White Paper

Securing Your DevOps Platform

Software Pipelines, Middleware and Infrastructure for **SaaS Companies**

CloudOps
Own your destiny in the cloud
Cloud and code agnostic, but opinionated

423 rue Saint-Nicolas, 2e étage, Montreal, QC H2Y 2P4
1 (888) 796-8364 | info@cloudops.com | @cloudops_

Security Challenges Faced by SaaS Companies

Web applications usually accumulate large amounts of sensitive data, which makes SaaS companies particularly attractive targets for hackers. Entrusted to protect personal data provided to them by customers, SaaS companies have a responsibility to address security issues and safeguard information in order to minimize the risk of breaches and maintain the trust of their customers.

More and more SaaS customers demand concrete information about the procedures and controls that a SaaS business has in place. SaaS customers are becoming more educated and concerned about the security risks of their information. They are asking questions like:

- What are the authentication and access control policies?
- What encryption policies will protect their data when it is transferred or being stored?
- How does multi-tenant hosting impact data? How can it be ensured that the SaaS' security policy will match their own?
- Are my APIs and underlying infrastructure secured?

It is quite common to see RFPs for SaaS solutions seek independent third-party assurance, such as Service Organization Control (SOC) 2 Report and Cloud Security Alliance (CSA) STAR, for security certifications or controls for the SaaS business. This may guarantee high availability levels, ensure processing integrity, and provide sufficient confidentiality/privacy protection.

Nowadays, SaaS companies are expected to offer transparency when they learn about a security infringement. In Canada, as part of the Digital Privacy Act, fines may reach up to $100,000 per violation when an organization violates the breach notification requirements.[1] In the U.S., several new bills were introduced to Congress. If they become law, company executives could face jail time for not reporting data breaches in a timely manner.[2] Europe has followed a similar path with the introduction of the General Data Protection Regulation (GDPR) that replaced the Data Protection Act 1998 in May 2018.[3] With this legislation and the increased news coverage of data breaches, companies cannot claim ignorance when it comes to broad cyber security. If they don't properly mitigate the risks against cyber threats and compliance obligations, they may face serious business and personal consequences.

While SaaS companies try to prevent data breaches, their ecosystem is constantly changing. There are multiple factors that make this task even more difficult:[4]

- 43% of organizations are pushing out changes weekly, daily, or continuously. The increased speed of change introduces difficulty in understanding and reviewing the security consequences. There is not enough time to conduct exhaustive testing or reviews and the risk profile changes constantly.
- Different programming languages and toolsets directly affect how engineering and security teams deliver and test. It is important to understand security risks at the language and library level. For example, JavaScript and other dynamic scripting languages, such as PHP and Python, are more difficult to check at build time than static languages, which means that more issues can escape, to be found only at runtime.

[1] On June 18, 2015, the Digital Privacy Act (also known as Bill S-4) amended Canada's private sector privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA or the Act), regarding the establishment of mandatory data breach reporting requirements.

[2] For example, bill H.R. 3806, the Personal Data Notification and Protection Act of 2017 (PDNP Act) and bill S. 1815, the Data Broker Accountability and Transparency Act of 2017 (DBAT Act)

[3] General Data Protection Regulation (GDPR), Europe.

[4] The 2017 State of Application Security: Balancing Speed and Risk

- As cloud platforms and containers are becoming the default infrastructure for SaaS companies, they introduce risks around identity and access control, untrusted images, security orchestration, container "breakouts" and other issues that stem from developers' ability to provision their own infrastructure on the fly. Security teams must catch up and understand these evolving architectures and how to keep them secure.
- External parties (auditors, penetration testers, vulnerability scanning services) and internal security teams are primarily responsible for security testing and assessments, while development teams and system architects are primarily responsible for corrective actions.

Most organizations are still heavily dependent on manual testing and reviews, including penetration testing and external compliance audits.

Every day, new attacks are launched that exploit another hidden weakness in cloud-based applications. This means new vulnerabilities are being exposed and exploited faster, at a pace that many organizations simply cannot match. This highlights the importance of compliance in supporting security programs and controls.

Does Security Compliance Provide a Viable Solution?

Access, storage and processing of sensitive data needs to be carefully controlled and may be governed under various regulations, Acts or industry standards such as ISO-27001, SOC 2 Report, CSA STAR, the Personal Information Protection and Electronic Documents Act (PIPEDA), Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI-DSS) and Health Insurance Portability and Accountability Act (HIPAA).

The SOC 2 Report concentrates specifically on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system. It is the most focused report for understanding SOC and how they are tested. SOC reports can be either Type 1 or Type 2. A Type 1 report describes the controls and auditor's opinion at a particular point in time. This is usually the starting point that establishes the controls design, how often you perform certain activities and how certain processes are performed. A Type 2 report contains the auditor's opinion of how the SaaS provider is performing those activities over a period of time (i.e., typically six months or longer). Historically, only large and established SaaS players obtained SOC 2 Reports, but as SaaS customers better understand the scope of the SOC 2 Report, the demand for compliance affected every size of SaaS company.

