White Paper
December 2021

IT@Intel
Securing the Cloud for Enterprise Workloads: The Journey Continues

Establishing and maintaining good cloud security is not a sprint—it is a marathon.

Intel IT Authors

Shachaf Levi
Cloud Security Architect

Kevin Bleckmann
Cloud Solution Architect

David Fong
Cyber Risk Management

Oscar Monge España
Cloud Security Engineer

Jane Odero Greene
Cyber Risk Management

Dave Shrestha
Cloud Solution Architect

Jon Slusser
Cloud Solution Architect

Table of Contents

Executive Overview

Intel IT's multi-cloud strategy focuses on abstracting the application stack from the infrastructure to enable anything-as-a-service (XaaS) capabilities. This approach helps to accelerate innovation and allow application developers to focus on writing code, not rounding up compute, storage, and network resources, while IT handles workload placement. However, information security is still paramount in our continual quest to drive business agility.

We have found the following key steps enable us to maintain a high level of security while supporting our multi-cloud strategy:

- Approach security holistically and understand that not all clouds are the same.
- Utilize existing investments and new technologies to drive security operational excellence and key performance indicators.
- Establish distributed accountability.
- Secure sensitive workloads.
- Encourage collaboration between the application development community, business units, and IT groups.

While IT creates many of the applications and services in use at Intel, many more are developed by Intel's several lines of business, such as product development, validation, or sales. In our experience, security can be better maintained if we make our security controls easy for business application owners to use and understand.

Establishing and maintaining good cloud security is not a sprint—it is a marathon. Read on to learn about our cloud security experiences as we continue our journey to multi-cloud.

Background

Intel IT is no stranger to cloud computing or to cloud security. For example, when we built our private enterprise cloud over a decade ago, we established a solid threat model that uses Threat Agent Risk Assessment (TARA) to help us identify critical information security areas.[1] As Intel workloads began moving to the public cloud in 2013, we added new capabilities to inspect data as it moved to the cloud and new controls to block or warn of insecure or inappropriate usages and risks.

Today, we are well into our journey of shifting to a multi-cloud environment, where we engage with multiple cloud service providers (CSPs) and our own private cloud.[2] To better enable Intel's digital transformation, we have employed a "right workload in the right place" strategy, backed by a "cloud-first" mindset. Our strategy is key to providing the flexibility, scalability, availability, agility, and mobility that Intel needs to compete in today's fast-paced business environment.

Historically, Intel has been cautious about what data is moved to the cloud, because some business owners mistrust the cloud. But we have challenged that position: As cloud solutions have matured, cloud security is now a key enabler of cloud adoption because it is often equivalent to or better than traditional on-premises security. Depending on the CSP, cloud solutions adhere to industry security standards developed by organizations such as the Cloud Security Alliance, National Institute of Standards and Technology (NIST), and the International Organization for Standardization. Examples of such standards include SOC 2 – Type II, ISO 27001, and ISAE 3402.

[1] See our white papers, "Identifying Critical Information Security Areas with Threat Agent Risk Assessment" and "Understanding Cyberthreat Motivations to Improve Defense."

[2] See our white paper, "Intel IT's Multi-Cloud Strategy: Focused on the Business."

Our cloud strategy supports the enterprise-wide adoption of the Agile/DevOps model at Intel. Just like other DevOps teams, security teams can take advantage of the service-oriented, elastic, and agile nature of the cloud, bringing solutions to execution faster (sometimes referred to as DevSecOps). We have moved far beyond simple software-as-a-service (SaaS) solutions to encompass virtually anything as a service (XaaS)—including information security (InfoSec) as a service.

Our multi-cloud strategy lets us use CSPs to foster innovation and corporate resource agility. It also enables us to maintain a security posture that helps protect Intel's valuable data, regardless of where it is stored.

Solution

As mentioned in the Executive Overview, we consider the following steps to be foundational to securing enterprise workloads in a multi-cloud environment.

- Approach security holistically.
- Make the right technology choices.
- Establish distributed accountability.
- Secure sensitive public infrastructure-as-a-service (IaaS) workloads.
- Make security easy to consume through automation and collaboration.

