White Paper
August 2015

IT@Intel
SaaS Security Best Practices: Minimizing Risk in the Cloud

We're making it safe to "go fast" when adopting new SaaS solutions.

Executive Overview

To support Intel business groups' increasing demand for software-as-a-service (SaaS) applications, Intel IT has developed several best practices that can help enhance SaaS security and protect Intel's intellectual property.

SaaS applications can provide efficiency and agility, cost savings, and enhanced collaboration especially with suppliers and customers. At the same time, SaaS applications present security challenges because they are typically hosted on third-party infrastructure and run third-party application code.

To minimize risk in the cloud, we have established the following best practices:

- Develop a SaaS security strategy and build a SaaS security reference architecture that reflects that strategy.
- Balance risk and productivity.
- Implement SaaS security controls.
- Keep up with technology development.

In our experience, SaaS security controls fall into the following categories:

- **Identity and access management controls.** These controls help ensure that SaaS applications are accessed by the appropriate users and only from approved devices.
- **Application and data controls.** As interfaces to data, applications must be registered and evaluated to determine whether they meet security requirements. Data encryption, tokenization, and data loss prevention techniques protect data and help detect storage or transmission of sensitive information. Data controls can be applied in real-time to cloud traffic or to content that is already stored in the cloud.
- **Logging and monitoring controls.** These controls help us detect information security violations, send alerts to the appropriate IT staff, initiate appropriate responses, and correct the situation.

Our SaaS security best practices enhance security, privacy, and legal compliance at Intel. They also make it possible for business groups to quickly adopt new SaaS solutions.

Shachaf Levi
Cloud and Mobile Security Engineer, Intel IT

Eran Birk
Principal Engineer Mobile and Cloud Security Architect, Intel IT

Esteban Gutierrez
Information Security Risk Specialist, Intel IT

Kenneth J. Logan
Data Protection Engineer, Intel IT

Jac Noel
Security Systems Engineer, Intel IT

Nooshin Zand
Security Systems Engineer, Intel IT

Carlton Ashley
Enterprise Security Architect, Intel IT

Thai Bui
Identity and Access Engineer, Intel IT

Paul Matthews
Data Protection Engineer, Intel IT

Contents

Contributors

Jerzy Rub, Information Security Risk Management Manager, Intel IT

Deanne Smith, SaaS Security Project Manager, Intel IT

Tarun Viswanathan, Enterprise Security Architect, Intel IT

Acronyms

DLP	data loss prevention
OTP	one-time password
SaaS	software as a service
SBI	security business intelligence
SCIM	system for cross-domain identity management
SMACI	social, mobile, analytics, cloud, and Internet of Things

Business Challenge

Public cloud-based software as a service (SaaS) has become a common delivery model for many business applications in use at Intel, including office applications and sales-and-marketing software.[1] As a result, Intel business groups, as well as external partners and customers, need Intel IT to support cloud-based SaaS applications.

SaaS is best suited for situations with the following requirements:[2]

- **Efficiency, velocity, and agility.** Business groups want to quickly adopt new applications as well as quickly change from one service provider to another.
- **Cost-effective.** Short-term licensing offers cost-saving opportunities.
- **Better collaboration.** Business groups want to collaborate with external customers, suppliers, OEMs, subsidiaries, and acquisitions.

Adoption of SaaS is part of Intel's social, mobile, analytics, cloud, and Internet of Things (SMACI) strategy, which is built on the following pillars:

- Enable movement of diverse information to more places.
- Accommodate growth in a variety of devices and Internet touchpoints, and through a range of access methods.
- Support more custom mobile applications and services within the enterprise.
- Adopt standard applications for SaaS in the public cloud.

[1] Although it is possible for SaaS applications to be based in a private cloud, for the rest of this paper, references to "SaaS" will assume public cloud-based SaaS.

[2] Software as a service is not appropriate for some use cases, such as handling top secret documents.

Solution

Intel IT recognizes the growing demand for and business value of SaaS solutions. SaaS solutions pose information security challenges, because they are hosted on third-party infrastructure and run third-party application code (both of which are out of Intel IT's control).

