WHITE PAPER
JANUARY 2017

IT@INTEL

Boosting IaaS and PaaS Security in the Public Cloud

We continually assess and enhance security and privacy capabilities, processes, and people's skills to protect Intel's data and the data of our customers.

Intel IT Authors

Shachaf Levi
Cloud Security Architect

Catalin Baicu
Sr. Technical Information Security Program Manager

Andrew Ambrosia
Security and Controls Technologist

Carlton Ashley
Enterprise Security Architect

Kevin Bleckmann
IT Cloud Broker

Oscar Monge España
Cloud Security Engineer

David Fong
Cloud Security Strategist

Jason Hardie
Sr. Information Security Specialist

Jac Noel
Security Systems Engineer

Laurie Yocum
Technical Project Manager

Elaine Rainbolt
Industry Engagement Manager

Executive Overview

IT departments everywhere face what appears to be conflicting business needs: the need to take advantage of the agility and technology provided by the public cloud and the need to keep proprietary information secure.

Recently, Intel IT has developed a public cloud infrastructure-as-a-service (IaaS) security strategy, which also encompasses platform-as-a-service (PaaS) security. This strategy, complemented by a comprehensive IaaS security architecture, enables Intel business units to use public cloud IaaS to accelerate innovation and time to market while cutting costs. We have also moved some of our IT services to public cloud IaaS to reap similar benefits.

Successful public cloud usage involves more than just technology. We have adopted new tools, made substantial enhancements to relevant processes, and invested in people's skill sets. We have found that we must regularly invest in developing our IT skills to securely enable Intel's growing number of public cloud IaaS use cases.

Our long-term public cloud IaaS security strategy, supported by a robust IaaS security architecture, enables us to apply a compliance process not just to individual IaaS components but also to the entire cloud security configuration.

Other benefits include:

- Reduced cost through reuse of security tools and services
- More agile response to business needs
- Alignment between on-premises and public cloud IaaS security strategies and architectures

Key learnings pave the way for future work:

- Distributed accountability for IaaS security
- Effective discovery, vulnerability management, and compliance processes for IaaS use cases
- Strong identity lifecycle management process and data protection
- Choice of cloud-oriented solutions
- Cross-domain team building, combined with various skillsets

We continually assess and enhance security and privacy capabilities, processes, and people's skills to protect Intel's data and the data of our customers.

Contents

Acronyms

IaaS	infrastructure as a service
PaaS	platform as a service

Business Challenge

Like many organizations, Intel IT needs to enable business units to take advantage of the agility and technology provided by public cloud infrastructure as a service (IaaS) and platform as a service (PaaS) while maintaining high standards for information security.

Beginning in 2013, Intel business units began to move various workloads to the public cloud. Initially, business units were attracted to public cloud IaaS[1] for its cost effectiveness and ease of use. Today, while cost is still a deciding factor, access to emerging technology and nimble ramp-up of infrastructure resources are now the key motivators of public cloud IaaS adoption. Intel's business units seek to accelerate innovation, enter new markets, and reduce time to market. We are also enabling digital transformation of Intel IT's services, some of which run on public cloud IaaS.

Intel IT's Role: Move toward Shared Responsibility

Traditionally, Intel IT managed all aspects of a workload running in our enterprise private cloud, including applications and data, compute and storage resources, the network, and security. As more workloads and data move to public cloud IaaS, none of these aspects is exclusively controlled by IT any more. Instead, the responsibility for all these aspects is shared by IT, the business account owner, and the cloud provider.

Technology: New Control Capabilities

Our traditional enterprise security controls were not sufficient to regulate public cloud IaaS, so we deployed new capabilities to monitor and log events as data moves to public cloud IaaS. This includes new capabilities to inspect data as it moves to the cloud and new controls to block or warn of usages and risks as appropriate.

Processes: New Usages Require New Methods of Discovery

We continue to learn about the use cases and workloads that can run in the public cloud. We define new processes, supported by new technologies, to identify new cloud usages for business units and for IT. To meet our security policies, we also create new compliance processes as needed.

People's Skills: Continual Learning

Intel IT and business account owners continually learn about the opportunities and risks of using public cloud IaaS. We teach business account owners how to assess the types of data and services they are putting in the public cloud. Then we can develop the right level of controls to align with the value of the data.