These steps are described in more detail below.

Approaching Security Holistically

As summarized in Figure 1, a combination of people, processes, and technology empowers cloud security. Our security strategy and architecture (compute, storage, and network) tie all three together.

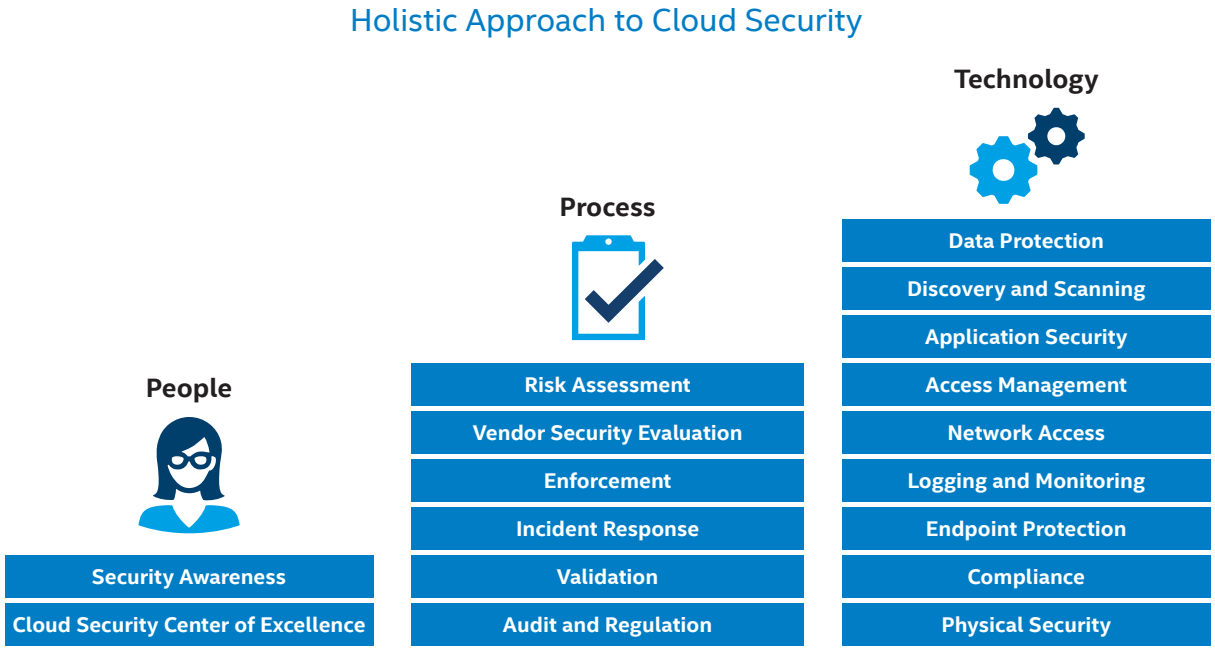

Figure 1. We take a holistic approach to cloud security. People, processes, and technology combine to create the highest level of security possible.

People

We work to raise awareness of cloud security—how it can be enhanced and common pitfalls—because the considerations for keeping an application or service secure in the cloud can be substantially different than traditional administration of an application or service. We have found that knowledge boosts security. We strive to educate cloud users about the various levels of accountability—who is responsible for what. (See "Establishing Distributed Accountability" for more details.)

In 2016, we established the Intel Security College, which offers over 100 cybersecurity courses for 11 different technical roles. The Security College improves our security posture and helps reduce costs by training our developers to write secure code from the outset. According to NIST, it costs 30x more to fix application vulnerabilities once an application or service is in production.[3] Our Security College courses are based on industry best practices, such as the NIST 800.16 security training requirements. Course content can be used as Continuing Professional Education credits for existing technical certifications and is available in five localized languages.

Our Cloud Center of Excellence (CoE) brings practitioners from Intel together including application owners, developers, business units, and IT service providers. CoE's core members understand the benefits, features, and risks associated with the cloud security. The CoE provides leadership, solutions, best practices, research, support, and training for the rest of Intel. Through this collaboration, tangible outputs of the CoE include consumable services, patterns, and other best-known methods that have security built in, providing practitioners with secure foundational components that accelerate their application time to market.