Security for SaaS companies is not a straightforward task due to shared responsibilities. With the SaaS model, the responsibility for security can be split between four different levels (See figure 1):

1. There is the data centre/colocation facility, which covers areas such as physical security, power and HVAC (heating, ventilation, and air conditioning).
2. The IaaS (Infrastructure as a Service) provider covers responsibilities such as hypervisors, network, storage, servers, virtualization, and firewalls.
3. The application platform includes the runtime, the middleware, and the operating system. This tier typically consists of elements that are standardized even though the configuration is customized for a particular application.
4. The application level includes areas such as the application logic/code, programming languages, databases, transactions, external interfaces, and relevant security policies and processes.

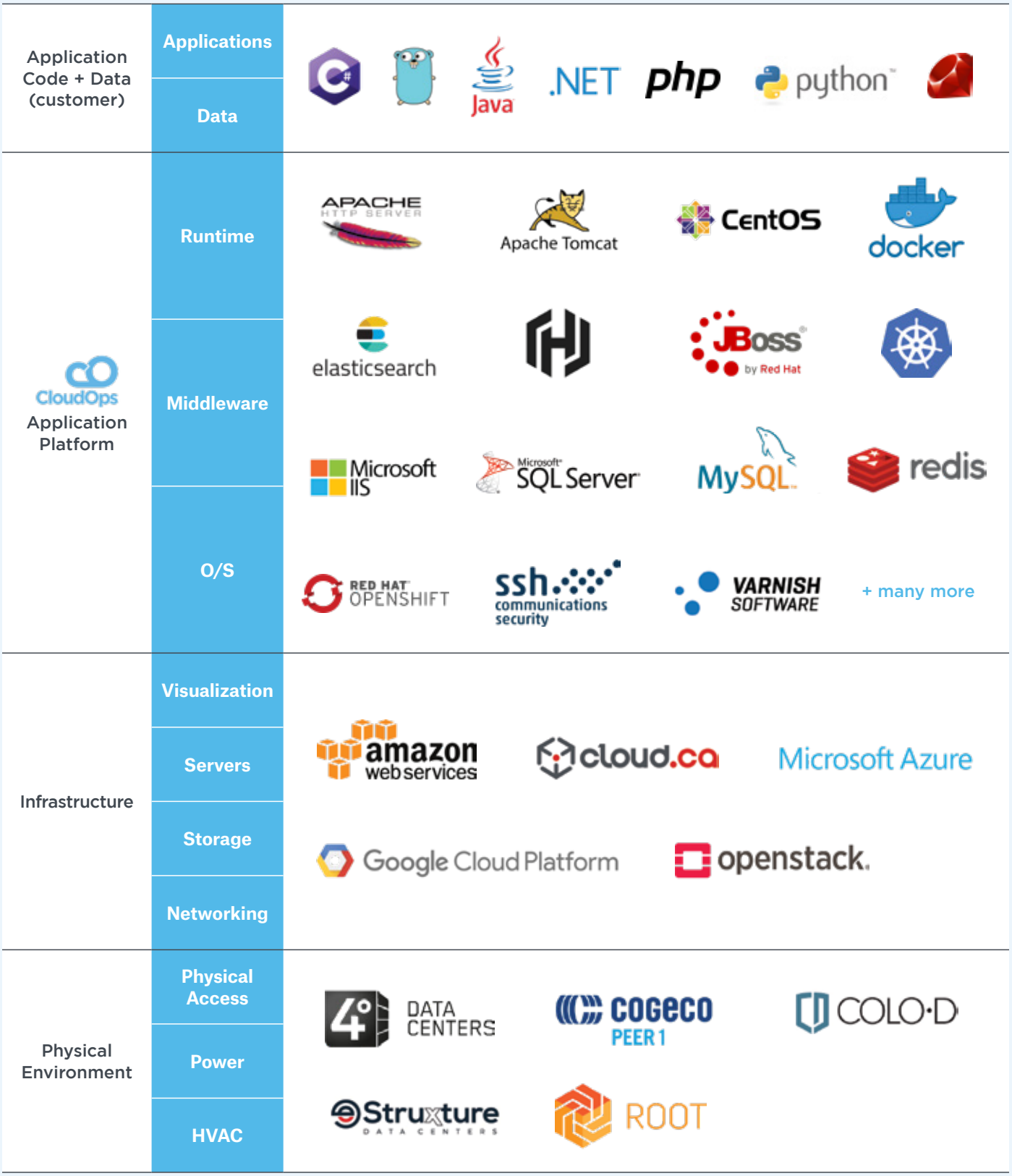

Figure 1: Realms of responsibility
(Source: CloudOps)

Being affiliated with a previously SOC 2 audited cloud IaaS provider or data centre does not offer the SaaS application a transitive level of compliance. Though a data centre or hosting provider may have a SOC 2 Report, this does not imply that the SaaS company has a corresponding SOC 2 Report that is relevant to their particular scope of services.