[1] Throughout this paper, references to IaaS include PaaS.

Developing a Public Cloud IaaS Security Strategy

Creating a team from various IT domains, we have embraced public cloud IaaS usage and are enabling Intel's business units to quickly adopt a secure posture in the public cloud. We have built a strategy and architecture to enable secure usage of public cloud IaaS. The strategy represents a multiyear program that has resulted from a collaboration between many business functions and units. Our public cloud IaaS security strategy is built for the long term, focusing not only on technology (security tools) but also on the structure around technology.

Our public cloud IaaS security strategy reflects a commitment to security by design rather than a patchwork approach to security issues. As a result, our strategy not only establishes security today but also can adapt to future needs and use cases. We have established a close working relationship with the business units, in which Intel IT protects the workloads without slowing down business. We have accomplished this by defining a granular and simplified security policy that enables fast-track, low-risk usage of the public cloud. As public cloud IaaS usage becomes more widespread at Intel, we are expanding our security efforts to include a mixture of traditional approaches, new capabilities, and verification wrapped in a security-as-a-service framework.

As mentioned in the Business Challenge section, when we developed our public cloud IaaS security strategy, we felt it was important to address not just technology but processes and people's skills as well. In fact, without well-defined processes and knowledgeable staff, all the technology in the world cannot provide end-to-end security.

Key Learnings

Our success in helping business units adopt public cloud IaaS quickly and securely has come from the following key learnings:

- **Approach security holistically.** We include technology, processes, and people in our public cloud IaaS security strategy.
- **Establish distributed accountability.** Intel IT and the business account owner share the responsibility for security. Intel IT provides the security solutions and the overall governance and compliance without interrupting the business units' work. The business account owner takes responsibility for fulfilling the security requirements. The cloud provider, through contractual specifications, takes responsibility for supporting the infrastructure and for monitoring security with appropriate tools.
- **Implement an effective discovery process.** We have developed repeatable processes that help us discover which workloads are running on public cloud IaaS and then help us apply appropriate compliance controls.
- **Develop a strong data-protection policy.** We have well-defined compliance controls that protect intellectual property by allowing and protecting certain categories of data to be stored and used on public cloud IaaS.
- **Identify and implement security solutions that are designed for the cloud.** Rather than simply extending traditional on-premises enterprise security tools to the cloud, we prefer to take a security-as-a-service approach to providing public cloud IaaS security. Cloud-specific solutions tend to work better—and they tend to be more scalable and cost-effective—than on-premises security tools.
- **Make security easy for business account owners.** Our business units have a strong understanding of public cloud IaaS, but they may not know how to best protect Intel's intellectual property. Therefore, we educate business account owners about security issues and the tools that are available to them.
- **Understand the limits of our control.** As Intel IT's role shifts to include cloud brokering, we accept that not all workloads can run on-premises. We transfer the risk to our selected service providers, trusting them to follow business best practices and ISO standards. We think of it as "trust and obligate" (via contracts) instead of "trust but verify."
- **Take a team approach.** Our public cloud IaaS security team involves Intel IT staff from several functional domains to create a new set of IT experts that can provide a secure consumption of public cloud IaaS. For example, we need software developers who can help automate the use of cloud APIs. We invest in continual learning so that IT capabilities evolve as rapidly as public cloud use cases. We also work with cloud providers to further enhance security and compliance.

Improving the Technology

Software-defined security, by its nature, requires advanced techniques, such as machine learning, behavioral learning, automation, and distributed security. These technologies enable us to keep up with the changing public cloud and risk landscapes. Because security tools change often, it is important to create tool-agnostic controls. We have created a modular security architecture that allows us to quickly replace security solutions without redesigning the controls. For efficiency's sake, we are consolidating the security controls used for our enterprise private cloud and those used for public cloud IaaS, creating a unified control set that is a standard part of the hosting processes.

Technologies like machine learning and automation are founded on good data and context. Therefore, our public cloud IaaS security strategy depends on appropriate definitions of what data is important and then rigorous collection of that data.