We augment the Security College and the CoE by working with Intel's business units to improve application and service security and security processes. Legacy applications exist that may not reflect modern information security practices. As we work with the business units, we are partners, not gatekeepers or enforcers. We provide customized guidance for specific applications or services. In addition, information security is built into each DevOps team at Intel, which contributes to enterprise security overall.

All these efforts help create a security-conscious culture at Intel,[4] where security is a daily and easy part of doing business, not an afterthought.

Process

Our end-to-end cloud security processes start with the request to host an application or service in the cloud and provide support until the end of its life. With our "right workload in the right place" strategy, IT is the decision maker on the hosting location, taking into account both security and latency needs.

We are aware that security levels differ from one CSP to another. Each CSP provides different levels of controls and processes, certifications, and investment in security. Hence, for each CSP, we perform a thorough security risk assessment of the hosting infrastructure and the application or service being hosted. (See "Securing Sensitive Public IaaS Workloads" for more details about these evaluations.)

Once the assessment is complete, we use well-defined processes that enforce the relevant security policies and standards as the application or service is deployed (these processes are referred to as "guardrails"). Examples of such processes include configuration management; data protection; application/service updates; and compliance with national, regional, and local governance regulations.

Ideally, our policies and guardrails prevent security incidents. But in the real world, incidents do happen. We have established processes that can detect an incident and respond, ranging from sending an alert to disabling the account. We also conduct an investigation after an incident so that key learnings can be shared across Intel's security teams.

We regularly perform audit and validation processes to track application/service security status. These processes generate valuable data and insights that can improve security.

Technology

While people and processes are important aspects of cloud security, technology is also critical. We use various technologies to perform a wide variety of security tasks:

- **Data protection.** In the cloud, data is the main asset. Knowing where the data is, encrypting it, controlling access to it, and avoiding exposure are key elements of cloud security.
- **Discovery and scanning.** The basic security rule is that "you cannot protect what you do not see." Virtually all CSPs provide excellent visibility into hosted assets and services, and all assets are associated with an "owner," making our job easier. We detect which applications or services are hosted publicly, determine their configuration and usage, and scan them for misconfiguration and vulnerabilities.
- **Application and service security.** In both our public and private cloud environments, each application or service must be registered in our internal application repository and is assigned metadata tags for cloud resources. Once it is registered and tagged, we perform both static and dynamic code scanning.
- **Access control.** Our goal is to ensure accounts are accessed only through approved channels (that is, cloud tenants should not be able to access their Intel cloud account without going through the appropriate controls). To this end, we use multifactor authentication for administrator access and an account lifecycle and entitlement system to manage access control.
- **Network security.** We apply industry best practices for secure network configuration and security alerting.
- **Logging and monitoring.** Fast, appropriate incident response requires the ability to obtain detailed logs and

[3] "The Economic Impacts of Inadequate Infrastructure for Software Testing," nist.gov/sites/default/files/documents/director/planning/report02-3.pdf

[4] For more information, listen to the podcast, "Inside IT: Strengthening Intel's Security Culture."

alerts in real time—these are the "eyes and ears" in the cloud. Based on these logs, we can send alerts when an incident occurs, trace previous actions, and act. We choose CSPs who can provide "security alerts as a service" (instead of creating our own alert rules), because they have the most knowledge about their applications and infrastructures. Our cloud logging and monitoring processes are integrated with our security operations center.

- **Endpoint protection.** Anti-malware and more advanced solutions can protect data on endpoint devices. This is another area where public cloud offers tangible security benefits. The ability to provision compute and other services on a virtual machine (VM) or in a container for a short period of time and then delete that VM or container when it is no longer needed can reduce risk.
- **Compliance.** We use tools to compare an application or service's configuration to the configuration policy to support our enforcement process. (See "Measuring Compliance" for more details.)
- **Physical access.** In both the private or public cloud, we validate the physical security of the infrastructure.