In fact, the SANS Institute's 2017 State of Application Security report argues that web applications running on the public cloud are the biggest source of data breaches (See figure 2 below), as reported in the past by the SANS Institute.[5]

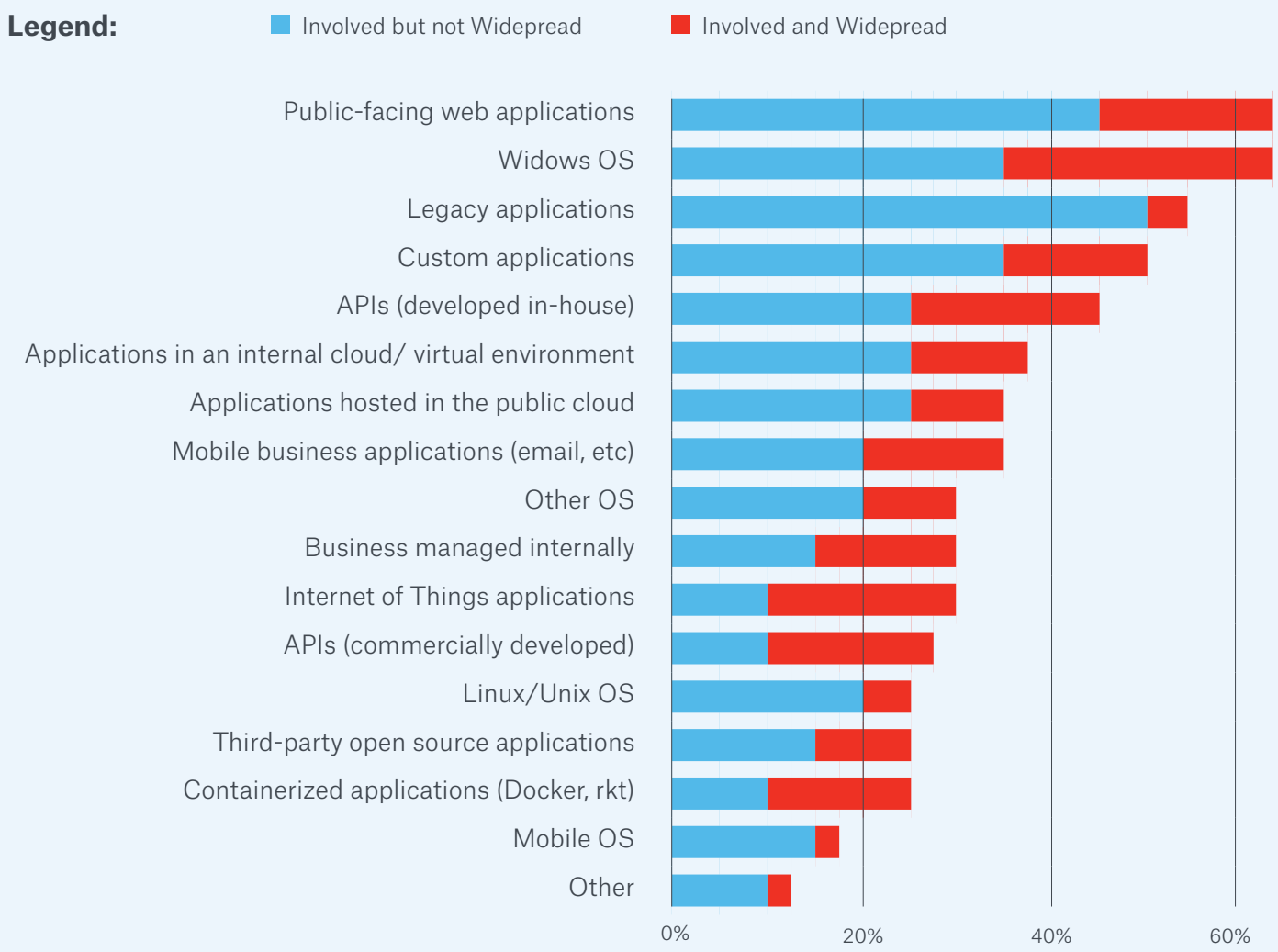

Figure 2: Applications/components involved in security breaches
(Source: SANS Institute)

[5] The 2017 State of Application Security: Balancing Speed and Risk, page 5.

