WHITE PAPER

Cyber Security for Competitive Advantage:

How SaaS Providers are Transforming their Business

NOPSEC

nopsec.com | hello@nopsec.com

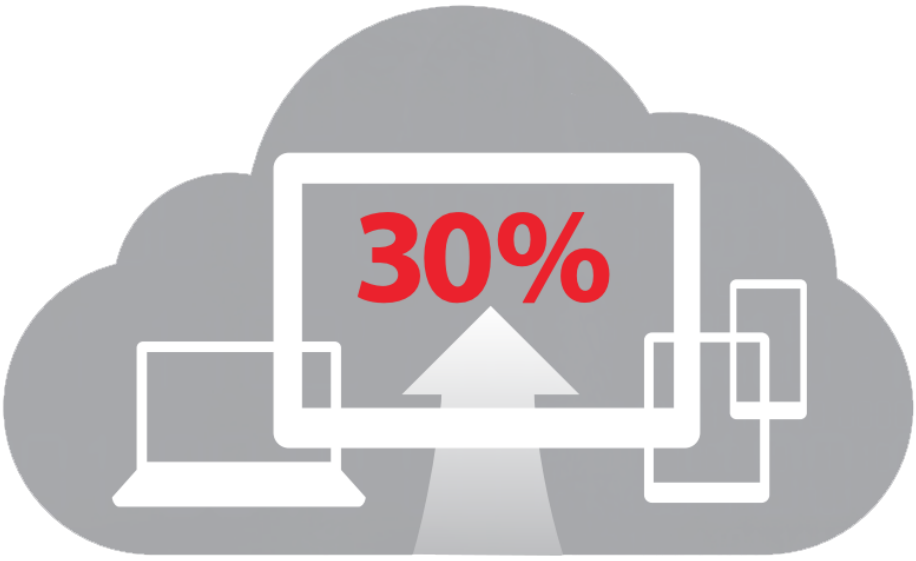
Table of Contents

Introduction

The move from internal premises-based apps to the cloud is transforming the way organizations work and how they engage customers. Globally, the growth trajectory continues for cloud computing – a market that is expected to increase 30% and reach $270 billion by 2020.

Within this increasingly crowded and competitive marketplace, the software-as-a-service (SaaS) model delivers on the cloud's promise of business agility. SaaS providers stake their success and reputation on two factors: uptime and security. Besides the availability of an application, security is the single biggest concern for organizations that are looking to engage a SaaS provider.

This White Paper examines the current challenges in demonstrating security compliance and how SaaS providers are using cybersecurity to radically differentiate their offering and transform their business.

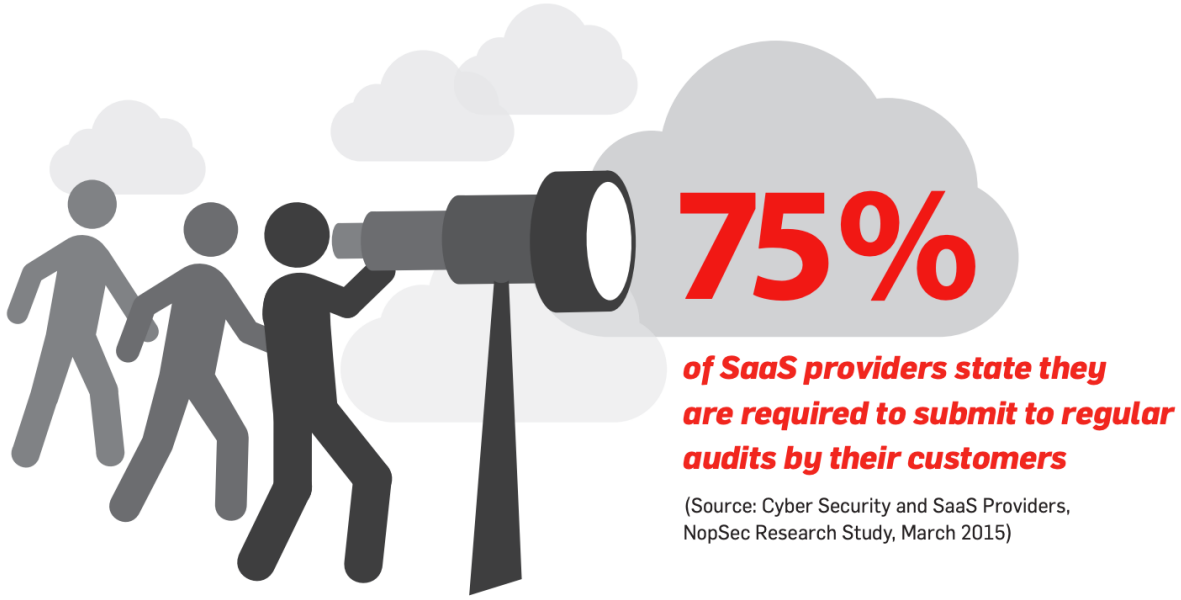


Regulators Require Security - And So Do Your Customers

In 2014, one in six breaches involved a third-party provider. Statistics like these make it more important than ever for SaaS providers to be able to demonstrate to prospective customers that they take security seriously in their dynamic cloud environment.