Making the Right Technology Choices

The market offers many choices for security technology. Various CSPs use a wide variety of security-focused tools, and we have built additional security tools in-house. As is the case for many IT endeavors, one size does not fit all. Certain on-premises technologies may be the perfect fit for some situations, but in others, it might be best to use tools and capabilities provided by the CSP. We work to find the right blend of tools—our own, the CSPs', or perhaps a new investment—that best meets the current and future needs for Intel.

We have found that considering technical debt is the key factor in deciding between the options of extending existing on-premises tools to the cloud, using CSP offerings, or investing in additional third-party tools. For each security capability, we compare the three options to determine what satisfies the minimal viable product requirements. We prefer to use an existing investment. However, if that is not feasible, the choice between cloud-native and third-party tools is more complicated and is based on value and cost of the solution.

In reality, our security controls are a blend of all three options, and we continually look for opportunities to consolidate as the cloud security industry matures.

Establishing Distributed Accountability

Cloud security is a team effort. As shown in Figure 2, there is no single repository for security ownership. Instead, we use a distributed accountability model where IT, the business owner, and the CSP all share responsibility for security.

Overall, business owners are accountable for securing their data and, in collaboration with IT, verifying that the appropriate controls are in place. Securing the data includes managing the application or service lifecycle, data management, network configuration, managed security services for compute resources, and operations. Each of these feeds into a related IT-owned function, such as key management and network governance.

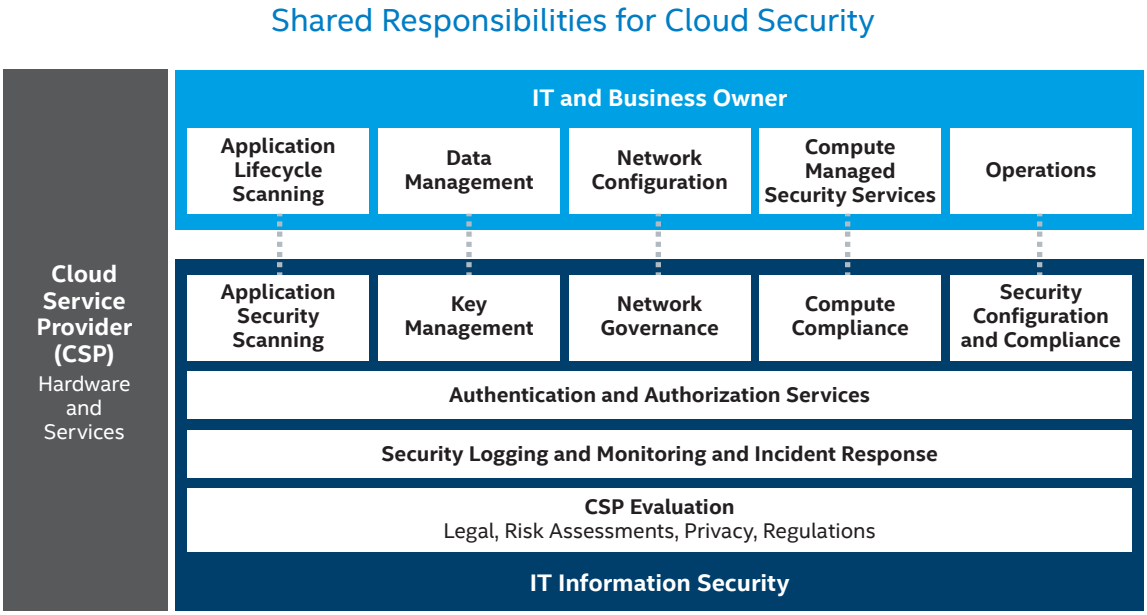

Figure 2. Accountability for cloud security does not rest with a single person or department. The responsibility is shared between the cloud service provider, the business owner, IT, and Information Security.