When you break down the different types of attacks on web applications, you can see that 65% come from Cross-Site Scripting (XSS) and SQL Injection (See figure 3).[6] SQL Injection is used to access sensitive information or run operating system commands for further system access. In addition, Information Leak and XML Injection, can both lead to a disclosure of information.[7]

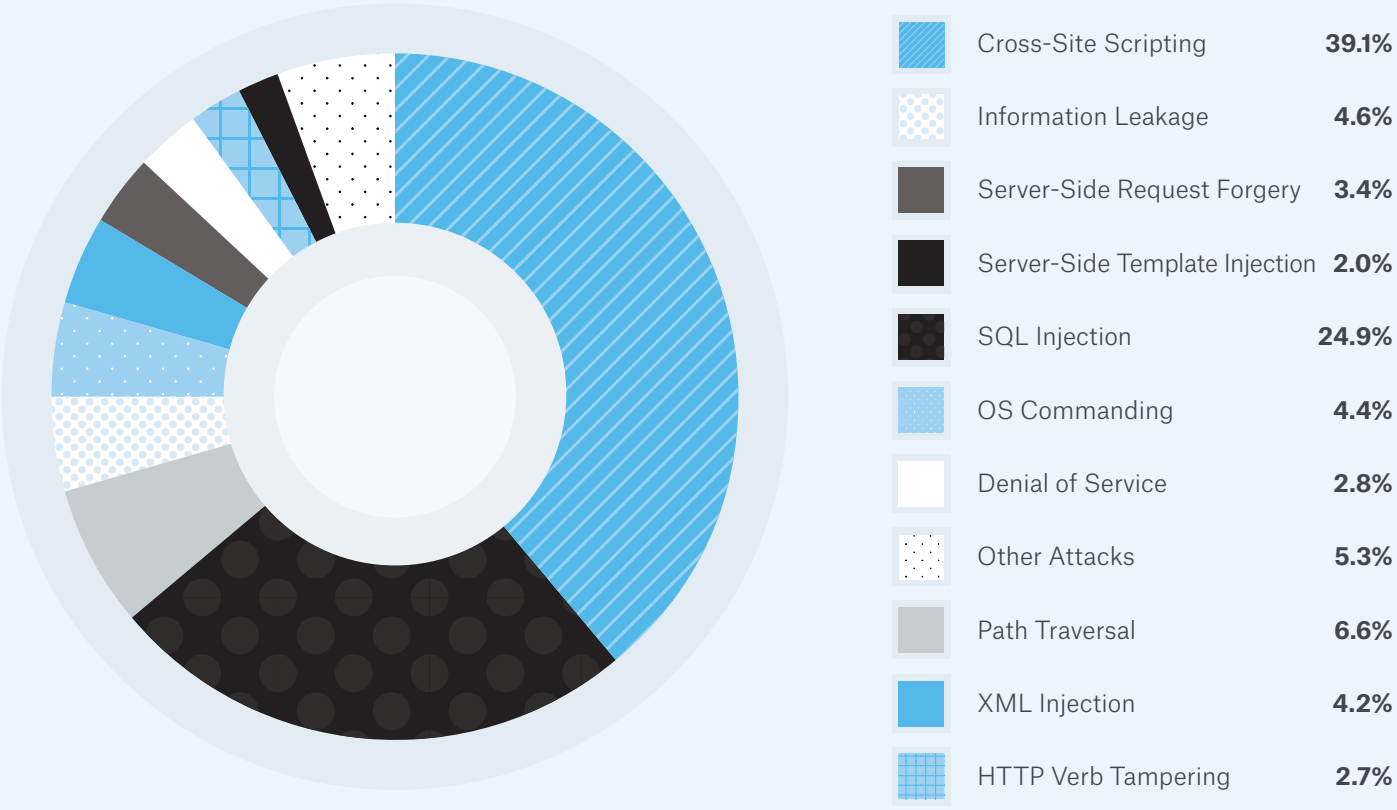

Figure 3: Distribution of attack types that are used against SaaS applications
(Source: Positive Technologies)

It is clear that the application code level is one of the most vulnerable layers. It is the sole responsibility of each SaaS company to be accountable and compliant to the relevant security certification, audit report, or regulatory requirements for the specific risks inherent in its deployment model and the potential security exposure specific to its case.

[6] XSS is a client-side code injection attack to exploit a vulnerability within a website or web application that the infected victim would visit.

[7] The Web Application Attack Statistics Q2 2017, page 5.

