White Paper
January 2021

# IT@Intel Next Step to Multicloud: Native Cloud Security Controls

As we evolve our multicloud strategy and as cloud security matures, we are able to boost business agility, improve user experience, and reduce complexity by taking advantage of cloud service providers' integrated security solutions


## Intel IT Authors

**Andrew Ambrosia**
Vulnerability Management
Product Owner

**Mitch Baskette**
Vulnerability Assessment
Solution Architect

**Kevin Bleckmann**
Cloud Solution Architect

**Samion Kuptiev**
Compliance Management
Product Owner

**Shachaf Levi**
Cloud Security Architect

**Shahar Rand**
Cloud Security Engineer

**Dave Shrestha**
Cloud Solution Architect


## Table of Contents



## Executive Summary


Intel IT has replaced many of our third-party security solutions with native cloud security controls. We made this significant change to our multicloud strategy because of three reasons:

- Technology: Cloud service provider (CSP) integrated security controls have matured to the point where many of them meet our stringent security requirements.
- Process: We standardized our cloud security processes so that we can better understand and work with CSPs.
- People: Our team embraces change and has acquired the necessary skillset.

It is important to note that where needed and as part of due diligence, we continue to use some third-party solutions to augment native controls. We evaluate each cloud-based security control to verify that it meets our minimal viable product requirements. This helps us provide Intel with "defense in depth."

We've been adjusting and streamlining our multicloud strategy for several years, and the process is not yet over—there is still much to learn and more changes to make. But the move to native cloud security controls has produced significant business benefits, including faster deployment and business agility; more consistent, cloud-native user and developer experience; and reduced complexity and costs.

## Contributors

**Christine Coe,** Enterprise Hosting Manager
**David Fong,** Info Security Risk Management Specialist
**Jeff Sedayao,** Industry Engagement Manager
**Jessica Tran,** Cloud Security Specialist


## Acronyms

| | |
|---|---|
| **CIP** | Cyber Intelligence Platform |
| **CSP** | cloud service provider |
| **OU** | organizational unit |

## Business Challenge

Intel IT's transition to multicloud began nearly a decade ago. Intel's business units often want to use multiple cloud service providers (CSPs) because they meet different business needs. Our multicloud strategy provides the flexibility, scalability, availability, agility, and mobility that Intel needs to compete in today's fast-paced business environment. However, we found it difficult and costly to integrate and revise on-premises security capabilities as business units switched from one CSP to another. We decided to evaluate how we could enhance and streamline our security in the public cloud, as part of our commitment to improving our strategies and processes.

At the outset of the public cloud era, many CSPs had relatively immature security capabilities that did not meet Intel's security requirements. Thus, we often used third-party cloud security solutions. While these solutions helped us to improve our public cloud security posture, they also posed challenges:

- Integration is often complex, which increases costs and delays deployment.
- Inconsistent and non-cloud-native user and developer experience.
- Lack of security capabilities that are part of our minimal viable product definition.
- Failure to deliver true multicloud support, where the solution touts support for multiple CSPs but in reality only includes a full set of features and capabilities for one CSP; in some cases, there was no third-party solution for a particular CSP.
- Licensing fees, which can be expensive, increase the cost of security.

These challenges highlighted the need to use native CSP security offerings as much as possible.

## Solution

The cloud security industry has greatly matured. In addition, we have grown our own skill sets and processes, so we can better assess the end-to-end value and impact of transitioning to native cloud-based security controls. The combination of these two trends presented an opportunity to evolve our multicloud strategy and improve both security and user experience.

During the past year, our cross-IT team extensively tested the native cloud security controls of two major CSPs. We determined which native capabilities are applicable to our strategy and which of these offerings had matured to the point where we could "go native." As we transitioned from third-party security solutions to native CSP security solutions—where possible—we had three primary goals (see Figure 1):

- Meet our security requirements natively in the CSP's platform.
- Improve the user and developer experience by allowing them to work intuitively in the native platform, and through proactive controls integration—all of which can lower our support cost as well as reduce the burden on our tenants.
- Ensure compatibility and integration with on-premises processes such as data correlation, threat management, enforcement, and remediation.