Securing Sensitive Public IaaS Workloads

As mentioned earlier, we contend that all Intel data (even our highest level of classification) can be hosted in the cloud, given the appropriate levels of security and if the cloud solution provides the necessary return on investment and responsiveness. At Intel, there is a growing demand to host sensitive workloads on public cloud IaaS, plus additional public cloud usage models are emerging. Intel has about 230 SaaS solutions deployed on the public cloud, with another 120 or so in the pipeline. Of the already-hosted solutions, 15 of them are deployed with sensitive data. Since we already have sensitive data hosted externally through SaaS, the next step is to host this kind of data on public cloud IaaS, using containerization technology and new security controls (see "Securing Containers in the Cloud"). In this way, we secure sensitive workloads across the entire cloud spectrum.

Beyond our well-defined processes and distributed accountability discussed previously, securing sensitive workloads includes the following steps:

- **Risk assessment.** We evaluate the CSP's infrastructure and SaaS security posture. Considerations include encryption and key management, logs, response process, interaction with application/service owner, network, monitoring capabilities, service-level agreements, and more (see Figure 3). For the application or service, we determine what the consequences would be if data were exposed. We implement controls that are proportionate with the level of consequences.
- **Encryption mapping and management.** Several encryption methods exist, and we choose the one most appropriate for the application or service. Key usage and alerting logs are included in standard logs, alerts, and incident response processes.
- **Legal documentation.** For every workload, we sign a contract and a nondisclosure agreement with the CSP.
- **Measuring compliance.** We continually monitor for compliance and enforce secure infrastructure configurations.

Two of these steps, encryption mapping and measuring compliance, are discussed in more detail in the following sections.

Mapping Data to an Encryption-at-Rest Method

Based on our established threat model, not all assets need to be protected the same way, and protection levels must be cost-effective. For example, external-facing applications or services may require a different level of protection than internal-facing applications and services. At-rest encryption methods include file, whole-disk, cell, and transparent database encryption.

For cloud hosted-sensitive workloads, we can choose between service-managed key, bring-your-own key, and on premises-managed key. Table 1 illustrates our data-to-encryption model for various types of data services. The more we move to native cloud services, the more we strive to consume native cloud encryption. For example, for database as a service we use the CSP's key service, but we create our own key for the service. In contrast, a physical database on a VM might consume our on-premises encryption capability.

Besides choosing the appropriate at-rest encryption method for the data type, we have also established an operational process we believe can track and manage key usage throughout the lifecycle of an application or service.

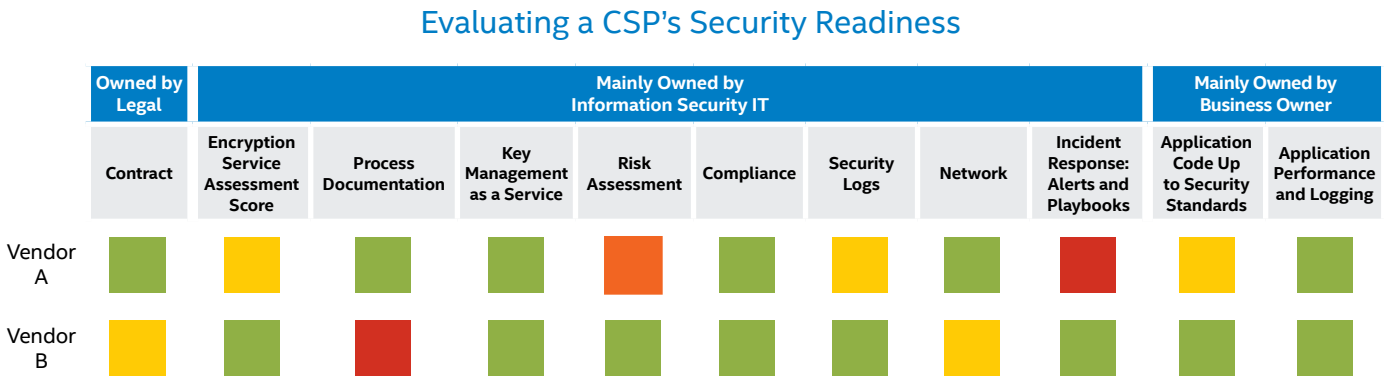

Figure 3. Our CSP evaluation process enables us to determine whether a sensitive workload can be hosted securely.