Adapting Our Processes

With multiple business units running hundreds of workloads on public cloud IaaS, a one-by-one approach to establishing security was not practical. Therefore, software-defined security lies at the heart of our public cloud IaaS security strategy. This means that, just like public cloud IaaS itself, our security controls are API-driven so they can support a distributed, self-managed, autonomous approach that can defend itself and survive enterprise attacks. This method helps security solutions and operations to be easily reused and integrated.

To create API-driven security, we have coded security policy into our security tools so that the code "controls the controls." The APIs automate continuous discovery of approved and nonapproved public cloud IaaS usages as well as compliance, auditing, and self-healing. The greatest advantage to the API approach is its flexibility, which enables us—and the business account owners—to move fast without sacrificing protection.

We realize that technology and use cases change rapidly. In response, we evaluate our controls frequently so we can move between solutions quickly when necessary.

Another central change to our processes is the establishment of distributed accountability. Our security solutions are used by business account owners and by our security staff. In this way, we encourage business units to share accountability for security with Intel IT.

Training Our People

Technology and knowledge are both required to create robust public cloud IaaS security. Therefore, we invest in training our security personnel to build skills and encourage professional growth. Areas of training include automation, machine learning, cloud advantages, and the security-controls landscape.

We also rely on our cloud service providers' knowledge, realizing that the infrastructure has many aspects we do not know about. We select service providers that follow industry best practices and adhere to ISO standards that complement our public cloud IaaS security strategy. We maintain tight working relationships with the cloud provider's technical subject matter experts. For example, we have identified which OS versions cloud providers are using, which helps us develop better controls and address future risks.

Creating a Public Cloud IaaS Security Architecture

Our IaaS security architecture supports our public cloud IaaS security strategy. Since the security architecture could not be completed in a short time, we divided it into a two-phase project. First, we improved our discovery processes and established a foundational set of public cloud IaaS security controls. Change occurs quickly in the cloud and security environments. Therefore, in the second (ongoing) phase, we are refining our approach by doing the following:

- Building a cloud capabilities framework that supports security as a service
- Solidifying our operational and support model
- Architecting controls that enable higher data classifications to be utilized in the public cloud

PHASE 1
Improving Discovery and Establishing Controls

PHASE 2
Refining Our Controls

Phase 1: Improving Discovery and Establishing a Foundational Set of Controls

In phase 1, we developed ways to learn about which workloads are running on public cloud IaaS, which service providers are being used, and what data is being processed in the public cloud. We also established a foundational set of security controls that provided immediate information security enhancements, even if the solutions we initially chose were not the most efficient for the public cloud environment.

Making Public Cloud Use Cases Visible to IT

We worked closely with Intel's Purchasing department to discover which business units were using public cloud IaaS and for what purpose. We developed a cloud brokering process, which enables us to help business units choose a public cloud IaaS provider that matches the technical and other requirements of a particular workload. We established working relationships with our public cloud IaaS providers so they could help us learn about new use cases.

Applying Existing Knowledge

To move as quickly as possible, we applied our existing knowledge of tools for enterprise security compliance and management. The business units helped identify where security could be enhanced and provided feedback on a chosen solution to assist us in evaluating the solution's effectiveness.

As a result of this evaluation, we quickly realized that on-premises, private cloud security tools are not always the best choice for public cloud usage. First, the tools do not always work the same way in the public cloud that they do on premises. Second, they often fail to support the dynamic, highly-scalable, distributed nature of public cloud IaaS. Infrastructure instances in the public cloud can be created—and decommissioned—quickly, and many on-premises tools are not agile enough to handle this well.

To educate ourselves about tools that might work better in certain use cases, we performed internal research and also participated in peer-group discussions with other IT departments. As we identified potentially useful solutions, we evaluated them to determine whether they could integrate with our internal compliance tools. The result of this research led us to phase 2.

Phase 2: Refining Our Approach

We are now engaged in phase 2— Refining Our Approach. It is an ongoing process of keeping what is working well and changing what is not. We have learned that we must be flexible when selecting tools and suppliers. Public cloud IaaS use cases may store data or use infrastructure from one provider or another—and some may switch providers.