We are currently servicing 250 SaaS use cases with 139,000 users. Based on our experience with these use cases, we have developed a set of best practices for minimizing the risk of using SaaS applications in the enterprise.

First, we defined a strategy for SaaS adoption and built a reference architecture that reflects that strategy. We also determined how to assess risk and implement controls to help enhance security in a SaaS solution and protect Intel's intellectual property. We are committed to keeping up with technology development so that our reference architecture embodies best-in-class SaaS security. These best practices enable business groups to "go fast" while meeting security policy and privacy and compliance requirements.

Best Practice #1: Develop a SaaS Security Strategy and Build a Corresponding Reference Architecture

To securely and successfully adopt cloud-based SaaS applications in the enterprise, we first developed a SaaS security strategy that guides the rest of our SaaS activities. Our strategy embodies five steps:

- Educate the IT security team about SaaS, its use cases, and its functionality.
- Identify provider, tenant, and enterprise security controls, determine residual risk, and obtain business unit acceptance.
- Understand how to calculate and mitigate risk. See Best Practice #2: Balance Risk and Productivity.
- Define who is responsible for SaaS security controls and then implement them. See Best Practice #3: Implement SaaS Security Controls.
- Perform security reviews during the SaaS life cycle. See Best Practice #4: Keep Up with Technology Development.

We realize that there is a growing demand for SaaS solutions at Intel. Therefore, as shown in Table 1, we established criteria for our SaaS implementation. These criteria have four characteristics: agility, flexibility, security, and usability.

Four Best Practices for Minimizing Risk When Adopting SaaS as a Delivery Model for Enterprise Business Applications

1. Develop a SaaS security strategy and build a corresponding reference architecture
2. Balance risk and productivity
3. Implement SaaS security controls
4. Keep up with technology development

Table 1. Strategic Characteristics of Intel IT's Information Security Support for Software as a Service (SaaS)

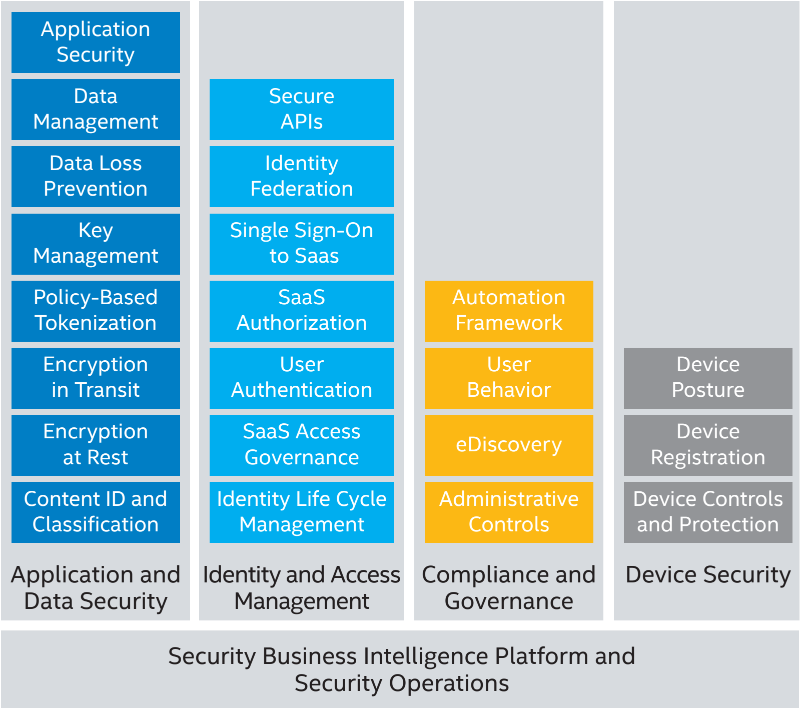
Characteristic	Details
Agility	• Supports multiple SaaS solutions, which minimize the adoption effort of the next SaaS solution
Flexibility	• Supports large SaaS deployments • Supports use cases that involve Intel employees and external personnel as well as managed and non-managed devices
Security	• Establishes a balance of controls and risk acceptance
Usability	• Avoids negatively impacting key functional requirements • Provides an easy, unified experience from anywhere and any device • Is generic, easily reused, and easily configured