Table 1. Data-to-Encryption Model

Priority	Data Services	Service-Managed Key	Customer-Managed Key	On Premises- Managed Key	Client-side Encryption
1	Object storage		X		Based on demand
2	Volume storage		X		Based on demand
3	Database			X	Based on demand
4	Database as a service	X	X		Based on demand
5	VM with data		X		Based on demand

Securing Containers in the Cloud

We realize that application developers do not want to spend lots of time securing their development environments. Instead, they want an environment that can be provisioned quickly and is already secured. We are working to conduct a proof of concept where we bolster our existing guardrails to create a more secure sandbox environment for application developers. We plan to accomplish this through a combination of containerization technology and access controls to boost both security and agility. We are also developing a standard set of rules—essentially a cloud deployment template—that applies to every CSP account. These rules are expected to provide a secure zone for Intel's business owners to consume.

We use a third-party product to perform a vulnerability assessment of containers. The tool can validate that the containers are running in the correct state (non-root) and may be able to identify which vulnerabilities are affecting the static images. We chose a tool that can integrate with our existing cloud security solutions to scan both the host and the containers, reducing operational overhead while aligning with Intel's technical debt-reduction goals.

Measuring Compliance

We integrate data provided by the CSP with data delivered by third-party solutions to track key performance indicators (KPIs) for compliance, as shown in Table 2. We have found that for workloads hosted in the public cloud, measuring compliance of the infrastructure configuration (to identify and rectify mistakes) as well as measuring the traditional operating system vulnerabilities and patch compliance measurements is valuable. The reports generated by our compliance measurement tools are incorporated into our operational excellence process and included in our overall compliance reporting processes as well.

Figure 4 shows the compelling results of our cloud security strategy and compliance audits—a vulnerability scanner shows the reduction of vulnerabilities.

Table 2. Example of Compliance Result for Two CSPs

KPIs for Security	Vendor A		Vendor B	
	Account	VM	Account	VM
Percent of systems with compliance agent installed		95%		99%
Percent of accounts that are compliant with high-security best practices	98%		97%	
Percent of object storage configurations that adhere to security best practices	99%		99%	
Percent of systems without vulnerabilities		99%		95%

Making Security Easier to Consume through Automation and Collaboration

In reality, we know that if security is hard to consume, it will be harder to use and potentially avoided. We automate as much as we can so that everything operates normally behind the scenes. For example, guardrails such as setting up an account-level encryption key or launching security logging are triggered by an account request; the requester does not have to specifically think about such things. Another way we make security easier is to choose security solutions that are built for the cloud. Cloud-native security is agile and easily integrated into the continuous integration/continuous delivery (CI/CD) pipeline. We also understand business owners' automation needs and provide scripts that are compatible with their configuration management solutions.

We offer application developers several tools that encourage security-conscious application development. For example, we have an easy-to-use portal that provides self-service application security certification and a wiki that explains what controls and steps are required to secure the deployment. This wiki helps business owners better understand their security responsibilities when deploying their application or services on public cloud infrastructure. We expect to deploy cloud security soon that could help protect a public cloud account from violating a policy and will automatically take enforcement actions (see "Next Steps").