This flexibility also requires continual assessment of security controls. As an example, Figure 1 provides a snapshot of our current public cloud IaaS security architecture. Some of the controls are hosted on-premise, while others are hosted off-premise. However, the architecture may change as new technologies emerge, new public cloud services are offered, and the security-threat landscape evolves. Despite this constantly shifting landscape, our goal is to have all our security tools centrally available from a "single pane of glass" no matter where they are hosted.

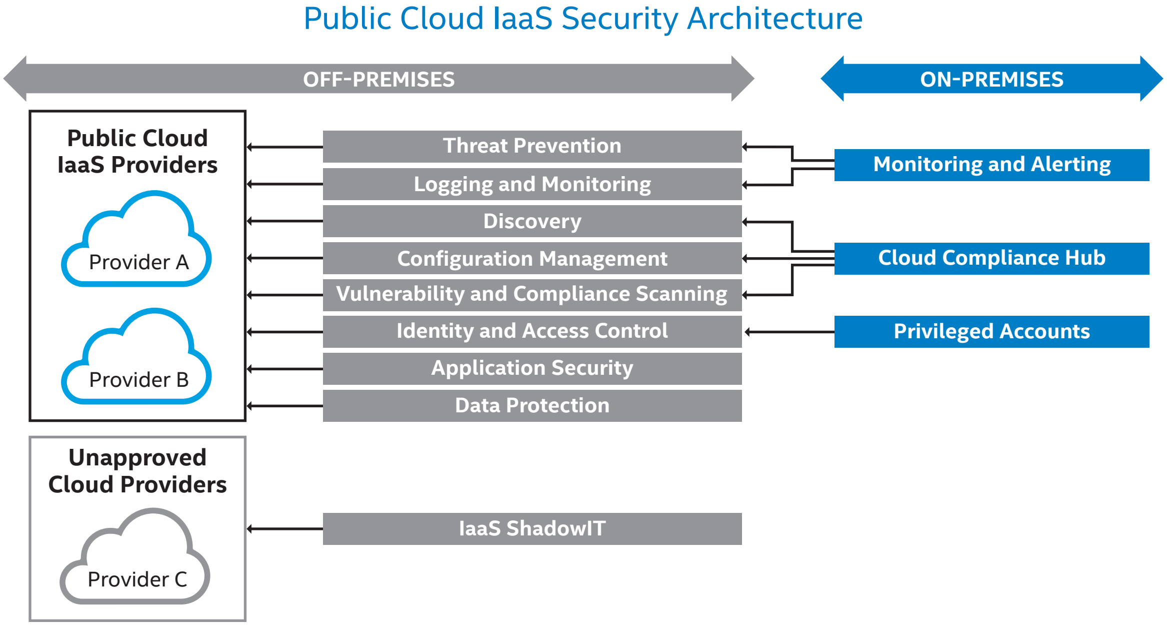


Figure 1. Our public cloud IaaS security architecture consists of many controls, some of which are hosted in the public cloud while others are hosted on-premises.