The Value of Industry Certification and Audit

When data breaches occur, companies are faced with negative publicity, decreased customer loyalty and lost revenues. The Ponemon Institute has indicated that cyber attacks are becoming more costly every year. The global average cost due to damage or theft of IT assets and infrastructure increased from $879,582 to $1,027,053 in 2017 alone. Likewise, the average cost due to disruption to normal operations increased from $955,429 to $1,207,965.[8] Looking at the top countries based on cost of data breaches per capita,[9] the U.S. takes the first place, followed by Canada and then Germany.[10]

Using an industry certification program or external audit report enables a SaaS company to ensure the highest security procedures and controls and minimize security risks. Industry certifications, such as CSA STAR or audit reports such as SOC 2, rely on proven security controls that in turn help minimize and prevent the cost of data breaches. Certifications and external audit reports also bring indirect added value to the SaaS company:

- Certification and external audit reports can drive new sales or at least ensure that security is not a hindrance to new business. Having a detailed audit report can be a deciding factor in whether a client is comfortable using your SaaS platform.
- Awareness that your business adheres to the highest security standards in the industry increases client trust and encourages pride in being part of your community. This may lead to higher levels of customer loyalty and acquisition.
- Certain industries/prospects have audit and compliance requirements (e.g. HIPAA for healthcare, PCI-DSS for eCommerce) that can only be met with a third-party security audit and certification. The various security frameworks offer an exhaustive inventory of possible security requirements that could be applied to SaaS companies.

Reputable industry security certifications and external audit reports can minimize the number of responses to security due diligence and audit requests from customers or prospects, dramatically reducing a SaaS company's overhead, service delivery risks, and costs.

Options to Secure Your DevOps Platform

Now let's assume that we have decided to build and operate a DevOps Platform following best practices to obtain a SOC 2 Report. There are two ways to go about it:

The Do-It-Yourself (DIY) Approach:

This option requires as prerequisites having knowledgeable in-house security resources to purchase the required hardware and software and to have the expertise to define security controls. In-house experts should define the controls and procedures based for SOC 2, set up and configure the servers, select the software tools and establish the monitoring and the customization to ensure that all aspects of security controls are addressed.

This approach is usually implemented in the following use cases:

- The use of proprietary technology that does not fit with standard security tools/processes that are in use by third-party service providers.
- Security procedures requiring a high-level of customization and full control over the platform.
- An already established mature secure operations centre.

Many organizations lack the talent, tools, and expertise required to succeed in a DIY approach.

[8] The 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB), Ponemon Institute Research Report, page 2.

[9] The 2017 Cost of Data Breach Study: Global Overview, page 8.

[10] Per capita cost is defined as the total cost of data breaches divided by the size of the data breach (i.e., the number of lost or stolen records).

The Managed Services Approach:

This outsourcing model, also called Security as a Service (SECaaS), provides management of the application platform, security policies, and general administration over the cloud. Security tools and their expert teams are constantly working to ensure compliance with the predefined security controls and meeting the SOC 2 Report requirements. It is still important to highlight that application developers must own the security of the application code as they fall outside the responsibilities of the application platform.

The common use cases for this approach are when the organization hopes to:

- Focus primarily on developing code/products without being distracted by managing security operations and procedures.
- Reduce high investments in building and maintaining the application platform, security tools, and extensive team training.

Cost Analysis

In order to compare the DIY approach with the managed services approach, we selected a profile of a typical SaaS company and conducted a cost analysis based on the following assumptions:

- The SaaS company collects personal or sensitive information from their customers or partners.
- The company is committed contractually to reach certain security obligations.
- A SaaS company would like to gain a SOC 2 Report in order to strengthen its market competitiveness.
- The company has fewer than 100 employees or contractors on its payroll.
- The company does not have dedicated cyber security staff or has only one person who is a partially dedicated resource, but this person does not have security experience with SOC 2 Report controls or complete knowledge of the process.
- The company has few documented security policies or defined procedures in place.
- The company has implemented few basic traditional security tools to detect security events or vulnerabilities.

Now, let's compare the estimated costs of obtaining a SOC 2 Report in the two types of implementations. The cost analysis calculation takes into consideration the following aspects:

- Costs are split according to when they occur, either only in the first year (i.e., one-time costs) or during subsequent years on an annual basis (i.e., recurring).
- As SaaS companies are not all the same, we have created a range of expenses: starting from a SaaS company that is an early startup (i.e., low-end) to a SaaS company that is a more established organization (i.e., high-end). This may also depend on the company size and complexity of its cloud security scope.
- The costs were calculated separately for internal HR effort, consulting fees, tools, and auditor fees.

Here's the cost analysis explanation comparing DIY (see figure 4) and managed security services (see figure 5):

DIY

	ONE-TIME COSTS	RECURRING LOW-END	RECURRING HIGH-END
Internal HR effort	$15,000	$40,000	$90,000
Consulting fees	$15,000	$3,000	$6,000
Tools	$5,000	$15,000	$30,000
Auditor fees	$15,000	$10,000	$50,000
TOTAL:	**$50,000**	**$68,000**	**$176,000**

Figure 4: Cost estimation[12] for DIY implementation of SOC 2 Report controls for Security and Availability[11]
(Source: CloudOps)

Managed Security Services

	ONE-TIME COSTS	RECURRING LOW-END	RECURRING HIGH-END
Internal HR effort	$5,000	$25,000	$50,000
Consulting fees	$5,000	$2,500	$2,500
Tools	$4,000	$5,000	$10,000
Auditor fees	$7,000	$10,000	$42,000
TOTAL:	**$21,000**	**$42,000**	**$104,500**

Figure 5: Cost estimation for managed security services implementation of SOC 2 Report controls for Security and Availability[12]
(Source: CloudOps)

[11] The cost estimation is based on a dozen implementations of SOC Type 1 and 2.

