SaaS Security Checklist

A Guide for Information Security Professionals

identropy™

WHY SHOULD I READ THIS?

This eBook will help you, **the person in the organization who cares deeply about security and compliance posture of the company**, to regain some sanity amidst all of the SaaS chaos.

This eBook will help you think through a set of questions for each SaaS application you own. The questions are categorized based on risk type. Based on your organization's risk management framework, you may wish to add or remove categories.

- ✓ **Usage Risk**
- ✓ **Application Risk**
- ✓ **Data Security Risk**

AN INTRODUCTION

The advent of the SaaS delivery model for applications brings a new twist to the role of the CISO in managing risk. The threats posed by SaaS applications have changed the thread landscape considerably, and the new challenge for CISOs is to manage risk when a third-party is responsible for managing the defenses.

The CISO must ensure that risk is understood and that enterprise information security policies are adhered to in the cloud, as they are on-premises. The below checklist is meant to serve as a how-to guide for CISOs to understand and manage their risk from SaaS applications. Finally, a strategy to mitigate risk will be presented in the final step.

KNOW YOUR FOOTPRINT

Knowing what SaaS applications are being used by your workforce is often the first step.

Your inventory should include all SaaS applications in use even if they are not officially sanctioned. Data for the inventory can come from multiple sources, including:

BUSINESS STAKEHOLDERS

SURVEYS OF THE WORKFORCE

FIREWALL/PROXY LOG ANALYSIS

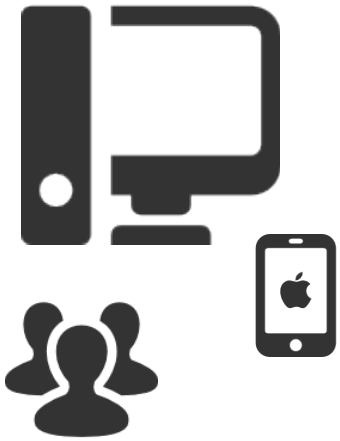
THE KEY WORD IS *RISK*

The ABCs of security apply with SaaS applications just as they do with enterprise applications. After inventorying your SaaS application footprint, you should quantitatively measure the risk an application poses. This will differ based on industry and applicable regulations but the risk profiling process used for enterprise applications is usually the same for SaaS applications.

It is important to define requirements. Ask the questions, “What data am I trying to protect and where is that data sitting? What risk and regulatory impact does each app contain?” Obtaining the answers will require collaboration with the owners you identified during the inventory.

If your enterprise lacks an existing risk profiling framework, take a look at ISO 27002. If you need more help, work with a consulting firm experienced in designing such frameworks.

- ✓ Is the application being used by the organization for a critical business function?
- ✓ What is the uptime SLA provided by the service provider?
- ✓ Does the service provider offer 24 x 7 phone support?
- ✓ Does the service provider provide a web-based console that reports on infrastructure status?
- ✓ What compliance certifications has the service provider obtained?
  - ✓ Safe harbor certification
  - ✓ SAS 70/ SSAE 16-3
  - ✓ PCI Compliance
  - ✓ CSA Security, Trust & Assurance registry (STAR)
  - ✓ Any other certifications?
- ✓ Where is the company's headquarters based?
- ✓ Where is the application physically hosted?
- ✓ Where is DR site physically hosted?
- ✓ What level of logging is built into the application and available to the customer via download or through a web application?
  - ✓ User to role/privilege mapping
  - ✓ Access request and granting
  - ✓ User activity
  - ✓ Administrative activity



- ✓ Does the SaaS application allow for anonymous usage? What areas require authentication?
- ✓ Does the SaaS application support SAML?
- ✓ Does the application support...
  - ✓ SCIM or SPML?
  - ✓ OAuth?
  - ✓ multi-factor authentication?
  - ✓ one-time password (OTP) feature?
- ✓ What type of password retrieval methods are utilized by the application? Static challenge/response? Dynamic knowledge-based authentication?
- ✓ Does the service provider offer an iOS or Android app? If so, is any data stored on the mobile device?
- ✓ Does a jail broken version of your mobile app exist that is available for download?
- ✓ Does the application provide a desktop client for data synchronization? If so, describe the type of data that is being synchronized.
- ✓ Does the application require any software to run on any of the customer's enterprise servers? If so, describe the function of the software and the nature of its communication with your SaaS application.
- ✓ Does the application support the automated import of identities (e.g. from Active Directory)?
- ✓ Does the application support authentication filtering based on device and/or IP address?

