WHITE PAPER

SIMPLIFYING SECURITY FOR SOFTWARE-AS-A-SERVICE

TABLE OF CONTENTS

INTRODUCTION

The growth of software-as-a-service (SaaS) companies has been crucial for both businesses and consumers to be successful in an ever-evolving digital world. With your main goal of solving a market challenge through automation and technology, you're able to save your customers significant time and money as well as quickly respond to changing needs.

Think back to the origins of your SaaS company. The founders strategized that the newly formed company needed to get to market and iterate to achieve product and market fit as rapidly as possible—which meant that code development was a priority and anything that got in the way of that was secondary. In fact, to this day, many companies continue to have this mindset.

However, a company's practices around usage and storage of personally identifiable information (PII) has become paramount to obtaining customer confidence and high retention rates, and a determining factor for large businesses and enterprises when purchasing a technology provider. Any issue that exposes the larger entity's environment or data could result in a loss of that relationship and even legal jeopardy if data is disclosed publicly.

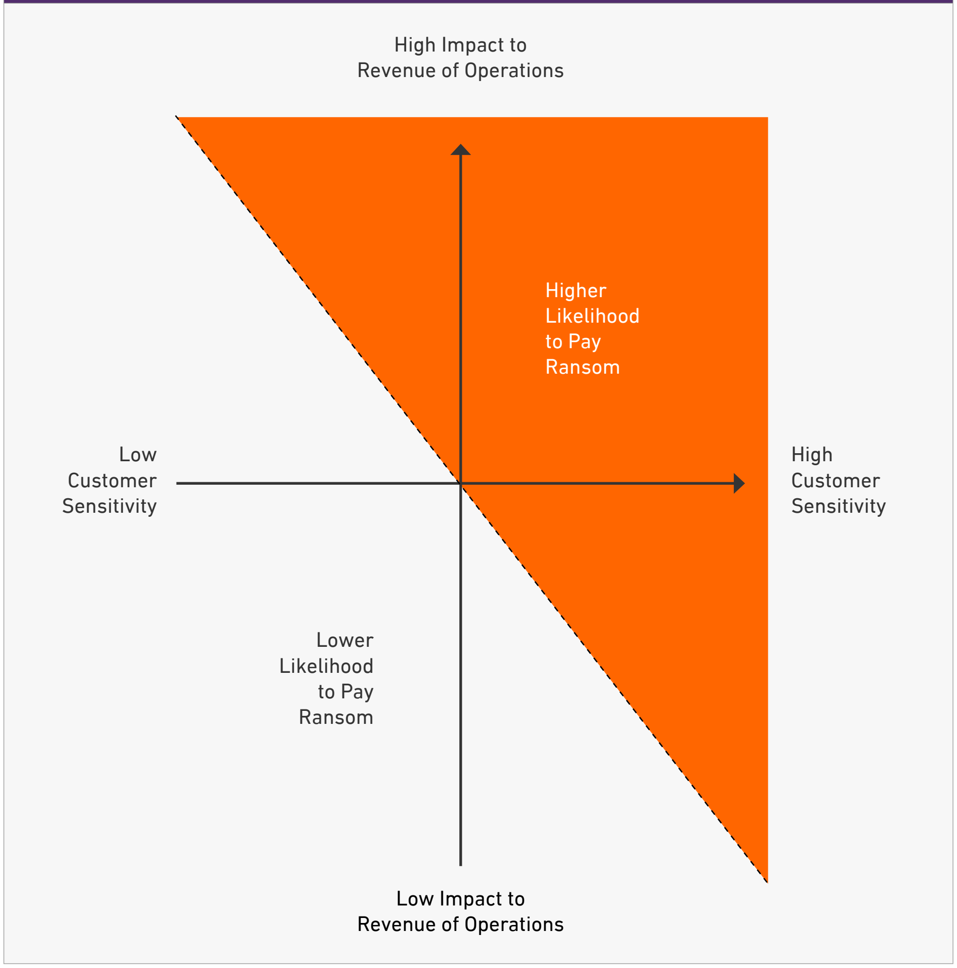
A narrowed focus on rapid iteration and improvement of your applications without a wider perspective of the impact to security and compliance could leave your business in shambles—if not bankrupt due to a breach.