[12] The cost estimation is based on SOC 2 Report with CloudOps DevOps-as-a-Service offering.

Internal HR Efforts

It can be difficult and time-consuming to stay up to date with the ever-evolving requirements for security compliance or SOC 2 controls. Once you start implementing new security procedures, the company is committed to routinely conducting the required testing or monitoring. This often brings a need for new hires, sometimes even enough to equip a 24/7 team. Some of the internal costs of maintaining compliance for security programs in the DIY approach include hiring and training staff.

For many SaaS companies, it makes sense to hire a third-party SECaaS provider in order to focus on software development and the creation of code and avoid being distracted by managing certain security controls and procedures. These external resources have the necessary expertise and they keep current with the latest regulations and compliance requirements. If the SaaS business grows, outsourced resources can scale immediately to address new needs. The opportunity of having multi-skilled people that serve more than one team, or more than one purpose, is becoming a necessity in today's cloud environments.

Consulting Fees

Traditionally, we see that even organizations that choose to go with the DIY approach require some initial support from external consultants to either complement the skills that are available in-house or to validate certain internal decisions. As in-house resources usually do not have enough time to receive a refresher about the changes in the security program, an expert is often hired to advise the in-house team that would be responsible for the majority of the work. This means that some external consulting fees would be needed for a DIY approach.

When managed security services are implemented, most of these consulting fees are saved, as the professionals that provide the service are up-to-date with the latest security control requirements and how to implement it. The only part that they need to address is the special considerations that are unique to the deployment of the specific SaaS business. This means that the consulting fees for the managed security services will be a fraction of the ones charged in a DIY approach.

Tools

In a DIY approach, the SaaS company needs to evaluate, learn, design, deploy, and manage the commercial security tools related to security monitoring, vulnerability detection, etc. In subsequent years, the company is expected to purchase and implement the security tools and pay maintenance.

With managed security services, the outsourced staff that support the SaaS business have deep knowledge of the required security tools. Depending on the SaaS company security control needs, some tools will no longer be needed as they would overlap with the tools of the managed security platform. This may result in a lower cost for tools in the managed security services approach.

Auditor Fees

While the DIY method requires that the SaaS company design and implement all security controls, in the case of managed security services, companies can reduce the cost of the external audit firm. The managed security services minimize compliance gaps by leveraging an already audited third-party platform that has a proven solution. This reduces the level of auditing for security controls already addressed by the SECaaS. By reducing the scope of audit that the auditors must address, the auditor fees shrink for the SaaS business.

All in all, first-year costs of a SOC 2 Report with the DIY implementation are estimated to be between $118,000 and $226,000. For subsequent years the cost estimate is between $68,000 and $176,000. Using the managed security services approach, the estimated cost for the first year of SOC 2 Report implementation is between $63,500 and $125,500, while subsequent years' cost estimate is between $42,500 and $104,500. Thus, when you use managed security services, the estimated savings in the first year can be between $53,500 and $100,500 compared to the DIY approach. In subsequent years, the estimated savings on the recurring fees would be between $25,500 and $71,500 per year.

Conclusion

Leveraging expertise from third-party managed security services organizations allows SaaS companies to:

- Quickly adopt cloud native security best practices and reduce overall cyber risk;
- Rapidly achieve reputable industry security audit reports, such as SOC 2, in order to help drive new sales;
- Reduce the need for additional staff, training and investment in security tools;
- Focus on developing new code and products, as opposed to managing security compliance programs;
- Minimize service delivery risk while lowering their operational costs.

In fact, the market for managed security services is growing at a fast pace. According to Allied Market Research, the global market is expected to garner $40.97 billion by 2022, registering a CAGR of 16.6% during the 2016-2022 period.[13] SaaS companies have found success leveraging third-party managed services.

[13] Managed Security Services Market Is Expected to Reach $40.97 Billion, globally by 2022.

About the CloudOps DevOps Platform
(DevOps-as-a-Service)

The DevOps Platform allows small to medium-sized businesses to take full advantage of the cloud and SOC 2 compliance. Our managed service allows your application to run the cloud configuration that will best meet your business and technical requirements as your organization grows, while lowering your security risks.