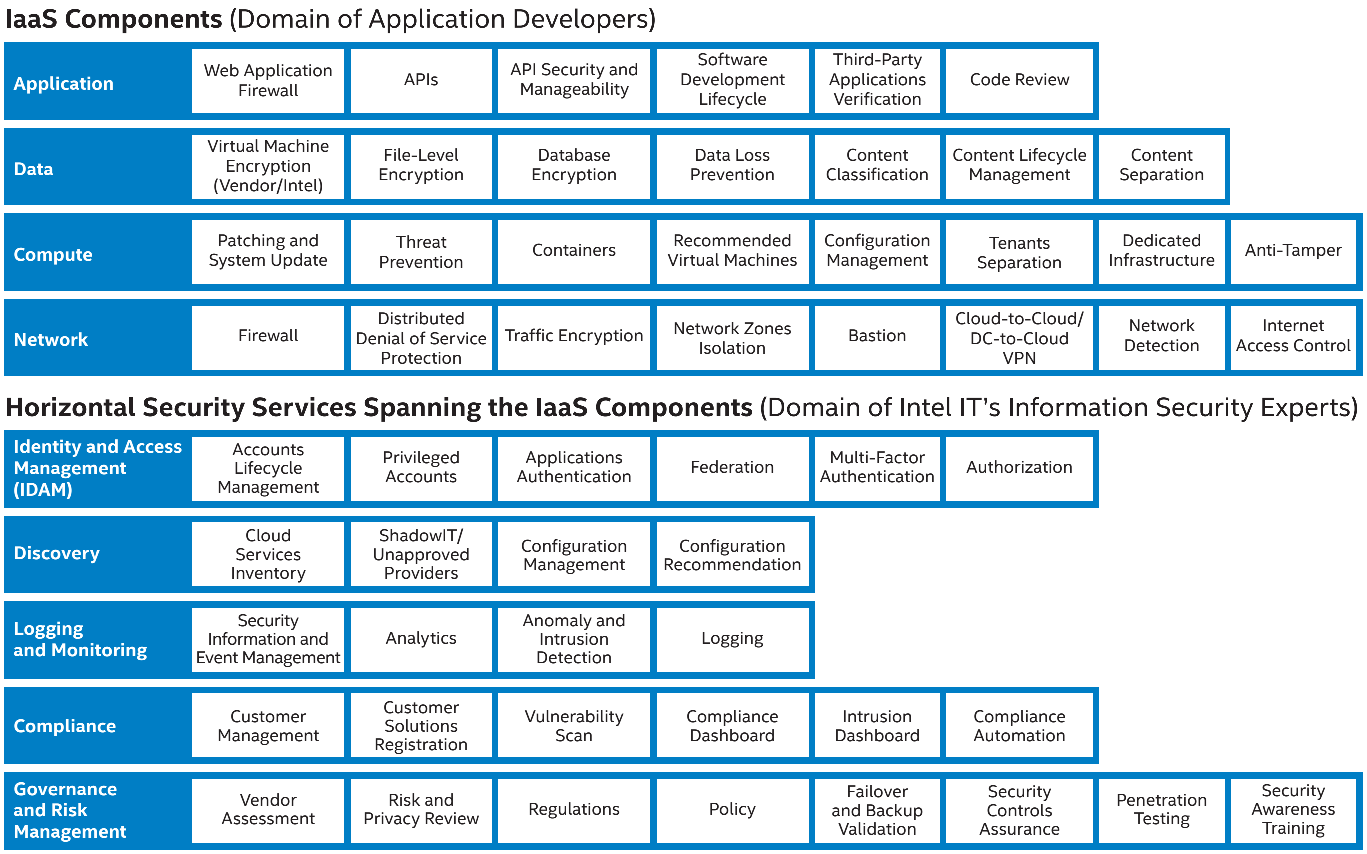
Cloud Capabilities Framework

To support our public cloud IaaS security strategy and architecture, we have defined a cloud capabilities framework (see Figure 2) that includes all IaaS components as well as horizontal security services that span those components. The IaaS components—applications (including APIs), data, compute, and network—pertain to the security efforts of application developers. The horizontal security services are the domain of Intel IT's information security experts.

These two concepts apply to every aspect of the cloud capabilities framework:

- **Asset management.** This is the process of identifying, maintaining, and disposing of assets continuously and effectively. Asset management is an essential component of our public cloud IaaS security strategy. All other horizontal security services depend on well-managed assets.
- **Privacy.** We strive to verify that our entire public cloud IaaS security architecture adheres to Intel Privacy Principles as we collect data about each IaaS deployment to help us identify and implement the necessary security controls. We notify customers according to these Principles and do not default to opt-in. We declare how we use the data, and we validate regulatory requirements for the countries in which application data must reside.

Table 1. Cloud Capabilities Framework Details, on the next page, provides details about each aspect of the cloud capabilities framework, including the challenges we encountered and how we solved them.