THE THREAT LANDSCAPE SAAS COMPANIES FACE

Cloud-based software providers represent a compelling target for threat actors—as they manipulate and store hundreds or even thousands of customers' data. This raises the profile and appeal that successfully breaching the defenses of one of these providers can yield substantially more return, in terms of data acquired or applications and systems accessible for exploit (and access to partner environments in some cases).

As a result, there is much greater pressure to pay out ransoms rather than risk the loss of data or continued unavailability of services.

LIKELIHOOD OF PAYING RANSOM DUE TO THE ABSENCE OF A ROBUST SECURITY POSTURE


High Impact to Revenue of Operations
Higher Likelihood to Pay Ransom
Low Customer Sensitivity
High Customer Sensitivity
Lower Likelihood to Pay Ransom
Low Impact to Revenue of Operations

NOTABLE SAAS DATA BREACH EXAMPLES:	
Wolters Kluwer	Wolters Kluwer[1], a global tax and accounting software provider, experienced a malware attack, which impacted the availability of its software and delayed tax filing for firms across the United States. The IRS even made allowances to filers using the software who were concerned about missing IRS deadlines.
iNSYNQ	iNSYNQ[2], another accounting software provider, was hit by ransomware that locked out access to accounting firms across the country using its services. The ransomware encrypted accounting data for iNSYNQ's customers and limited access to its services.
apex Human Capital Management	Payroll software provider, Apex Human Capital Management[3], was infected with ransomware that crippled access to services. The "ransomware never touched customer data, but instead encrypted and disrupted everything in the company's computer systems and at its off-site disaster recovery systems." And though Apex paid a ransom, the decryption key did not work completely, which further delayed access to services and data.
zynga	Zynga[4], one of the most successful mobile game companies, experienced a data breach of account login information affecting more than 200 million players of Words with Friends and Draw Something.
DOORDASH	DoorDash[5], a popular food-delivery startup, reported nearly 5 million accounts were hacked, affecting customers, merchants, and workers' account logins and revealing the last four digits of credit card and bank account information.
f Cambridge Analytica	The Facebook & Cambridge Analytica[6] data scandal, in which Cambridge Analytica harvested the personal data of millions of people's Facebook profiles without their consent and used it for political advertising purposes, was a major turning point for data-driven companies and the use of data by third-party partners.

[1] Fazzini, K. (2019, May). A malware attack against accounting software giant Wolters Kluwer is causing a 'quiet panic' at accounting firms. Retrieved from CNBC: https://www.cnbc.com/2019/05/08/wolters-kluwer-accounting-giant-hit-by-malware-causing-quiet-panic.htm

[2] Krebs, B. (2019, July). QuickBooks Cloud Hosting Firm iNSYNQ Hit in Ransomware Attack. Retrieved from Krebs on Security: https://krebsonsecurity.com/2019/07/quickbooks-cloud-hosting-firm-insynq-hit-in-ransomware-attack/

[3] Krebs, B. (2019, February). Payroll Provider Gives Extortionists a Payday. Retrieved from Krebs on Security: https://krebsonsecurity.com/2019/02/payroll-provider-gives-extortionists-a-payday/

[4] Ivanova, I. (2019, October). Zynga Data Breach Exposed 200 Million Words with Friends Players. Retrieved from CBS News: https://www.cbsnews.com/news/words-with-friends-hack-zynga-data-breach-exposes-200-million-users/

[5] Ivanova, I. (2019, September). DoorDash Data Breach Exposes Nearly 5 Million Accounts. Retrieved from CBS News: https://www.cbsnews.com/news/doordash-data-breach-exposes-nearly-5-million-accounts/

[6] Wong, J. C. (2019, March). The Cambridge Analytica Scandal Changed the World - But It Didn't Change Facebook. Retrieved from The Guardian: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

For some perspective on how software companies are responding to cybersecurity threats, Microsoft spends more than a $1 billion each year on security research and development. A Microsoft executive recently quipped that his company is “the biggest security company you’ve never heard of.” Intacct is one of many enterprise SaaS providers that are addressing security issues with a variety of methods and recommended best practices, which the company detailed at its Advantage user conference[7].