In addition, every industry has regulatory requirements and security best practices that they must employ to ensure compliance. In most cases, these requirements also extend to third party service providers engaged by organizations.

SaaS providers who not only implement strong security – but can also demonstrate the protection that's in place through third-party audits, penetration testing and other security controls – will have the advantage over providers who have no visibility into their cybersecurity posture and cannot exhibit proof of protection.



Cybersecurity Sets You Apart from the Pack

The multi-tenancy and shared infrastructures common in hosted cloud offerings understandably ignite additional security fears for organizations. The ability to calm these fears will set SaaS providers apart from the pack.

To address these challenges, SaaS providers may choose to partner with security vulnerability management vendors which, according to IDC, allows a SaaS provider's potential customers to assess the security posture of the cloud infrastructure they will be utilizing and provides consistency regarding the scans, assessments, and reporting.

of reported vulnerabilities in 2014 were identified in third-party applications.

(Source: National Vulnerability Database)

Build Time or Downtime

For SaaS providers, uptime is business-critical. Downtime in the cloud is visible and potentially damaging to the provider's brand because it affects multiple customers and companies.

That's why it's vital to build security into the process early on rather than having to fix it later due to coding or configuration vulnerabilities that were overlooked. Providing what users expect – the promise of always-on infrastructure – means eliminating all possible points of failure, and that is why building security into the cloud architecture from the ground up and testing and assessing for vulnerabilities throughout the development lifecycle is so critical for SaaS providers.

18

The number of security vulnerabilities per asset for SaaS providers

50

The average number of days it takes a SaaS provider to remediate a vulnerability

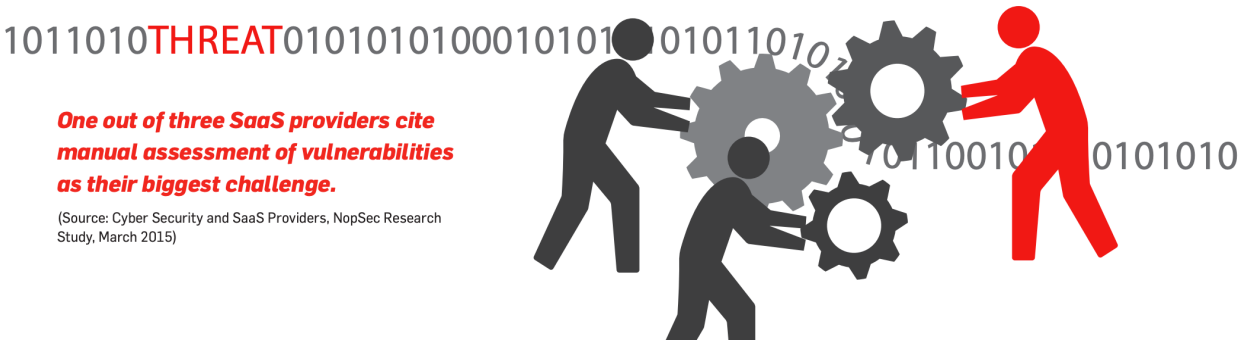
The Power of Automation

Without the detection and remediation of security vulnerabilities, any organization – SaaS providers included – will fall into a pattern of reactive security, responding to attacks only after they have occurred.

Manual processes are challenging and time consuming – and not very effective – in removing vulnerabilities from the cloud environment, given the thousands of paralyzing data points generated in the scanning process.

An automated approach to vulnerability management in the cloud environment helps to improve the effectiveness of detecting and addressing security vulnerabilities before they are exploited.

SaaS providers that implement automation tools such as NopSec Unified VRM can automate the process of finding, filtering, and fixing exploitable – and business-critical – vulnerabilities in their cloud infrastructures and applications.



One out of three SaaS providers cite manual assessment of vulnerabilities as their biggest challenge.

(Source: Cyber Security and SaaS Providers, NopSec Research Study, March 2015)

Taking the Lead

Security remains a top concern for organizations making a move to the cloud and is the main barrier to faster cloud adoption. For SaaS providers who rely so heavily on their Web-facing applications, this means ensuring those assets are immune from attack through integration of vulnerability scanning into the pre-production build cycle.

NopSec Unified VRM delivers ongoing risk assessments as a native capability within the software development lifecycle as well as continuous scanning in production environments, and on-demand visibility and risk-based reporting capabilities into the current state of security across web applications.

As the market for SaaS offerings grows and competition for services intensifies, SaaS providers who take proactive steps – including those outlined in this eBook – to address prospective and customer organizations' security concerns can differentiate their offering significantly.

NopSec Unified VRM delivers ongoing risk assessments as a native capability within the software development lifecycle as well as continuous scanning in production environments.

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or email hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions.

NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.

NopSec Inc. • www.nopsec.com • info@nopsec.com