Intel's SaaS Security Reference Architecture

As shown in Figure 1, our SaaS security reference architecture uses the following categories of building blocks:

- **Application and data security.** Various techniques and tools help protect corporate and employee data.
- **Identity and access.** Identity management, single sign-on, and multifactor authentication are just some of the ways we verify that the appropriate people have access to the appropriate SaaS applications.
- **Compliance and governance.** We use several approaches to meet regulatory compliance requirements, including educating employees about using the cloud safely. In addition, enterprise governance controls ensure that SaaS deployments are meeting security policy and privacy requirements. We also review SaaS cloud service providers with respect to the security assurance of the cloud service and their ability to demonstrate their adherence to industry standards.
- **Device security.** We have established a security framework for device management, including device registration and security controls. These controls are based on device attributes and security compliance (also known as device posture).
- **Security business intelligence (SBI) platform and security operations.** This platform serves as the foundation of our information security efforts, supporting logging, monitoring, incident response, and advanced analytics.

SAAS SECURITY REFERENCE ARCHITECTURE



Application Security			
Data Management	Secure APIs		
Data Loss Prevention	Identity Federation		
Key Management	Single Sign-On to Saas		
Policy-Based Tokenization	SaaS Authorization	Automation Framework	
Encryption in Transit	User Authentication	User Behavior	Device Posture
Encryption at Rest	SaaS Access Governance	eDiscovery	Device Registration
Content ID and Classification	Identity Life Cycle Management	Administrative Controls	Device Controls and Protection
Application and Data Security	Identity and Access Management	Compliance and Governance	Device Security
Security Business Intelligence Platform and Security Operations			

Figure 1. Our SaaS security reference architecture comprises building blocks in the categories of application and data security, identity and access management, compliance and governance, device security, and security business intelligence platform and operations.

Benefits of the SaaS Security Reference Architecture

Our SaaS security reference architecture provides the level of security, privacy, and legal compliance that is necessary in our large enterprise.

- **Security.** Through the controls we have implemented, we have provided a more secure way to enable enterprise use of SaaS. Intel can now "go fast" when adopting SaaS solutions. We have also reduced the risk of unapproved use of SaaS solutions, data loss, or unauthorized access. (See the sidebar, Evaluating the Risks of Shadow IT.)
- **Privacy.** Our controls protect employees' personally identifiable information, reducing the likelihood that it reaches SaaS providers and attackers.
- **Legal compliance.** Our governance, risk management, and compliance efforts help keep Intel compliant with regulatory requirements.

Keeping the Reference Architecture Agile

One of our key learnings while building our SaaS security reference architecture is that SaaS technology is constantly changing. A secure SaaS security reference architecture requires frequent adjustments and a continuing market for new and enhanced solutions. Security capabilities vary between suppliers, who may take different approaches to file encryption, authentication, logging, remediation work flows, and so on. It is important that we use an Agile method of implementation and make modifications to our architecture when necessary.

Best Practice #2: Balance Risk and Productivity

Intel IT is committed to protecting Intel's intellectual property and employees' personally identifiable information. For example, we institute controls to protect against known malware, phishing sites and software, and loss of intellectual property. However, we do not want to arbitrarily block services and the movement of data. We also want to encourage personal responsibility, educating employees about risks and ways to mitigate them through safe cloud behavior. We want to empower users to understand the risks yet be innovative and productive.

We have established a method of balancing risk and productivity to achieve the appropriate level of risk tolerance. While risk may seem difficult to quantify, Intel has developed methods based on industry standards to calculate information security risk as a function of threat, vulnerability, and consequence in the context of risk scenarios. Risk scenarios are developed in conjunction with subject-matter experts and information security specialists. These risk scenarios allow us to measure the probability that a specific threat agent will exploit a vulnerability or produce a negative business impact.