We often find that many businesses develop an urgency to evaluate and make significant improvements to their cybersecurity program due to experiencing either a breach, as mentioned above, or changes in compliance regulations—whether that is the actual standard itself or new regulations that will impact the way in which they store and use customer data.

ACHIEVE COMPLIANCE

Security and data governance audits are less an optional state of checks and balances and more a legal and regulatory requirement these days. Therefore, the responsibility has shifted to technology providers to help deal with and prepare for some of these experiences. Increasingly, SaaS clients require records on IT security audits, clear-cut data storage, handling and protection policies, performance standards, and even risk management or disaster recovery plans. In other words, you may be initially audited by clients, in a way, before any legal audits take place.

More than proper planning and documentation, it helps to have these elements established long before your clients even ask, so that when the time comes you can provide the necessary assurances.

[7] Dunlapm, T. (2016, November). Enterprise SaaS Providers Step Up Security Measures. Retrieved from Computer Economics: https://computereconomics.com/article.cfm?id=2289

HERE ARE SOME THINGS TO CONSIDER FOR FUTURE AND PRESENT AUDITS:
Do you have a corporate security policy?
Is there a dedicated security team in place to handle events and failures?
Do you have a formal procedure for reporting a security violation or data breach?
Do you regularly conduct penetration testing or have a third-party handle the process? When was the last relevant test performed, and what were the results? What are you doing to remedy any flaws or vulnerabilities discovered?
Whether through external means or internal discovery, what are you doing to both identify and remediate vulnerabilities in your system and network?
How often are applications or software tools updated? What is the process for doing so and how does this affect security? What about customer or client downtime? How long will the update process take?
Do you have a process for announcing and sharing scheduled maintenance sessions?
Is there API access or external integration support? How does this relate to data security and protections?
Are all API units authenticated, data encrypted, and monitored?
How do you physically secure access to your data facilities or operations sites?
How do you comply with HIPAA, Sarbanes-Oxley, PCI DSS 3.0, GDPR, and other similar-level regulations? Do you have documentation to support this?
Are all your processes, including data backups, documented in full with details on how you handle operations?
How far does your disaster recovery plan extend? What will you do if your customers are affected by a breach? How will you continue to ensure their privacy and security?

In addition to data-specific regulations such as HIPAA for healthcare information or PCI for credit card data, most SaaS companies will need to be within GDPR (General Data Protection Regulation). This regulation is designed to protect businesses from overreaching and provide more assurance for EU citizens regarding personal data and privacy. The impact of this regulation on data security in SaaS companies is astronomical–especially as it's being set as a standard and replicated across the world in various other countries including Brazil, Australia, Japan, South Korea, and Thailand, and some U.S. states such as California.[8]

Since enterprise SaaS is not inherently a consumer-focused business, it's easy to think that GDPR doesn't apply, but it does and, in some cases, even on multiple levels. For some SaaS companies, the protections may extend to customers, a customer's customers, and beyond. This means that even if your company or business doesn't serve affected customers, but one of your clients or service users does, then you're obligated to comply where applicable.

Under GDPR, the purpose, nature, and storage duration of data must all be supplied and honored. That is, if you say you're going to keep data for a set amount of time, then you must immediately remove it after said period. You must also define and adhere to the type of data being processed, while also considering the responsibilities, rights, and requirements of customers who generally serve as the source or inherent "owner" of specific data sets.

This also extends to security protections. Customers must be informed of a breach or security issues as soon as the SaaS company is aware of it. Providers must ensure that protections are in place to prevent data breaches and fully secure customer information. Failure to do so will result in hefty fines.

