them the opportunity to get granularity on what is the actual enterprise readiness of these applications in question, including application categorization, required permission level, application vendor reputation, application risk evaluation, etc., and based on the findings, limit the access for third-party applications and/or other OAuth applications.

Other finer organization-specific permission configurations and the resulting risk score could then be a click away. Most importantly, if an incident occurs, the process can be followed by predefined custom rules on alerts for a third-party and OAuth application, with a step-by-step remediation instruction, all while ensuring compliance standards are adhered to. These predefined rules can also extend to security configurations for approving usage of third-party applications, so that security practitioners can proactively cap an application that is risky. By leveraging real-time lookup of APIs embedded with the applications in question, alerts can be instant and action taken immediate.

After all, implementing robust risk management processes enables organizations to identify vulnerabilities and address them before they can be exploited, especially for applications that are difficult to detect because of their cloud-to-cloud or API-to-API nature.

Unified visibility

With the increase in cloud adoption and migration of sensitive data to the cloud, SaaS applications have become a prime target for cybercriminals. IBM’s Cost of a Data Breach 2023 Report quotes that breaches due to cloud misconfiguration were one of the top causes among compromised SaaS applications.

With a hybrid workforce being the new normal and employees accessing SaaS applications from different geo locations, often via unmanaged devices, the attack surface has grown multiple folds. Verizon’s Data Breach Investigations 2024 Report found web application attacks were the most common external threat against SaaS applications, representing 50% of breaches.

Baseline is the growing complexity of SaaS environments, combined with incomplete visibility and control over security. With more than a few hundreds of SaaS applications in use on average, many containing sensitive data, it’s extremely difficult for security teams to effectively manage permissions, configurations, and security across their entire SaaS footprint.

IT teams require comprehensive insights into the usage, performance, and security of all their applications, either sanctioned or unsanctioned; that is where they will be able to gain maximum value on the investment. With a single vantage point wherein all the information related to the applications across the organization, from multiple sources and platforms, gets consolidated in a single dashboard, not only will they be able to present key metrics, usage patterns, and trends across the application landscape, but they will also be able to harvest as much context as possible out of SaaS applications to make proper security decisions. This same dashboard can be harnessed for risk assessment of applications and highly targeted real-time and data-at-rest policies.

In addition to deeper insights and better understanding of risk, the ultimate benefit to organizations is the ability to utilize risk-reducing policy controls, like user coaching mechanisms and self-remediation actions, in real time without impacting end-user productivity. This can help lower alert fatigue while increasing security efficacy.

With a full visibility of the SaaS landscape, organizations can effectively manage their application inventory, optimize resource allocation, identify potential security risks, and make informed decisions about their business applications.

After all, by having a complete view of their application environment, organizations can enhance operational efficiency, improve performance, and ensure a secure and well-managed application ecosystem.

CLOSE THE SAAS SECURITY GAPS

Cloud adoption will accelerate further in the days to come and with it the investment and associated complexity involved with cloud service delivery models, primarily SaaS. If organizations are aware of the challenges associated with SaaS adoption and proactively address any security concerns on SaaS applications, this relatively popular trend can help them enhance customer experience and accelerate business initiatives.

That said, there are a few measures an organization can consider undertaking to ensure a robust security posture:

- Leverage Modern Cloud Access Security Brokers (CASB): To unearth unauthorized and unsanctioned SaaS applications that are being used, and to consider continued usage versus replacement with better alternatives. CASBs also provide a single control point to manage risk across a set of cloud services (set policy, monitor behavior, and manage risk across the entire stack).
- Ensure Enterprise Readiness of Applications: Proactively recommend applications that are enterprise-ready and appropriate for business and technical needs, so that security standards can be maintained and timely deployment can be exercised.
- Benefit from Threat Protection: Take advantage of extended visibility offered by SSPM and advanced threat protection features offered by CASB to proactively defend against threats.

For more details, please visit the Netskope One CASB page.

Interested in learning more?

Request a demo

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.