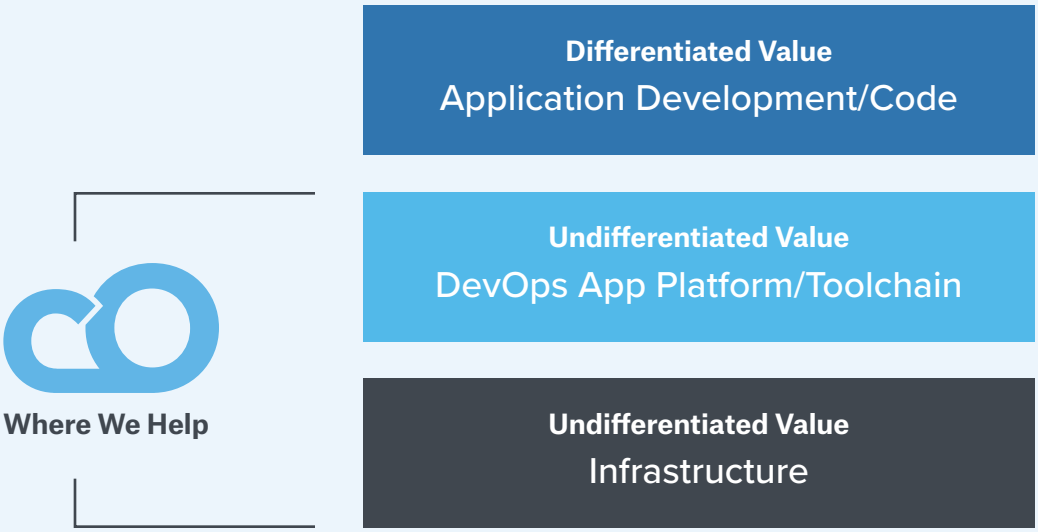

Figure 6: Differentiated vs undifferentiated value
(Source: CloudOps)

Technology stacks are comprised of three tiers: the application development, the application platform, and the infrastructure. In order to thrive, SaaS companies must focus their attention on their application development, where they must differentiate themselves in order to deliver differentiated value to their customers. In contrast, the application platform and the infrastructure deliver undifferentiated value. Their role is to provide application development with the self-service, utility economics, and API-automated continuous delivery of IT that cloud enables.

CloudOps' DevOps-as-a-Service helps you in the application platform, tool chain, and the infrastructure. Our DevOps teams support, manage, monitor, and automate the application platform you are running on 24/7. Our delivery involves assessing your requirements, defining your strategy, and then building your application platform or parts of your application platform. We build and manage high velocity application platforms that are comprised of scalable solutions and work across multiple customers and domains.

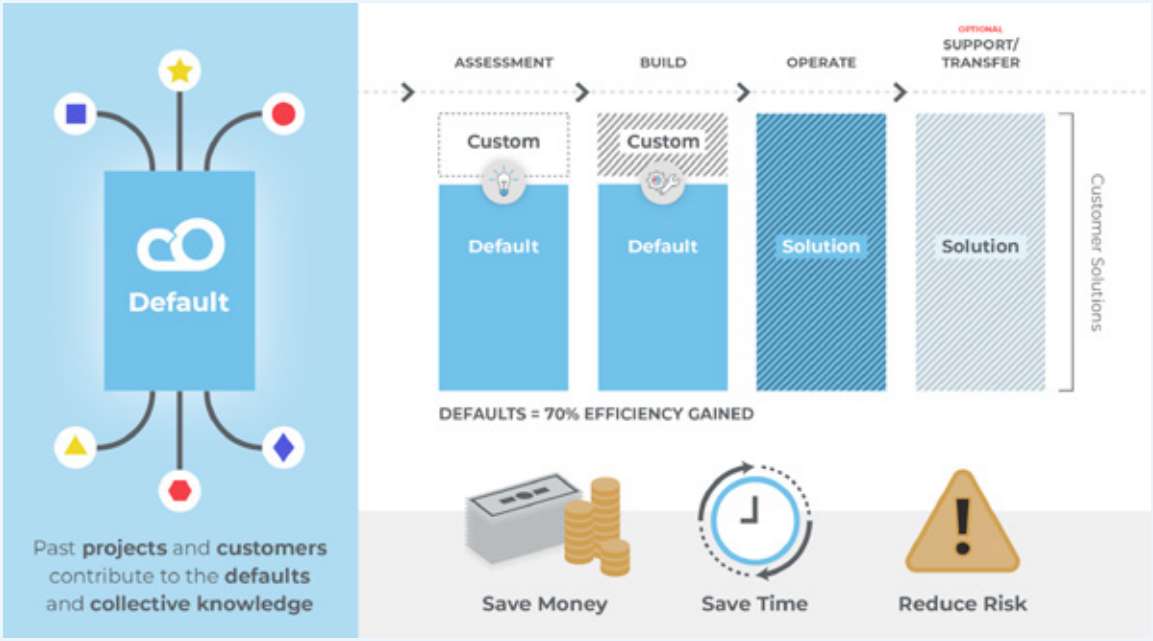

Figure 7: Defaults
(Source: CloudOps)

Our DevOps Platform benefits from the collective knowledge of a team of experts and the residual value of all projects that we have worked on. With every project, we improve shared libraries of automation recipes, which become default components that provide value to all platforms. These are complemented with components that are customized to customers' specific business and technical requirements. We provide faster time to value and the right expertise at the right time, allowing customers to focus on their application development without worrying about how to design and build their application platform and infrastructure.