[8] Simmons, D. (2019, January). 6 Countries with GDPR-like Data Privacy Laws. Retrieved from comforte Insights: https://insights.comforte.com/6-countries-with-gdpr-like-data-privacy-laws

UNDERSTAND INHERENT RISKS IN THE CLOUD

To properly vet risks to your cloud environment, you must first understand the two types of security threats that greatly impact any data-driven company—accidental (misconfigured cloud environments, potentially exposing an application or data to an exploit) and intentional (malware attacks, phishing, and social engineering in attempts to compromise applications).

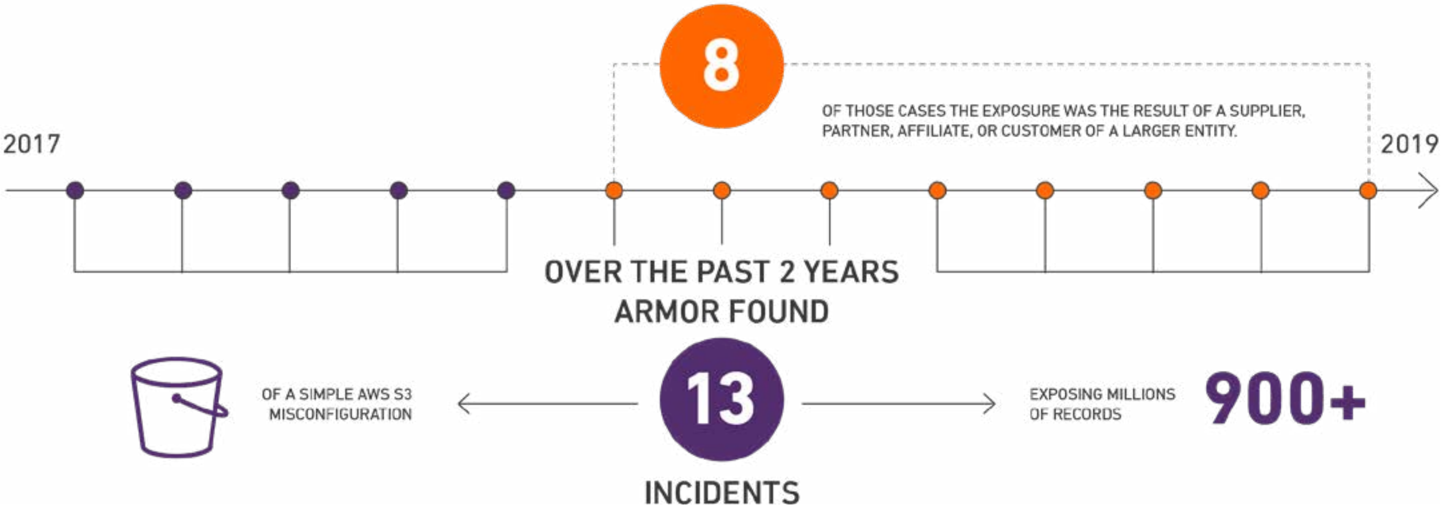
ACCIDENTAL

Armor conducted research covering large-scale data exposures over the past two years. We found 13 incidents of a simple AWS S3 misconfiguration exposed over 900 million records[9], and in eight of those cases the exposure was the result of a supplier, partner, affiliate, or customer of a larger entity.

Approaching accidental threats begins with a development process that joins the application development and security teams and leverages automation to simplify security and expedite deployment. Bolstering that approach means taking the defense-in-depth approach from traditional on-premise environments and moving that mentality to the cloud.

Integrating the right security tools into the development lifecycle instead of bolting them on afterward, SaaS companies can add another layer of protection to their cloud applications and environments. Doing this well enables them to address the challenges of misconfigurations, bugs, and other vulnerabilities before an application is in production.

This layered approach should also include cloud workload protection platform (CWPP) technologies, which provide host-based protections such as workload behavior monitoring, traffic visibility, and anti-malware scanning. The prospect of increased integration between CWPP capabilities and the scanning and remediation capabilities of cloud security posture management (CSPM) tools deepens the ability of users to maintain security and confidence as they continue to move towards the cloud.


