CyberActive℠ SaaS

Differentiate and Protect Your SaaS Business with Cyber Security

Author:

Rajat Mohanty,
CEO, Paladion Networks

PALADION
HIGH SPEED CYBER DEFENSE

As businesses increasingly see the advantages of using the cloud and SaaS solutions, they become aware of the need to entrust important, even critical data to systems outside their direct control. For many organizations, SaaS solutions that can bring them benefit may also represent a leap in the dark when it comes to security.

"SaaS solutions that can bring enterprises benefit may also be seen as a leap in the dark when it comes to security."

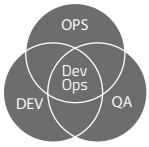
- Customers will demand that critical enterprise processes and the systems on which they run must be properly secured, whether they are in the cloud or in-house, and will look favorably on solutions that satisfy these requirements
- IT departments can reject SaaS applications whose security is lacking or cannot be proven, and they can instruct end-users to do the same for any end-user selected SaaS solution
- It only takes one security mishap in a SaaS solution to wreck the reputation of the solution and of the vendor providing that solution.

As a SaaS solution vendor, your business needs both the positive differentiation and the protection against negative impact, which good cyber security offers. Cybersecurity can help position your SaaS offering as the solution of choice for CIOs, their end users, and their enterprises. It also safeguards your own business throughout your SaaS solution life cycle – from initial design, through development and testing, to deployment, and ongoing end customer subscriptions.

"Robust cyber security can help position a SaaS offering as the solution of choice."

Customer Perceptions of Information Security and Privacy

Customer priorities for cybersecurity can include robust password and user privilege management, protection against attacks at different levels, and the ability to show others (internal auditors, their own customers, regulatory authorities) that adequate measures have been taken. A SaaS vendor may be asked to demonstrate how it ensures the confidentiality and integrity of information, as part of the customer's vendor selection process. However, security measures in turn must not compromise information availability or application performance and scalability. Difficulties in these areas will hinder the uptake of the SaaS solution, lead to premature cancelation of subscriptions, and can ultimately cause the business model of the SaaS application vendor to fail.



DevOps Methods and Technologies, and SaaS Vendor Cybersecurity

Market trends and competition between vendors lead to continual pressure to enhance cloud solutions. Ongoing streams of new features and functionalities characterize SaaS applications. In turn, they affect the methods used by SaaS vendors to develop and release their software. A SaaS vendor cannot afford numerous to-and-fro cycles of software releases that work in development, but fail in production, and that must then be sent back to development for fixing. The speed and frequency of new releases oblige many development and operations departments to work more closely together, notably by using a DevOps model. New security vulnerabilities may be created, but so are opportunities to strengthen security in ways that surpass older approaches in conventional IT application development and deployment.

"New SaaS life cycle approaches like DevOps can create new risks, but also new opportunities to strengthen security."

- **New technologies.** Microservices and containers represent two fundamental changes in the ways SaaS vendors can now build their applications. Both technologies allow increased support for continual incremental release of functionality. Microservices, as small, self-contained modules of functionality are incremental by nature. Containers reduce host server dependencies by pre-packaging applications together with the specific resources they need to run. As a result, containers can increase the chances of successful first time deployment of new versions of software. Security can be designed into both microservices and containers, so that they each carry their security with them. However, while simpler to handle at the individual level, care must be taken to protect against vulnerabilities caused by the overall complexity when large numbers of these items are used to form one overall solution.

- **Automation.** Speed and frequency of new releases also drive needs for automation in order to make delivery and deployment processes more efficient and more reliable. When robust security processes are also part of the automation, they can be automatically enforced at the different stages of code testing, deployment, and subsequent monitoring and measuring in production.

- **Continuous feedback.** When delivery and deployment are incremental and continual, they offer the possibility of continuous feedback. Problems, weaknesses, and attacks can be fed back into the development and delivery chain as they are detected for correction in the next release, which may be a short time away. A rapid cycle of release and correction can be an effective security measure in itself, reducing the window of opportunity for cyber attackers to exploit any vulnerabilities.

- **Design and development.** In traditional software development methods, security has often been considered as an afterthought, layered on after functional and integration testing was done, or added by hardening already developed blocks of code. Neither approach is aligned to the fast-moving world of SaaS releases in which physical data boundaries are fading and information can be anywhere; at rest or in transit between replicating servers in different locations. Instead of being added afterwards, security must already be built into software, starting at the design and development stages.

A SaaS Vendor Roadmap to Effective Cybersecurity

Cybersecurity must be effective both internally and externally. In other words, it must make a SaaS solution inherently secure, protecting it against information loss, corruption, abuse, and theft. At the same time, it should also provide measurable and demonstrable assurance to customers that their information will be safe.

A roadmap to meet these requirements can be defined in three parts:

- **Define your security posture** in a way that lets you implement security effectively and efficiently, while being able to describe your security measures clearly and convincingly to your customers.
- **Build and operate** according to your security posture with the appropriate processes, activities, and measurements.
- **Achieve relevant security certification** such as ISO 27001 and SOC 2 Type II, recognized by customers as guarantees of a measurable level of security, as well as relevant regulatory compliance.

Your Security Posture as a Vendor

There are two popular opinions about cloud security. The first is that cloud security often improves measurably on the security that customers have in their own on premise environments. The second is that cloud solution providers often lack transparency and are too secretive about their security measures and posture. Both opinions are grounded in truth.