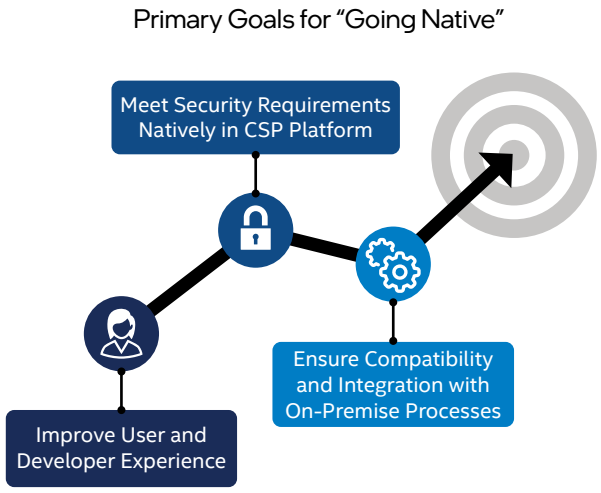


**Figure 1.** We are aiming to achieve several goals by transitioning from third-party security solutions to native cloud security controls.

Examples of native cloud security controls that we are using include threat detection as a service, key management service, web application firewall, vulnerability assessment agents, and integrated security consoles. However, we currently don't use native cloud security controls for every aspect of security. Instead, we defined a minimal viable product and performed a thorough validation to verify that a CSP's control is ready. In some cases, we still use third-party solutions such as for identity and access management; our Cyber Intelligence Platform (CIP), which includes a security data lake based on Splunk and Kafka; and network and application scanning. Figure 2 illustrates our conceptual multicloud security architecture, which is characterized by the following:

- Business enablement
- Native solutions
- Guard railing and automation
- Proactive compliance
- Cost efficiency

## Implementing Self-Service, Guard Rails, and Automation

Cloud security is unique from on-premises security because it is developer-driven, and everything—including infrastructure and security—is code. Users and developers can use APIs and command lines to make changes at scale. As we pursue continuous improvement and development throughout the lifecycle of the cloud security experience, we have implemented self-service and guard rails to streamline our processes and onboarding workflows. Self-service and guard rails are key to using native cloud security controls.

Self-service means that a business unit account owner can set up a cloud account without direct IT involvement. Guard rails are automated security policies that reduce the attack surface. They can be of three types:

- **Proactive**. Prevents a business unit account owner from doing something (intentionally or unintentionally) that violates our security policies or best practices. For example, a proactive guard rail prevents unrestricted public access to storage or blocks access to hazardous network ports.
- **Automated**. Controls are applied once services have been turned on and are being used by a business unit.
- **Reactive**. Notifies a business unit account owner of an issue, such as changes that have been made to security group permissions.

One example of a guardrail is disabling administrative ports such as 3389 or 22 at account set up. Another example is requiring all storage to have access control lists and limited internet exposure. This helps us and the business units to minimize the risk from the start.

The guard rails are constantly evolving to balance security against business demands. And there are always exceptions, because we must remain flexible to meet business needs. In addition to the guard rails, we rely on the CSP to implement industry benchmarks and best practices.

Through the use of native cloud security controls, proactive compliance is now attainable. These services improve the integration of typically segmented controls while helping to ensure cloud account configuration consistency. They also enable a reusable and modular security process and improve the user and developer experience, because the services are embedded in their cloud experience.