8
OF THOSE CASES THE EXPOSURE WAS THE RESULT OF A SUPPLIER, PARTNER, AFFILIATE, OR CUSTOMER OF A LARGER ENTITY.
2017
2019
OVER THE PAST 2 YEARS
ARMOR FOUND
OF A SIMPLE AWS S3 MISCONFIGURATION
13
EXPOSING MILLIONS OF RECORDS
900+
INCIDENTS

[9] Armor. (2019, April). Naked Data. Retrieved from Armor: https://armor.com/white-papers/naked-data

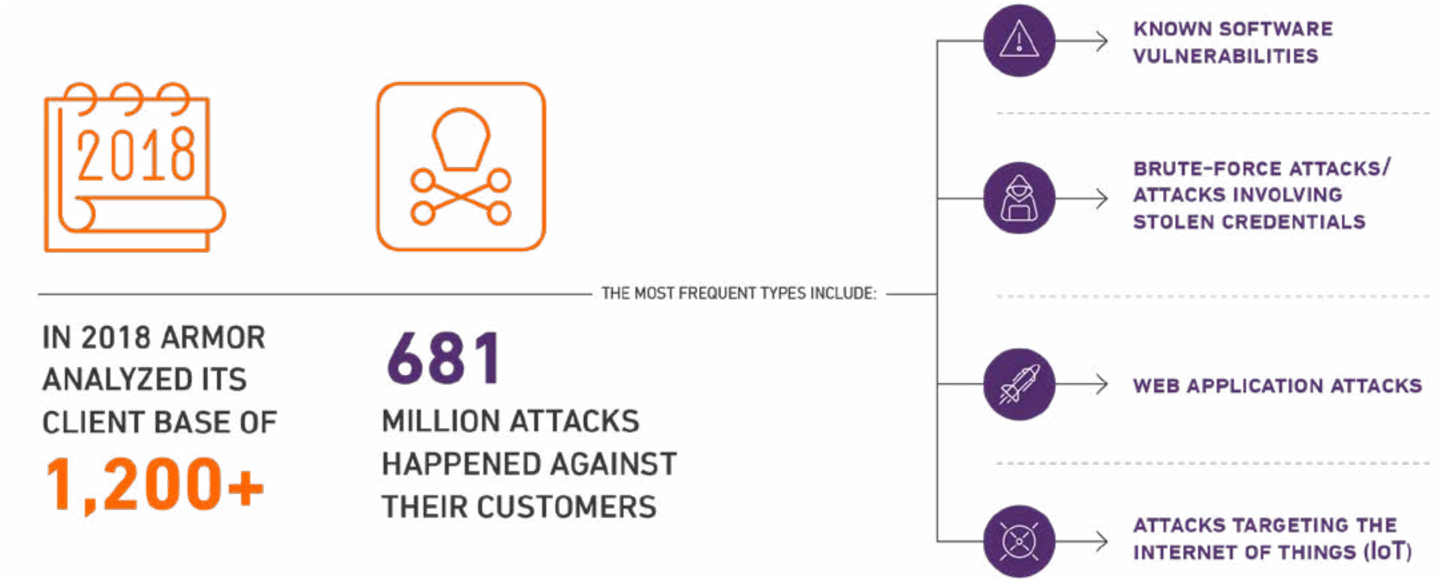
INTENTIONAL

The cloud is a hot commodity for threat actors. In fact, in an analysis of Armor's 1,200 clients in 2018, more than 681 million cyberattacks[10] happened, with the most frequent types including known software vulnerabilities, brute-force attacks/attacks involving stolen credentials, web application attacks, and attacks targeting the internet of things (IoT).

Armor's Threat Resistance Unit (TRU) expects even more in the future with an additional emphasis on distributed denial-of-service (DDoS) campaigns, exploits, targeted ransomware, sophisticated phishing campaigns, and attacks targeting containers and cloud services.