Evaluating the Risks of Shadow IT

Shadow IT is hardware or software within an enterprise that is not supported by the organization's central IT department. In the context of SaaS, shadow IT refers to personal technology that employees use at work or niche technology that meets the unique needs of a particular business group that is supported by a third-party service provider instead of by corporate IT.

Shadow IT (also known as cloud sprawl) leads to inefficiency, duplication, and business-related decisions being made outside of the formal governance processes of the organization—potentially leading to gaps in compliance and control for an organization along with possible leakage of intellectual property and data.

Intel IT is working to discover shadow IT SaaS services and respond appropriately. Our priorities are to validate the data and understand the environment, take control of the data, and implement governance and compliance. To this end, we have deployed a shadow IT detection tool that can analyze our cloud proxy and offline repository scan logs, detect cloud application usage across the enterprise, provide a risk rating for all discovered cloud applications, and provide usage analytics.

By reducing the use of shadow IT SaaS at Intel, we can identify cost-saving opportunities through supplier consolidation and better protect Intel's intellectual property.

For example, a given risk scenario may involve a high threat (such as active known malware propagating through the network), targeting highly vulnerable applications and systems (such as unpatched Transport Layer Security) that handle critical personal information. This information could be leaked in a successful compromise (a high consequence). Such a scenario would be rated as a high risk. If a threat is less likely to exploit vulnerabilities in a scenario—such as when the attack surface is reduced through proactive patching or strong access controls—then the risk may be low.[3]

For threats with a high risk rating, we may block a service entirely, or we may combine controls to mitigate the risk.

Best Practice #3: Implement SaaS Security Controls

To help securely support SaaS in the enterprise environment, security controls are necessary. In our experience, most SaaS security controls relate to one of three areas of risk, as shown in Figure 2:

- **Identity and access management controls.** A combination of several controls helps ensure that SaaS applications are accessed by the appropriate users in the appropriate computing environment.
- **Application and data controls.** Data encryption and tokenization help us protect the data, while data loss prevention (DLP) techniques help keep sensitive information from leaving the Intel premises. For some use cases, we combine encryption and DLP to provide a higher level of protection. Application controls are focused on registering applications and emulating code auditing through our supplier assessment or by third-party validation. Intel business group applications that use SaaS APIs in their code are also reviewed.
- **Logging and monitoring controls.** We have established controls that detect when information security violations (also known as anomalies or events) occur, send alerts to the appropriate IT staff, initiate appropriate responses, and correct the situation.

[3] For more information on information security and risk assessment at Intel, refer to the following white papers: "Aligning Business and Information Security Risk Assessments," "Prioritizing Information Security Risks with Threat Agent Risk Assessment," and "Understanding Cyberthreat Motivations to Improve Defense."

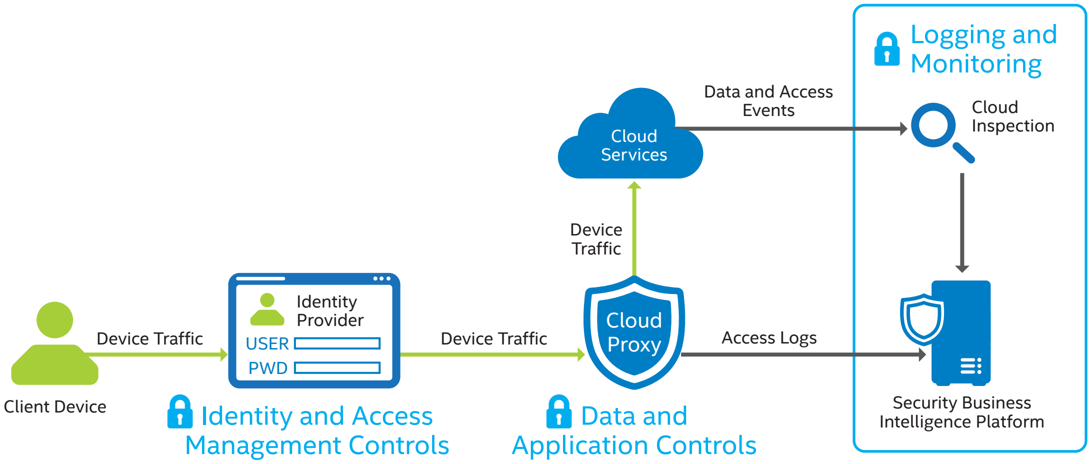


Figure 2. We focus our SaaS security controls in three areas: identity and access management, data, and logging and monitoring.

