SECURITY COMPASS WHITEPAPER

SaaS vs. On-Premise Solutions: Risk Implications

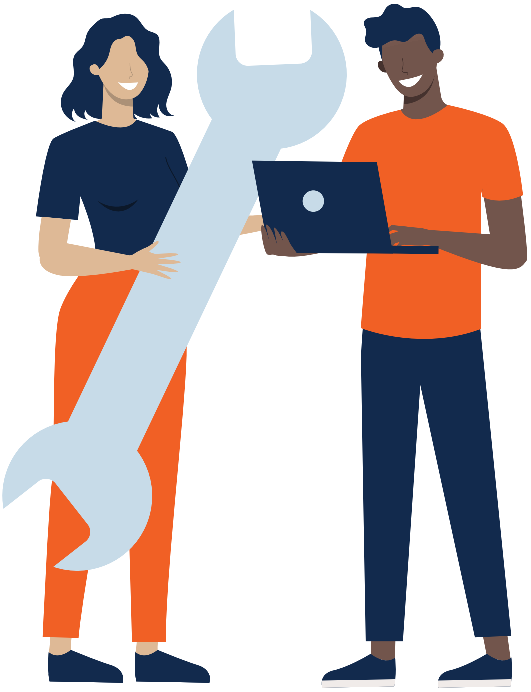
Security Compass

SD Elements helps organizations inject security early in the application development process. When used in a Software-as-a-Service (SaaS) model, questions often arise about the security implications of the information managed “in the cloud.” This whitepaper addresses the security, productivity, and financial implications of the deployment model.

Balanced Development Automation with SD Elements

DevOps teams use SD Elements to secure applications quickly and thoroughly, without burdening scarce security resources.

SE Elements uses a detailed and customizable survey to gather information about an application's technical stack and deployment environment and maps those to known threats and security controls. These controls are actionable tasks that include sample code and proven test plans to integrate security into the software development life cycle.



SaaS or On-Premise

The primary differences between running an application on-premise and a SaaS offering are where data resides and the responsibility for maintaining the application and deployment environment. Protecting that data is largely a matter of diligent security policies. These include:

Proper configuration: Security need not be complicated. Proper configuration of servers and applications can greatly reduce opportunities for attackers, yet recent research found that 51 percent of organizations publicly exposed at least one cloud storage service. As internal teams are stretched thin it can become a struggle to manage dedicated servers and datastores.

Identifying and prioritizing risk: Most threats to an application are inherent to the technology stack. Identifying these prior to starting a project allows development, security, and operations to mitigate risk as part of the application development process. The European Network and Information Security Agency (ENISA) published a list of common risks in cloud deployments across policy and organizational, technical, and legal categories.

Leveraging security resources: No organization has all the security experts it would like to have. A recent ISACA survey found that 62 percent of the respondents believe their organizations' cybersecurity teams are understaffed, and 70 percent said fewer than half of cybersecurity applicants are well-qualified. SaaS applications can leverage a vendor's security expertise and allow in-house security teams to focus on critical tasks.

Security implications of running SD Elements in the cloud environment

When considering a SaaS application, it is important to understand the criticality of the application, the information it manages, and the deployment model.

SD Elements is a low risk application

SD Elements does not require sensitive information such as source code, binaries, security test results, SDK, or URLs to operate. It has no direct interaction with operational systems or development code. As such, SD Elements presents low risk from an IT security perspective.

SD Elements does not scan for vulnerabilities

SD Elements is not a security testing tool. It does not scan applications to identify vulnerabilities or maintain a list of vulnerabilities. Instead, based on the technical stack and deployment environment, it identifies the controls required to prevent potential vulnerabilities.

SD Elements does not store identifiable vulnerability information

SD Elements can integrate with security testing tools including static and dynamic analysis solutions like Fortify, AppScan, Checkmarx, and Veracode. Rather than storing raw vulnerability information (e.g., URL, action, results for dynamic analysis or file name, line number, vulnerability description for static analysis), SD Elements maintains a vulnerability identifier from the tool.

It correlates these vulnerability identifiers with tasks SD Elements has determined are applicable to a given project. If a vulnerability identifier is suppressed through the scanning tool or does not appear in a subsequent scan, it is determined that a vulnerability has been deemed non-critical or remediated.

SD Elements stores limited personal information

SD Elements requires the names and email addresses of users to manage sign-ins, forgotten passwords, and for audit purposes. It also logs the IP addresses used on sign-ins for audit purposes.

SD Elements does not comingle customer environments

SD Elements runs in a single tenant environment. Each customer is assigned its own discrete computing service within the Amazon Web Services (AWS) environment, including a distinct EC2 instance and database. Computing services are controlled using industry best practices and not shared among customers.

All credentials are encrypted during transmission and at rest

The SD Elements application and API support only secure inbound communication over HTTPS/TLS 1.2. Outbound communication with other tools is controlled by user configuration and supports the use of secure transmission using HTTPS.

If a corporate Single Sign-On solution is used, SD Elements does not handle user passwords. Instead, it relies on the corporate Identity Management software to handle authentication. In password-based authentication, SD Elements employs BCrypt to salt passwords and multiple hashes to slow down potential brute-force attacks.

Software updates

While on-premise solutions require organizations to conduct upgrades and frequently lead to running out-of-date software, SaaS applications can be updated as frequently as needed. SD Elements updates are performed in a few minutes during scheduled off-hours maintenance windows, so users are always on the newest release. A study by IDG found that companies opting for cloud solutions reduced service disruptions by 72 percent.

SaaS or On-Premise – Which is right for you?

While on-premise deployments provide more direct control over an application, SaaS deployments can lower operating costs, ensure applications are updated quickly, and improve security. Whichever deployment model you select, our support team will work with you to ensure a successful launch and fast time-to-value.

Security Compass

Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt Balanced Development Automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on howorganizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
995 Market Street
2nd Floor
San Francisco, CA
USA 94103

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001