In addition to CWPP and CSPM tools, we recommend some additional strategies for SaaS providers to consider when securing their SaaS applications from accidental and intentional threats:

- **Implement strong identity and access management:** Whenever possible, multifactor authentication should be enforced and coupled with a policy that requires strong passwords.
- **Encrypt data:** Encrypting data at rest and in transit as much as possible adds an important layer of security. Accompany this with secure key management.
- **Bake security into the SDLC and DevOps processes:** Catching vulnerabilities earlier requires collaboration between security and development teams as well as using security technologies to scan for vulnerabilities before an application is launched.
- **Automate compliance and security:** Automation simplifies security and the use of compliance controls to ensure applications are operating in accordance with policies.
- **Prevent misconfigurations:** Automation and scanning tools can help with this process. Any error in security controls or access settings can result in the compromise of customer data as well as potential violations of compliance regulations.



IN 2018 ARMOR ANALYZED ITS CLIENT BASE OF 1,200+

681 MILLION ATTACKS HAPPENED AGAINST THEIR CUSTOMERS

THE MOST FREQUENT TYPES INCLUDE:

KNOWN SOFTWARE VULNERABILITIES

BRUTE-FORCE ATTACKS/ ATTACKS INVOLVING STOLEN CREDENTIALS

WEB APPLICATION ATTACKS

ATTACKS TARGETING THE INTERNET OF THINGS (IoT)

[10] Simmons, D. (2019, January). 6 Countries with GDPR-like Data Privacy Laws. Retrieved from comforte Insights: https://insights.comforte.com/6-countries-with-gdpr-like-data-privacy-laws

DEFINE YOUR ROLE IN CLOUD SECURITY

When considering security in the cloud, it's imperative that SaaS providers first understand the Shared Responsibility Model that each cloud service provider has articulated. The Shared Responsibility Model helps to clarify the boundaries between what security the cloud provider addresses (security of the cloud, i.e. infrastructure) and what the cloud customer is expected to address (security in the cloud, i.e. data).

Equally important, cloud customers must recognize that initial turn-up of cloud native security tools doesn't fully solve the security equation, and unfortunately, technology alone still doesn't solve the challenges of ongoing security operations and optimization. Teams, whether internal or from a third party, still need to review alerts, investigate their origins, and determine how best to remediate them on a 24/7/365 basis.

To get started, SaaS vendors must carefully weigh what security functions they are willing to take on and when, and how those decisions affect the ability to create new code and minimize the cost of additional rework. A brand-new "born in the cloud" startup SaaS may choose to outsource all their security functions to a third party who has the scale and expertise to protect their organization at a reasonable cost. A larger SaaS may have dedicated security staff in place and prefer to maintain a blend of internal security operations while leveraging third-party tools for analysis and correlation of events and subsequent alerting on areas of concern.

THINGS TO CONSIDER WHEN ESTABLISHING & OPTIMIZING YOUR SECURITY PROGRAM AS YOU SCALE:
Do you understand the Shared Responsibility Model and what your organization is responsible for in respect to security?
Is your organization subject to any compliance frameworks and, if so, do you understand how to address security controls for your workloads in the cloud?
Do you understand the various native tools and capabilities the cloud service provider offers that can help you secure your applications and data?
Do you understand both the advantages and limitations of these tools?
Have you identified additional security capabilities your organization will need to effectively secure your applications and data?
How does your organization plan to perform vulnerability scanning?
What will be the program for patching applications and systems to address vulnerabilities?
If you have or expect to have a blended on-premise, hosted and/or cloud environment, have you identified ways to unify security and visibility across that entire environment?
Who is going to monitor activity and alerting?
Who will be responsible for the review and investigation of alerts and determine how to respond and/or remediate them?
Who will be responsible for ongoing tuning and optimization of your security operations?

DECREASE TECHNICAL DEBT

While on your journey to iterate and scale securely, SaaS organizations must be ever vigilant against creeping technical debt, which can create friction and slow down future development efforts. From a security and compliance standpoint, technical debt is incurred when security and compliance controls are deployed "after the fact" or as a bolt-on versus as part of the application development process and/or scripted into automated controls.