CloudOps' services are all SOC 2 certified, meaning all systems have security mechanisms baked in. However, CloudOps' DevOps Platform has a SOC 2 Security option that will take additional precautions and includes:

- Systems administration
- Incident management
- Installation, tuning and optimization (device management including, in depth
- monitoring of instrumentation, notification and escalation procedures, runbook & customized operations guide creation)
- Security assessment
- Vulnerability scanning
- Security event monitoring
- Security as a Service (with SOC 2 Report)
- Network security - perimeter and network security
- Identity, log and Access Management (IAM), intrusion management
- Business continuity and disaster recovery (BC/DR)
- Adherence to service level agreements
- 24/7 support

The RACI chart below provides an overview of the areas of responsibility for DevOps-as-a-Service on top of AWS, Google Cloud Platform, Microsoft Azure, and cloud.ca. This chart is a high-level matrix of the activities and roles in the delivery of the application platform.

This RACI chart highlights who is **Responsible (R)**, **Accountable (A)**, **Consulted (C)** and **Informed (I)** for the different realms of responsibility.

Legend

Included in standard MAP offering	SOC 2 Security optional add-on

Application Development/Code

CloudOps	Application/Code Applications	Customer or 3rd Party
I	Application deployment and operations	RA
I	Application performance monitoring	RA
I	Application availability monitoring	RA
I	Architecture review and design	RA
I	Disaster recovery application restore	RA
CI	Backup restore testing	RA
I	Capacity or IaaS spend, management	RA
I	Application logging service	RAC
CI	Web Application Vulnerability	RA

Application Platform Operations

CloudOps	DevOps Platform/Toolchain	Customer or 3rd Party
RA	Guest VM/AMI + OS deployment and operations	CI
RA	Application platform installation and updates**	CI
RA	Application platform documentation	CI
RA	Backup execution and restore	CI
	Disaster recovery response*	CI
RA	Service desk for application platform and infrastructure	CI
RA	Identity and user access management (incuding secure multi-factor)	CI
RA	Application platform monitoring	CI
RA	Application platform availabilty	CI
RA	Server, local network and storage performance monitoring	CI
RA	Rigorous Incident Management for the application platform	CI
RA	Rigorous Change Management for the application platform	CI
RA	External Network Vulnerability Scanning	CI
RA	Internal Network Vulnerability Scanning	CI
RA	Vulnerability Management and Patching	CI
RA	Operating System Security Hardening (per supported OS)	CI
RA	Network Device Hardening (per supported network device)	CI
RA	Host Based Security Monitoring	CI
RA	Anti-Malware Management (per supported OS endpoint)	CI

** Recovery restore requires mutually agreed upon disaster recovery plan*

*** Application platform includes container orchestration*

Infrastructure Operations

CloudOps	Infrastructure	Customer or 3rd Party
I	Physical infra and host operations	RAC
	Hardware and hypervisor monitoring	RACI
I	Infrastructure and network availability	RAC
	Data centre security, power and environment	RAC
I	Network monitoring and operations	RACI

As can be seen, CloudOps' DevOps Platform places responsibility and accountability for the application platform in our hands. The SOC 2 add-on includes rigorous security mechanisms that have been audited by a third party and cover all known vulnerabilities.

Conclusion

SaaS companies have the responsibility to safeguard their customers' information, but this task is becoming more daunting each year amidst an increasingly chaotic landscape. Alongside widespread news coverage of data breaches, compliance requirements are becoming more stringent and urgent with heftier fines attached. SaaS companies are expected to put strong security mechanisms in place.

The SOC 2 certification is a gold standard for information security. It focuses specifically on non-financial reporting controls relating to security, availability, processing integrity, confidentiality, and system privacy. It comprehensively audits all systems and assesses potential vulnerabilities, helping prevent data breaches.

CloudOps' DevOps Platform can include SOC 2 certified processes for securely managing application platform components. This allows SaaS companies to focus on their application development while trusting the underlying health and security of their supporting application platform. Contact us for more information on how we can help build and operate secure application platforms.

CloudOps' is a cloud consulting and services company focused on helping customers own their destiny on the cloud. CloudOps uses open source cloud platforms and networking and offers multi-cloud solutions for software companies, businesses, and telecommunications providers.

423 rue Saint-Nicolas, 2e étage, Montreal, QC H2Y 2P4
1 (888) 796-8364 | info@cloudops.com | @cloudops_