The following three sections provide details about each of these SaaS security control areas. The final section describes how we match the controls with the risk rating arrived at with Best Practice #3.

Identity and Access Management Controls

The first level of control is to manage identity. We use single sign-on to improve the user experience. After the user signs on, we use several service providers' tools to enforce access controls and multifactor authentication controls to manage access. These controls help maintain a trustworthy computing environment by complying with Intel's last-day-at-the-office and least-privilege controls. Our overall goal is to make it easy yet secure for Intel employees and their collaborating partners to access SaaS applications.

Identity. The first-line SaaS security control is identity management. When Intel employees want to access a SaaS application, they open a browser window on their device and then sign in using their corporate identity. Intel employees have a single identity (username/password combination) that they can use to access multiple applications, using single sign-on. Single sign-on improves security and the user experience because employees do not need to keep track of multiple passwords and thus are not tempted to write them down to remember them all.

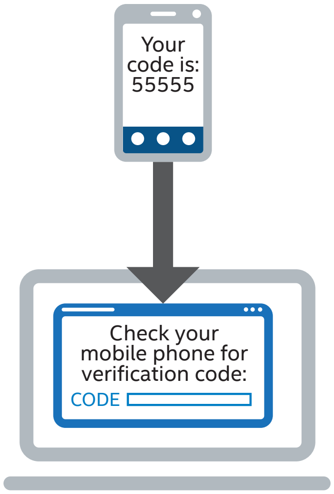
Identities are managed by identity providers, which can be internal (for Intel employees) or external (for non-Intel employees accessing the same SaaS application). We are developing a hybrid model where we manage identity accounts on Intel premises and synchronize them with external identity providers.

Intel IT manages the user account life cycle for SaaS applications in the same way that we manage any corporate application operating on the corporate network. Intel implements an integrated account provisioning framework to create, update, and disable accounts in the SaaS application. Intel embraces the SCIM (system for cross-domain identity management) account-provisioning standard in all cases where it is supported by the SaaS application provider.

Access Controls and Multifactor Authentication. While managing identities is important, access controls are also necessary to enhance SaaS security. We manage access controls through enrollment and entitlement workflows. We use a request/approval, role-based, and attribute-based process to manage access to SaaS applications. A context-aware access-control framework grants access to SaaS applications, taking into consideration factors beyond user group membership.

For example, we can use network location to inform an access decision. In some cases it may be important that access is granted only if the user is connected to the corporate network; if we detect that the user is off-network, we can ask for multifactor authentication to provide better assurance of identity. We use various tools for authentication, depending on the SaaS application; the authentication process varies with the device being used.

For certain SaaS applications, employees using a laptop have access to integrated Microsoft Windows* authentication, whereas employees using a small form factor device must complete a one-time form authentication. For our online office, storage, and collaboration environment, laptop users have access to integrated Windows authentication only if their laptop has intranet access; small form factor device users must use a VPN to authenticate for the first time.



Multifactor Authentication
Verification codes sent to a mobile phone can help improve SaaS security.

Our work with multifactor authentication is still in progress, and we understand that usability is key to a successful multifactor authentication rollout. Therefore, we are considering a rich set of options that can align with a user's computing preferences and level of connectivity. (We do know that we will not be using hardware tokens.) These options include the following:

- Smartphone push message one-time password (OTP)
- Smartphone and desktop OTP generator
- SMS-based OTP generator
- Audio-callback user verification

We plan to continue to adjust our multifactor authentication framework to blend usability and security needs as capabilities evolve.

Application and Data Controls

While identity and access controls provide a certain level of security, we also need application and data controls. Application security controls help verify that code using SaaS APIs and supporting the integration of SaaS applications into the enterprise is securely developed and follows best practices.