For instance, if developers failed to consider security at the outset of their application development, it's possible the application may create a stream of vulnerabilities over time that have to be remediated. Technical debt can also be accrued when development teams, or even DevOps, turn on native cloud security controls without considering the alert management and response aspects to doing so, and as a result, they introduce risk to the organization. Or, in another example, a development team deploys a workload into the cloud and exposes a S3 bucket containing sensitive data to the internet. The data exposure puts the overall business and development on lockdown to resolve the incident and put new controls in place to prevent a similar recurrence.

For those SaaS vendors looking to security service providers to help them secure their sensitive SaaS applications and data, technical debt potentially introduced by the third parties should be considered a criterion.

> Technical debt ripples into all corners of cybersecurity, including authentication and IT infrastructure. As you create more technical debt you often slow things down and increase your overall level of risk.[11]
>
> — Sean Duca,
> Vice President & Regional Chief Security Officer,
> Palo Alto Networks

[11] Greengard, S. (2018, June). 5 Ways to Mind Your Technical Debt. Retrieved from SecurityRoundtable.Org: https://securityroundtable.org/does-your-organization-face-technical-debt

Leverage these questions in any discussions with third-party security service providers to determine the extent of technical debt they may introduce versus offset for your organization.

- Is the security services provider able to unify security across your full environment (cloud, on-premise, hosted, etc.) or just one area?
- How do the provider's offerings and roadmap address any requirements your organization may have for security across a 2-year horizon?
- Does the security service provider require deployment of hardware into your environment? How difficult is implementation and how long will implementation take versus a software-based solution?
- What is the division of responsibilities between provider and customer, and what specific aspects of ongoing security operations is the security services provider handling?
- Will staff have access to the security service provider's security and compliance staff?
- Is billing fixed or does it allow for consumption-based billing, aka "pay only for what you use?"
- How integrated are the underlying capabilities of the vendor's solution?

SaaS companies focused on running a tight organization that minimizes the introduction of unnecessary technical debt should align with vendors whose approaches to security are designed to do the same.

SaaS

SECaaS

Seek out security-as-a-service providers whose offerings share characteristics similar to SaaS models:

- Rapid turn-up of comprehensive security and compliance controls
- Software-based versus hardware-based
- Subscription models with consumption-based pricing

BUILD CREDIBILITY & CUSTOMER CONFIDENCE

SaaS businesses are operating in a crowded market. In this environment, a reputation for availability and security are vital to success. As cloud and SaaS adoption increases, SaaS vendors can expect to see the number of attacks targeting them and their services to continue to grow. Adopting the right security practices and leveraging tools that can provide protection, valuable metrics, and visibility into vulnerabilities enable them to tell a security story to their customers that other vendors may not be able to match.

Leveraging a recognized security and/or compliance provider can have the effect of boosting the SaaS provider's credibility with their own customer base. In fact, some SaaS companies actively promote their security partnerships with their customers to communicate that they take security of their sensitive data seriously. Conversely, the message also allows positioning for the SaaS provider from a market and investor standpoint. It shows that the SaaS is singularly focused on iteration and innovation of its offerings to increase affinity and stickiness, creating value for customers and growing market share.

Just as the cloud has democratized access to infrastructure and allows almost anyone within your organizations to quickly and easily deploy more software, we need to think of the democratization of security and how this extends a level of duty to everyone within the organization to own security. It's the old Spiderman adage: With great power comes great responsibility.

ABOUT ARMOR

Armor is a cloud security company that takes the complexity out of protecting your data, whether it resides in a private, public or hybrid cloud–or in an on-premise IT environment. We provide security-as-a-service solutions that give you a clear picture of threats facing your organization. This allows us to provide you with the people and security resources to stop attacks before they happen and react quickly and effectively when they do–keeping your data safe and compliant. Wherever you are on your cloud journey, Armor can help. We make cybersecurity simple.

ARMOR

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167