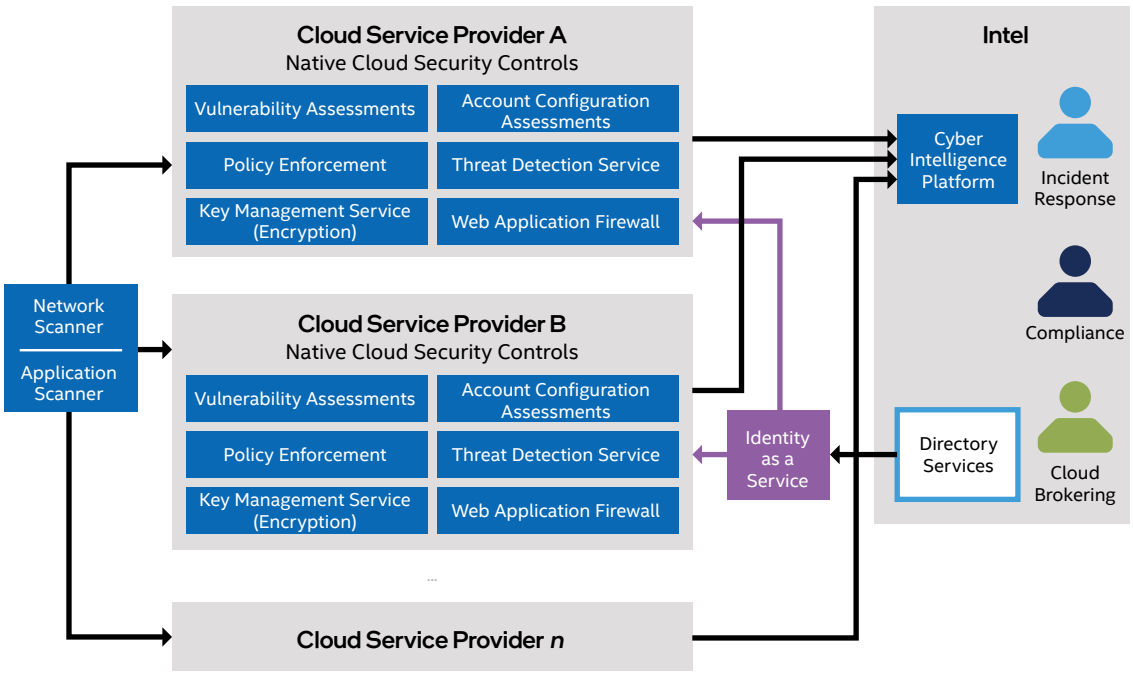


**Figure 2.** When using native cloud security controls, security processes are on-premises and the data comes from the CSP.

Figure 3 shows how we apply the native cloud security controls and policies across account owners to support different environments' lifecycle and risk requirements. For instance, a development environment may have different requirements than a production environment. Similar accounts are grouped into an organizational unit (OU), and all accounts are governed by the same policies and controls. For example, we prevent network management for accounts that are connected directly to Intel networks by placing these accounts in a special OU and blocking network management with policies applied at the OU level.

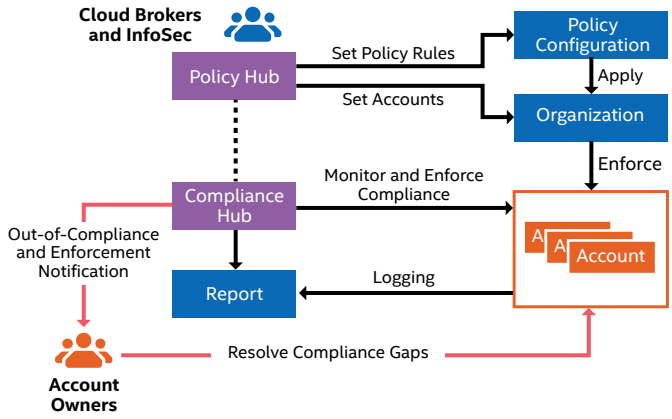


**Figure 3.** We use OUs to group accounts with similar needs. Policies and controls are applied at the OU level and apply to all accounts within that OU.

## Improving Efficiency

Cloud security efficiency is essential for Intel IT. Evaluation, analysis, and correlation determine which function and process will consume the data. Those steps, along with lifecycle management and determining time to detect, will help meet the business requirements and service level agreements such as Recovery Time Objectives and Recovery Point Objectives. They will also add value without incurring costs through acquiring more data than is required. For example, instead of sourcing unnecessary data with potentially increased costs, security events are filtered to focus on critical and necessary event-related data prior to consumption. We constantly communicate with our Security Operation Center and Incident Remediation Team to determine what data they need. This is a balancing act—obtain enough data to be effective without too much noise. For compliance data, we filter at the source, pulling only the relevant data that is required for vulnerability management. If business unit account owners require more information, they can use the native cloud security portal directly.