Once a user logs in to a SaaS application, the method we use for data protection depends on how the application is implemented. But in all cases, the data traffic flows through a cloud proxy where policy is enforced. Policies exist to protect specific types of data and to detect unapproved data.

Data encryption and tokenization. One type of data control includes data encryption and tokenization. The data is encrypted using an encryption key, which is stored on Intel premises. We can encrypt both structured data (specific fields in a database, for example) and unstructured data (such as entire files). Our encryption model is a hybrid in that some encryption is done on-premises and some off-premises. Encryption keys are pushed to the cloud proxy on a specified time interval. Keys are stored only in memory in the proxy environment—they are signed and can be used only by the appropriate tenant.

When tokenization is required for data residency for some fields or data elements, they are sent to the SaaS application as a replacement for the actual data. The use of tokenization requires an on-premises database, because an unencrypted index is created. Intel IT is investigating tokenization as a future use case.

Two Aspects of
Data Loss Prevention

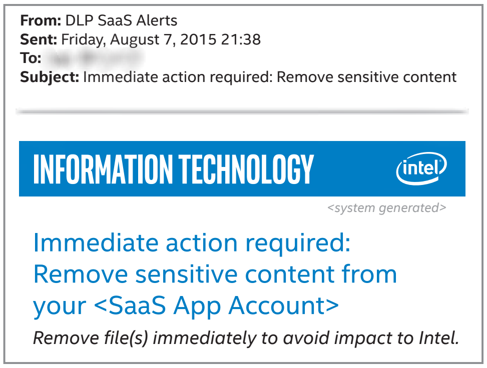
ACTION
SEC
DETECTION

Data loss prevention. DLP is another type of data control that helps us prevent the transfer of documents containing certain types of information. DLP has two aspects: detection and action. Detection means that we look for certain keywords or phrases (depending on policy), such as "top secret." If we detect a prohibited word or phrase, we instigate appropriate actions, such as informing the user of security policies and encrypting, quarantining, deleting, or unsharing a document.

We use two types of DLP controls:

- **Proxy-based real-time detection.** Detection and action occur as information passes from Intel's network into the cloud through the cloud proxy.
- **Offline repository inspection.** This tool uses SaaS APIs to access data where it resides in the cloud. SaaS providers make APIs available that enable us to discover who opened a file, whether they changed anything in the file, and other activities. The offline scan engine can also look for keywords, personally identifiable information (for example, social security numbers and birthdates), and content tagging (such as metadata that identifies a project name and data classification).

Depending on the use case, we can use either type or both types of DLP control. All DLP events are logged into our SBI platform (see Logging and Monitoring Controls for more details). With either type of control, if a keyword is found, the SBI platform receives an alert and opens a service ticket to the SaaS management team, which can then determine the appropriate response. For example, we can remove the file on the user's behalf, if necessary, or encrypt, quarantine, or unshare the file. In addition to alerting the SBI platform when inappropriate content is being sent to a SaaS application, the DLP controls send the user an alert message, similar to the one shown in Figure 3.



From: DLP SaaS Alerts
Sent: Friday, August 7, 2015 21:38
To: [redacted]
Subject: Immediate action required: Remove sensitive content

<system generated>

Immediate action required: Remove sensitive content from your <SaaS App Account>

Remove file(s) immediately to avoid impact to Intel.

Figure 3. The offline scan engine can send an alert to a user if it detects that inappropriate data has been sent to a SaaS application.

Matching Controls to the Risk Level

We match SaaS security controls to the security assessment and the risk level, instead of using every control on every SaaS application or in every use case. Figure 4 illustrates this concept. In the figure, the employee is using a client device (a smartphone, tablet, 2-in-1 device, or a laptop) to access two SaaS applications—an online office, storage, and collaboration environment and a sales and marketing CRM tool. We use a cloud proxy to route user traffic to the correct SaaS application, with the appropriate controls.