IaaS Components (Domain of Application Developers)

Application	Web Application Firewall	APIs	API Security and Manageability	Software Development Lifecycle	Third-Party Applications Verification	Code Review		
Data	Virtual Machine Encryption (Vendor/Intel)	File-Level Encryption	Database Encryption	Data Loss Prevention	Content Classification	Content Lifecycle Management	Content Separation	
Compute	Patching and System Update	Threat Prevention	Containers	Recommended Virtual Machines	Configuration Management	Tenants Separation	Dedicated Infrastructure	Anti-Tamper
Network	Firewall	Distributed Denial of Service Protection	Traffic Encryption	Network Zones Isolation	Bastion	Cloud-to-Cloud/ DC-to-Cloud VPN	Network Detection	Internet Access Control

Horizontal Security Services Spanning the IaaS Components (Domain of Intel IT's Information Security Experts)

Identity and Access Management (IDAM)	Accounts Lifecycle Management	Privileged Accounts	Applications Authentication	Federation	Multi-Factor Authentication	Authorization		
Discovery	Cloud Services Inventory	ShadowIT/ Unapproved Providers	Configuration Management	Configuration Recommendation				
Logging and Monitoring	Security Information and Event Management	Analytics	Anomaly and Intrusion Detection	Logging				
Compliance	Customer Management	Customer Solutions Registration	Vulnerability Scan	Compliance Dashboard	Intrusion Dashboard	Compliance Automation		
Governance and Risk Management	Vendor Assessment	Risk and Privacy Review	Regulations	Policy	Failover and Backup Validation	Security Controls Assurance	Penetration Testing	Security Awareness Training

Figure 2. To support our public cloud IaaS security strategy and architecture, our cloud capabilities framework encompasses all IaaS components—applications (including APIs), data, compute, and network—as well as a comprehensive set of horizontal security services that span those components.

Table 1. Cloud Capabilities Framework Details

COMPONENT OR SERVICE	DESCRIPTION	NOTES
PUBLIC CLOUD IAAS COMPONENTS		
Applications (including APIs)	The applications or services provided by the IaaS instance run on a number of web-application technologies.	We use the IaaS technology to scale up or down as needed. IaaS is commonly controlled by the APIs. We are enhancing our ability to use these APIs to automate discovery and provide more flexibility to our security-as-a-service approach.
Data	The data collected by the application or service hosted within the IaaS environment can be generated by users, machines, or applications and can be stored in a database or other storage method.	Our public cloud IaaS data policy states what categories of data are allowed on public cloud IaaS. Security controls enforce that policy, blocking or warning of inappropriate usage. We are in the process of implementing controls that will enable all categories of data to be securely used in public cloud IaaS use cases.
Compute	The compute components are the virtual instances created by customers to run their applications or services. These components interact with the network, databases, and other services to provide the intended application.	Our business account owners found substantial value in the ability to rapidly create and destroy virtual compute instances for short-term capacity needs and for application development and testing. These short-lived instances posed a problem for accurate compliance reporting because the instances were not active long enough for traditional compliance-reporting mechanisms to become aware of them. By understanding these use cases, we were able to create a process and policy that, when coupled with a compliance-reporting mechanism built for the cloud environment, yielded a more accurate overview of our security compliance.
Network	The network defines how application and data traffic is passed among the various components of the IaaS deployment. This traffic can stay local within a single private network or can be routed around the world to a cloud service provider's various data centers. In some cases the network may also connect to on-premises resources.	To decrease the attack vector, we are looking into best practices for which network interfaces should be exposed to the Internet and which should be blocked. We are also working to add the network into our compliance process. In addition, as we shift to software-defined networking, the role of the network is shifting to the application stack. We are increasingly using code, automation, and templates to control the network, thereby reducing configuration errors.
HORIZONTAL SECURITY SERVICES		
Identity and Access Management (IDAM)	We use federated single sign-on using Security Assertion Markup Language and OAuth with multifactor authentication to enforce privileged access controls on the IaaS platform.	We perform account lifecycle management for both IaaS service accounts and virtual machine (VM) local administration accounts. Account and identity data is reconciled from the IaaS and VM environments into the enterprise-access-governance system to support account lifecycle management, which is tied to HR and supply-chain processes.
Discovery	We employ a continuous process (both manual and automated) of discovering the public cloud IaaS use cases (both of approved and unapproved cloud providers), enabling us to take the relevant actions to bring services into compliance.	We work with Intel's Purchasing department and our public cloud IaaS providers to discover new use cases. Then we direct the business unit to our cloud brokering process. The brokering process helps to identify a public IaaS provider that supports the technical and other requirements of a particular workload.
Logging and Monitoring	Each service running on IaaS creates a log that we monitor for indications that unauthorized or malicious activities have been attempted or performed. Most IaaS components have the ability to generate audit logs, including the APIs themselves; these logs are an essential part of detecting threats and intrusions.	We have implemented a centralized approach to event logging so we need to look only in one place for alerts. We use threat intelligence to help identify threats and detect intrusions that attempt to subvert security controls before they succeed in compromising the confidentiality, integrity, or availability of the IaaS components.
Compliance	Compliance includes several areas of information security. It involves analyzing the vulnerability management data and applying the information obtained to provide effective follow-up actions so that the minimum security specifications are met.	Vulnerability scanning is a core part of our public cloud IaaS security strategy and is a cyclical process that continuously assesses and provides a real-time view of the security posture of the hosted service.
Governance and Risk Management	We define information security policies and requirements and measure each IaaS deployment against those policies.	Since each IaaS deployment is a unique infrastructure that needs to be secured, we apply: 1. Predeployment governance 2. Security requirements based on risk and regulatory compliance 3. Well-defined operational or continuous security controls