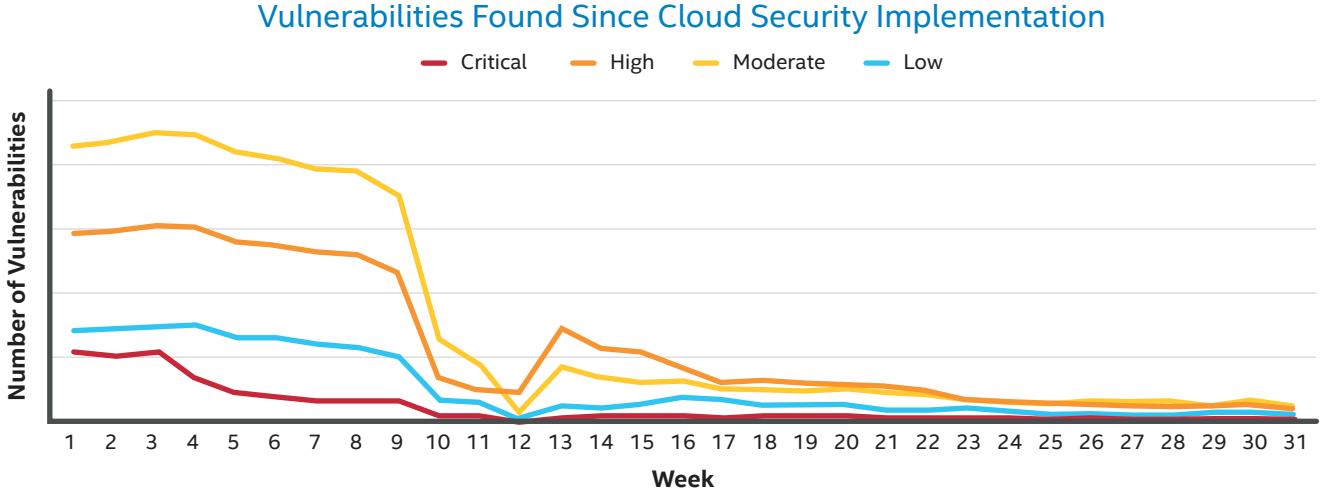

Figure 4. Since implementing our cloud security strategy, the number of security incidents has decreased substantially.

We review and collaborate with business units, application developers, and owners to create secured application and infrastructure designs, as there are many variations to how cloud services are being used.

We manage certain security features and requirements so that the business owner does not have to. In general, there are two types of IT-managed security features:

- **Operations that are sensitive** enough that they require IT to handle them
- **Operations that are essential enough to cloud security** that it makes sense for IT to own the core component (such as the compliance-measuring tool)

Overall, Intel IT Information Security wants to "make it safe for Intel to go fast" by being a trusted advisor to business units and creating security services and processes that are as seamless as possible.

Next Steps

We intend to further operationalize our investments to better support multiple IaaS environments across various CSPs. We are looking at ways to reuse and streamline solutions and processes as we transition to multi-cloud environments—speeding adoption and decreasing the learning curve of implementation over time. While the architecture and processes will remain the same, the toolset and some implementations can slightly vary. We may use one set of tools for private cloud security management and a very different toolset for one CSP, and yet different tools for another CSP. And of course, we will continue to evaluate new technologies, such as serverless security and artificial intelligence (AI) to keep pace with the industry and ensure that Intel's data is as secure as possible.

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 on Twitter or LinkedIn. Visit us today at intel.com/IT if you would like to learn more.

Conclusion

As our journey to the cloud continues, our information security efforts can help guide and secure our evolving multi-cloud business strategy. As we secure cloud usages, on-premises security teams can also benefit and are better able to improve security in various domains across the enterprise. But the journey is far from over. The high rate of change in technology and services requires a constant re-evaluation and modification of both technology and processes—which makes cloud security a very fascinating field of work.

Related Content

If you liked this paper, you may also be interested in these related stories:

- Intel IT's Multi-Cloud Strategy: Focused on the Business paper
- Boosting IaaS and PaaS Security in the Public Cloud paper
- Utilizing PaaS for Business Agility and IT Efficiency paper
- SaaS Security Best Practices: Minimizing Risk in the Cloud paper
- Taking Enterprise Security beyond the Edge paper
- Enhancing Cloud Security Using Data Anonymization paper
- Inside IT: Strengthening Intel's Security Culture podcast

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

Intel IT Contributors

Jessica Tran, Information Security Specialist
Alan Gonsalves, Information Security Manager
Suzan Hawbaker, Security Product Owner
Roberto Quinones, Security Architect
Corey Kukis, Cyber Risk Management
Ryan Clark, Security Engineer

Acronyms

CoS	Cloud Center of Excellence
CSP	cloud service provider
IaaS	infrastructure as a service
KPI	key performance indicator
NDA	nondisclosure agreement
NIST	National Institute of Standards and Technology
SaaS	software as a service
SLA	service-level agreement
VM	virtual machine
XaaS	anything as a service