"Customers find cloud solution providers often lack transparency about their security posture. Clear information helps customers feel confident."

Customers who want to feel confident about a SaaS solution provider's security can be reassured by clear information about how that provider handles:

- Integration of security into software development (architecture, code, releases)
- Testing of application and production environment security
- Segregation of data in a multitenant context
- Identity and access management
- Customer privacy policy
- Threat and vulnerability management
- Information integrity and availability
- Business continuity and disaster recovery
- Protection against internal or administrator abuse
- Security auditing

Proper planning and management of these items naturally prepares a SaaS vendor for security certification (see below.) Such certification can provide a shortcut or initial positioning statement to describe a vendor's security. However, a SaaS vendor will still need to describe and explain how it handles security on a practical, daily basis.

Building and Operating Secure SaaS Services

A robust security posture must have a correspondingly robust implementation in your software. There are two main areas to consider:

- Security of application code in agile design and development

- Security of the application and the full stack in test and production environments

While quality must be maintained, the lowest cost of effective, continuous security is also a factor. With these aspects in mind, each of these two areas are examined below.

Designing in Code Security

A SaaS business is built around software, typically developed using agile methodology and with constant stream of releases. A continuous code security program must dovetail with agile release management. Each time new code is checked in, it must undergo a code review using an appropriate combination of automated tools and manual testing. A code review software platform can be used, containing automated tools, solution repository and analytics, and integrated with the version management system to trigger security testing and review whenever new codes are checked in. By integrating the code review platform with the bug management system, the results of code security reviews can be logged for tracking and resolution.

These procedures and flows can be automated in the same way that 'builds' from software modules are automated as part of DevOps, and then sent to deployment management applications for distribution into a production environment. The code review software platform must also allow manual testing and the review of results by security software experts.

"SaaS security procedures and flows can be automated for greater efficiency and reliability."

As a result, SaaS development teams and their companies can:

- Architect the security components into software design
- Build in features to meet security and compliance requirements based on threats faced and industries served

- Maintain and grow an advanced code security platform with a repository of tools and test cases
- Make automated and customized reports and solutions available to developers for code uploaded to the platform for test.

Testing Application Security

As the software applications move through delivery stages or run in production, they must continue to be tested for vulnerabilities. A periodic testing program with a mix of high frequency tool based testing and longer interval manual penetration (pen) testing is often a suitable solution. As for code security during development, the test results should be seamlessly integrated with the existing bug reporting process, with fast resolution to match the agile application release cycles. Repositories of tools and test cases should also be available, as should the access for developers to test reports, analytics, and recommendations for solutions.

In particular, application security testing during staging towards deployment includes:

- Application Threat Modeling
- Walkthrough of the application by threat and compliance specialists
- Modeling of threat scenarios customized to each application
- Business logic testing for the integrity of results, as well as technical security testing for data confidentiality, integrity, and availability

Robust security testing for the application and stack adds:

- Network scanning, configuration audits, and application scanning of cloud assets
- Log monitoring of all assets

- User activity monitoring of your SaaS application
- Global threat intelligence applied to all cloud assets
- 24x7 monitoring of threats (attacks, misuse, abnormalities) and immediate response
- Daily vulnerability detection and mitigation
- Management of configuration, policies, and rules for the security controls that have been installed

Achieving Certification and Compliance

As a SaaS vendor, certifications allow you to showcase your security. They provide validation of your security systems and processes that is easy for a client to accept. Three types of certification stand out as being relevant and well-recognized:

"Security certifications provide validation that is easy for a client to see and accept."

- **ISO 27001.** This international standard from the International Standardization Organization (ISO) describes requirements for information security management in a company. So far (2014 figures), around 24,000 ISO 27001 certificates have been awarded overall.
- **ISO 22301.** This standard provides a framework for disaster recovery preparedness and business continuity management in your SaaS enterprise. Among other things, certification to ISO 22301 offers a guarantee to your customers that their information and your SaaS solution will continue to be available.

- **SOC 2.** Defined by American Institute of CPAs (AICPA); control criteria concerning security, availability, integrity, confidentiality, and privacy are audited for the data center in which your SaaS solution runs. SOC 2 certification can then be of Type 1 for one-time verification or Type II for continuing verification, making Type II the stronger version of SOC 2.

Cybersecurity as a Sales Differentiator

Correctly presented by articulate sales and security personnel, the methods, tools, processes, and certificates described above can all favorably influence customer buying decisions about your SaaS solution. With effective security management, a SaaS security platform can be used to demonstrate real time security and automated procedures to manage, risk, compliance, and unhindered development. This may also be crucial in satisfying auditors and allowing sales negotiations to proceed unhindered by audit requirements.

Conclusion

Cybersecurity affects the health of your SaaS business at several levels. Besides causing hurdles, exposing the Source Code of your proprietary product, putting your customers at risk and jeopardizing your business; it is also one of the criteria checked by many customers who will reject an offering they consider to be satisfactory for security reasons. Security certification provides a useful door-opener to start discussions with prospective clients in this case. Although as a SaaS vendor, you must have access to resources that can help you build your credibility in describing daily security procedures and precautions. A sound security posture from the start will facilitate such procedures and make it all the easier to convince customers that your SaaS solution is the right choice for them.

"The right security methods, tools, processes, certificates, and personnel can all favorably influence customer decisions about buying a SaaS solution."

PALADION
HIGH SPEED CYBER DEFENSE

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668

Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net