Operational and Support Model

As mentioned earlier, the distributed nature of public cloud IaaS deployments necessitates a distributed operational and support model (see Figure 3). For workloads running on public cloud IaaS, responsibilities do not reside solely with Intel IT. Instead, responsibilities are shared among the business account owners, the cloud service provider, Intel IT, and the Intel IT information security team. This distributed approach results in better, more efficient information security.

We understand that the business account owners may not understand the security and threat landscape as well as they understand their own IaaS needs, so we strive to provide training to them and make it easy to use the security solutions and controls that we provide.

Shared Responsibility for Public Cloud IaaS Security

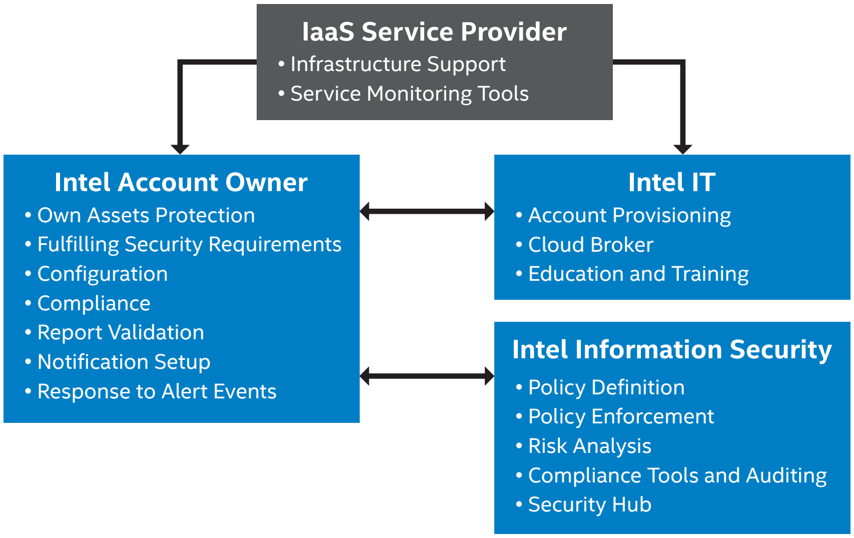


Figure 3. For workloads running on public cloud IaaS, the responsibility for security is shared between the Intel account owner (the business unit), Intel IT, the Intel IT information security team, and the IaaS service provider.