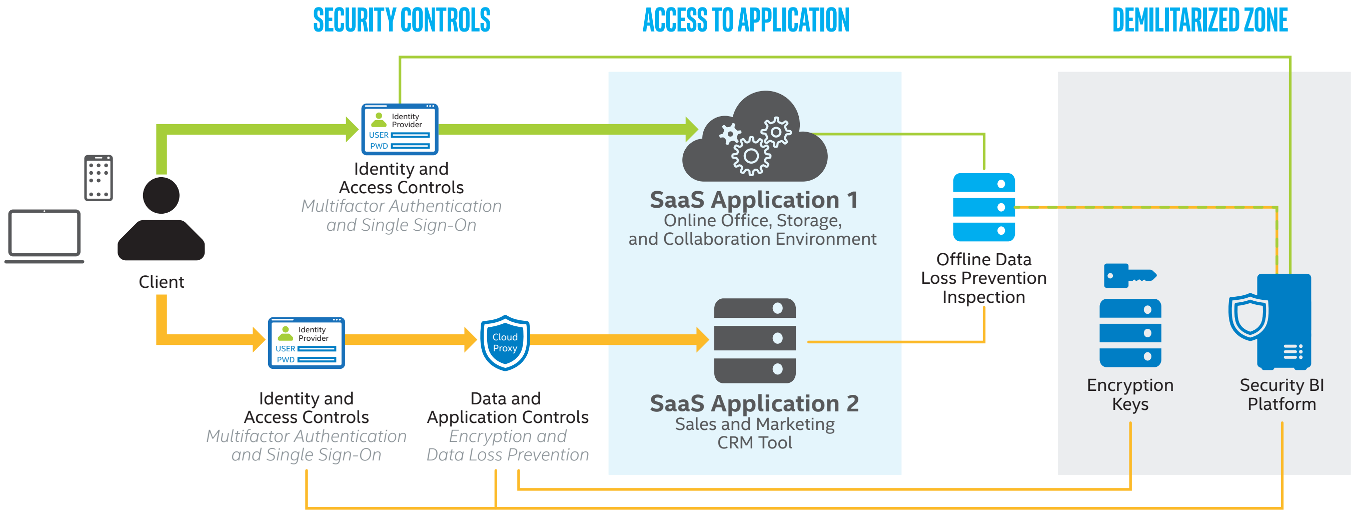
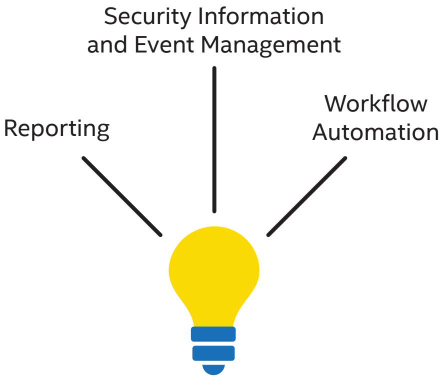

SECURITY CONTROLS
ACCESS TO APPLICATION
DEMILITARIZED ZONE
Identity Provider
USER
PWD
Identity and Access Controls
Multifactor Authentication and Single Sign-On
SaaS Application 1
Online Office, Storage, and Collaboration Environment
Offline Data Loss Prevention Inspection
Client
Identity Provider
USER
PWD
Cloud Proxy
Encryption Keys
Security BI Platform
Identity and Access Controls
Multifactor Authentication and Single Sign-On
Data and Application Controls
Encryption and Data Loss Prevention
SaaS Application 2
Sales and Marketing CRM Tool

Figure 4. Different SaaS applications have different risk levels. One application may use only identity and access controls with offline data loss prevention inspection; another application may combine identity and access controls with data controls such as encryption and data loss prevention.

Share:



SBI Capabilities

For example, for the online office, storage, and collaboration environment, we might use only identity and access controls on the front end and use offline DLP inspection on the back end. For the CRM tool, however, we might add encryption and real-time DLP controls to help protect the data.

Logging and Monitoring Controls

The third area of SaaS security controls that we focus on is logging and monitoring. We use our SBI platform as the focal point for logging, monitoring, alerting, responding to information security violations, and using advanced analytics to improve our information security environment. Security logs and alerts are collected from the cloud and fed into the platform. Actionable alerts are immediately sent to our IT security information and event management system for incident response and remediation purposes. Security data is correlated and monitored for anomaly detection.