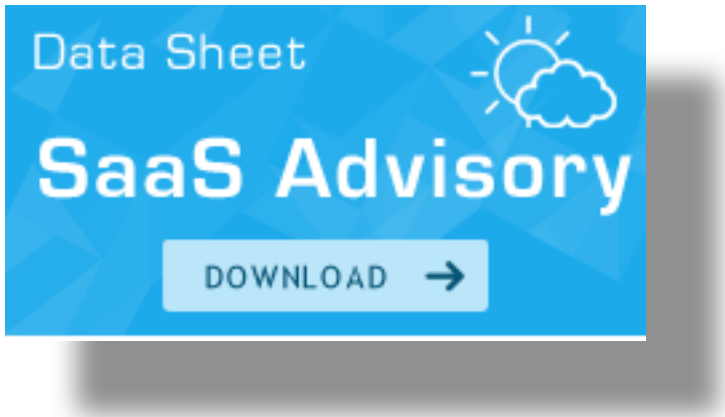
Has the SaaS application gone through thorough testing (as part of the Service Provider's development lifecycle) for the following security vulnerability categories:

- ✓ Information Gathering Vulnerabilities (search engine discovery, application discovery, error code information disclosure, application entry points, etc.)
- ✓ Configuration Management Vulnerabilities (file extension handling, old/ unreferenced files, access to admin interfaces, http and xst method enablement, ssl weakness, etc.)
- ✓ Authentication Vulnerabilities (user enumeration, guessable user accounts, brute forcing, weak password reset functions, browser cache weakness, weak 2FA, etc.)
- ✓ Session Management Vulnerabilities (bypassing session management schema, cookie attribute getting/setting, session fixation, cross-site request forgery (csrf), etc.)
- ✓ Authorization Vulnerabilities (path traversal, bypassing schema authorization, privilege escalation/role manipulation, etc.)
- ✓ Data Validation Vulnerabilities (cross site scripting, cross site flashing, SQL/ LDAP/XML/SMTP/code injection, OS commanding, buffer overflow, HTTP splitting, etc.)
- ✓ Denial of Service Vulnerabilities (SQL wildcards, locking customer accounts, DoS buffer overflows, user input as loop counter, writing user provided data to disk, too much data stored in session, etc.)
- ✓ Web Service Vulnerabilities (WSDL weakness, weak XML structure, XML content level testing, WS Naughty SOAP attachments, HTTP Get parameters/REST testing)

- ✓ Is all data encrypted in transit to and from the service provider? If only a subset is encrypted, describe the details of the delineation.
- ✓ Is data encrypted over the service provider's internal network?
- ✓ Is all data-at-rest encrypted? tokenized? anonymized? If so, please explain the process in detail.
- ✓ If encrypted, is it done at the mounted storage volume level? using transparent data encryption? at the file level?
- ✓ Is data encrypted on backup media?
- ✓ How are encryption keys managed? Does each customer have the option to manage their own encryption keys?
- ✓ If the SaaS provider will be managing the keys, what defined processes are in place for key lifecycle management? (key creation, deletion, storage, rotation, etc.)
- ✓ Do the provider's administrators have access to view the customer's data in clear text? Are there role-based processes in place to ensure that only the appropriate individuals within the service provider's organization will have access to customer data?
- ✓ Does the provider store PII (Personally Identifiable Information)? If so, how is PII data handled differently than other data?
- ✓ Is the provider's application a single-tenant or multi-tenant application?
- ✓ If multi-tenant, what steps have been taken to secure data from being accessed from other tenants?
- ✓ What kind of data can be obtained programmatically through an API? Identity attribute data? User access/entitlements? etc.

A SaaS Advisory Workshop Can Help You Gain the Visibility You Seek...

Identropy's SaaS Advisory delivers two key benefits:



- Gives you clear visibility into the SaaS applications that are currently being used in your enterprise
- Establishes a process to ensure that as new SaaS applications get adopted, they are quickly identified and rationalized into your Identity Management framework

You can contact us to schedule a call with one of our experts today.

www.identropy.com