Results

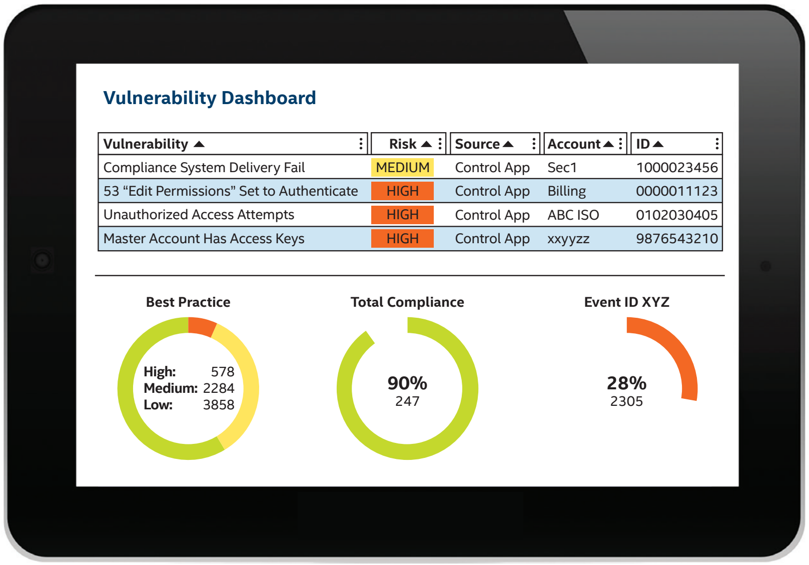
By developing a long-term public cloud IaaS security strategy supported by a robust IaaS security architecture and cloud capabilities framework, we can accomplish our mission of enabling business needs. Partnering with the business units enables us to meet our security objectives without limiting the business units' productivity and agility.

Results include the following:

- Enablement of security as a service, which reduces cost through reuse of security tools and services.
- The ability to discover primary public cloud IaaS use cases and workloads.
- Deployment of agile cloud security controls to support faster response to business needs and security.
- Enhanced identity lifecycle management and access controls for privileged accounts, including system accounts.

- A cross-functional team in which various subject matter experts share knowledge and solve problems.
- The development of a cloud security hub (see Figure 4) that integrates all cloud security data sources and security tools. This hub enables account owners and the Intel IT information security team to examine the cloud security status and matrix, avoiding the need to interact with multiple security tools.

Cloud Security Hub



Vulnerability Dashboard

Vulnerability ▲	Risk ▲	Source ▲	Account ▲	ID ▲
Compliance System Delivery Fail	MEDIUM	Control App	Sec1	1000023456
53 "Edit Permissions" Set to Authenticate	HIGH	Control App	Billing	0000011123
Unauthorized Access Attempts	HIGH	Control App	ABC ISO	0102030405
Master Account Has Access Keys	HIGH	Control App	xxyyzz	9876543210

Figure 4. A cloud security hub improves efficiency and accuracy by centralizing cloud security information and tools.

Next Steps

Our approach to public cloud IaaS security has evolved over the past year. We have more work to do. Examples include:

- Further automation of security configuration, discovery, and compliance.
- Secure new usage models that accommodate high-sensitivity workloads.
- Continue to refine both our public cloud IaaS security strategy and our security architecture, looking for services we can consume instead of building our own.
- Develop a well-defined process for evaluating newly discovered use cases that do not currently use an approved public cloud IaaS supplier.
- Consolidate processes and solutions, including those that can integrate into our current processes.
- Continue to build a cross-domain information security team that can help Intel IT skills and capabilities evolve as quickly as public cloud IaaS use cases.
- Enable additional public cloud IaaS providers and additional technologies, such as container security.
- Enhance threat detection through increased automation and use of cloud-focused security services.

Conclusion

As we work to enable end-to-end public cloud IaaS security, we have learned some important lessons:

- Business units will continue to use a mix of public cloud models and enterprise private cloud models as appropriate to their needs.
- A well-defined security strategy is crucial for supporting the use of public cloud IaaS.
- The best way to start is to determine what is most important to secure and then research to find the most appropriate solution.
- For public cloud IaaS security, the solutions that work best are those designed for the cloud.

With foundational safeguards in place to protect information and intellectual property, we are enabling business units to select the solution that suits their needs, improving business agility and supporting innovation while maintaining necessary security. Public cloud is constantly growing and changing. Our strategy is to take a long-term approach; we have approached this effort not as a sprint but as a journey. Our public cloud IaaS security strategy and cloud capabilities framework set the stage. In the future, we will continue to learn, consolidate processes and solutions, and enhance public cloud IaaS security.

For more information on Intel IT best practices, visit **www.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

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

- SaaS Security Best Practices: Minimizing Risk in the Cloud paper
- Taking Enterprise Security beyond the Edge 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. Check with your system manufacturer or retailer or learn more at intel.com.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

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.

Printed in USA ♻ Please Recycle 0117/ERAI/KC/PDF