We use detective controls to monitor cloud traffic for many kinds of anomalies, including the following:

- The user uploads or downloads unusual amounts of data compared to that person's normal usage.
- The user logs in from two geographies in an unrealistic time frame.
- The user tries to perform a task not allowed by his or her user privilege.

The SBI platform portal enables easy access to reporting capabilities, workflow automation, and the security and event management system.

Best Practice #4: Keep Up with Technology Development

We have learned that, just as enterprise applications and data are moving to SaaS, SaaS security controls are also moving to the SaaS model. That is, many security service providers currently host their services in the cloud, and we expect significant expansion of enterprise security capabilities delivered as SaaS. Therefore, we must decide which SaaS security controls will remain internally hosted and managed and which ones will be externally hosted and managed. Carefully evaluating SaaS providers can help us make these decisions based on the maturity of a particular provider's controls.

But a one-time evaluation is not enough—we must constantly reevaluate providers and controls because the public cloud, especially the SaaS ecosystem, is continually changing and evolving. We expect such technology development to occur for a significant period of time. Therefore, we will conduct continuous and short cycles of reviewing the SaaS landscape for security solutions so that we can enhance access controls, data protection and encryption, and device posture.

Areas to Explore

While we have developed best practices and security controls for supporting enterprise use of SaaS applications, we plan to explore the following risk management challenges, which are growing more and more complex:

- Integration, which includes both SaaS-to-SaaS integration and SaaS-to-enterprise application integration
- Privacy concerns, especially the legal complexities of personal information being shared in SaaS-to-SaaS systems
- Mixing of highly sensitive data (Intel Top Secret or Intel Restricted Secret) with less sensitive data (Intel Confidential or Public) in SaaS-to-SaaS systems
- Consistency in security controls and user experience regardless of where the application is hosted

As the SaaS ecosystem continues to mature, we will develop controls and additional best practices to address these areas of concern.

Conclusion

The SaaS delivery model for enterprise applications offers efficiency, velocity, agility, cost-effectiveness, and collaboration benefits for many enterprise use cases. To support the increasing demand at Intel for SaaS solutions, Intel IT has established several best practices to minimize risk in the cloud:

- Develop a SaaS security strategy and build a SaaS security reference architecture that reflects that strategy.
- Balance risk and productivity.
- Implement SaaS security controls.
- Keep up with technology development.

Our SaaS security controls have enhanced security, privacy, and legal compliance at Intel, and we are making it safe for business groups to "go fast" when adopting new SaaS solutions.

For more information on Intel IT best practices, visit intel.com/IT.

Receive objective and personalized advice from unbiased professionals at advisors.intel.com. Fill out a simple form and one of our experienced experts will contact you within 5 business days.

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation:

- Twitter
- #IntelIT
- LinkedIn
- IT Center Community

Visit us today at **intel.com/IT** or contact your local Intel representative if you would like to learn more.

Related Content

Visit **intel.com/IT** to find content on related topics:

Security

- Fast Threat Detection with Big Data Security Business Intelligence paper
- SaaS Security Playbook slideshare

Cloud Computing

- Cloud Computing Cost: Saving with a Hybrid Model paper
- Developing a Highly Available, Dynamic Hybrid Cloud Environment paper
- Enhancing Cloud Security Using Data Anonymization paper
- Making Private-Public Cloud Decisions on the Way to a Hybrid Cloud paper
- Planning for eDiscovery in the Cloud paper

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

THE INFORMATION PROVIDED IN THIS PAPER IS INTENDED TO BE GENERAL IN NATURE AND IS NOT SPECIFIC GUIDANCE. RECOMMENDATIONS (INCLUDING POTENTIAL COST SAVINGS) ARE BASED UPON INTEL'S EXPERIENCE AND ARE ESTIMATES ONLY. INTEL DOES NOT GUARANTEE OR WARRANT OTHERS WILL OBTAIN SIMILAR RESULTS.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS AND SERVICES. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS AND SERVICES INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

♻ Please Recycle

0815/ERAI/KC/PDF