Native cloud security controls can help improve efficiency and agility because the implementation of one or more controls occurs automatically and dynamically, as quickly as possible. Integrating and deploying a third-party solution often took several days. Also, visibility and resource risk posture can be assessed more efficiently because information is immediately available through the CSP environment. And finally, initial implementation scales with feature and service enhancements, thereby reducing repetitive effort and complexity.

## Building Relationships

Using native cloud security controls doesn't occur in a vacuum. We developed a strong working relationship with the CSPs, with a collaborative conversation about features and the user experience. Because Intel IT is similar to many large corporate IT shops, when we ask for a certain feature, the CSPs understand that feature is probably desirable across the IT industry. This collaboration benefits us, as well as the CSP. We become aware of their roadmap for cloud security posture management, and our feedback helps them to fine tune features, fix issues, and decide what's next for their product. The CSPs also work with the Intel business unit account owners. When a business unit account owner asks for something, the CSP can communicate best practices for security controls to help them avoid security vulnerabilities. The resulting three-way conversation between Intel IT, the CSPs, and the business unit account owners, with mutual responsibility for maintaining security, is a win-win for all involved.

### Extending Our Strategy to Additional CSPs

While we generally work with just two or three global cloud service providers (CSPs), our multicloud strategy and our experience with using native cloud security controls enables us to act quickly when the need arises. For example, prior to the outbreak of COVID-19, Intel IT worked with a Chinese-based CSP and the Tokyo Organizing Committee of the Olympic Games (Tokyo 2020) to apply Intel® technology to 3D Athlete Tracking (3DAT). This application uses artificial intelligence with near real-time insights and overlay visualizations during athletic events to enhance the viewing experience.

Although the pandemic postponed the Olympics competition, our existing industry-standard best practices and multicloud processes for evaluating and using native cloud security controls, as well as for performing vulnerability management, enabled us to be ready to work with a new CSP and use Intel technology in innovative ways.

# Results

We use two pillars to gauge the success of our security strategy: business enablement and business agility. We work with Intel's business units to drive new business that uses the public cloud, and we strive to deploy solutions quickly. Since adopting native cloud security controls where possible, we have achieved the following benefits:

- **Improved time to market and security.** CSPs often enhance their existing services, or offer a new service such as storage, compute, or containers. Because the native cloud security capabilities are already integrated into the CSP's release process, Intel's business units do not have to wait for us to deploy new changes, so they can adopt cloud-based solutions faster. Security becomes part of a seamless

user or developer experience. We can organically grow with the industry and the CSPs, taking advantage of whatever innovative technology they decide to offer.

- **Reduced complexity.** Native cloud security controls enable Intel's business units to take advantage of the deep integration with the CSPs' products and their rapid cadence of releasing new capabilities. We do not have to deploy third-party products, which may not be compatible with a CSP's changes.
- **Cost savings.** Direct cost savings have amounted to about USD 2 million per year in third-party licensing fees. Indirect cost savings accrue from not spending about 20 hours per month on processing agent exceptions or installing missing agents. Also, because many CSPs provide first-level support when issues arise with a security control, our support costs are reduced.
- **Better visibility and confidence.** Because security control agents are automatically installed, we have gained an 8 to 10 percent improvement in security visibility for virtual machines. Also, because the security controls are part of the CSP's security certification, they have been thoroughly validated by both the CSP and our team.
- **Enhanced user and developer experience.** The use of third-party security solutions resulted in an inconsistent user and developer experience. Web-based interfaces were different, and the solutions often weren't hosted on the CSPs' infrastructure, which caused delays in information due to data transfers. Now, users and developers have a cloud-native experience, with consistency across the CSPs' portals and accounts. Integration is simplified, and most problems can be resolved with a few mouse clicks to bring a configuration into compliance. In addition, now Intel's business units are speaking the same language as the Intel Information Security team.

## Key Learnings (So Far)

By using native cloud security controls, we are securing the business wherever it needs to do business. Here are some things we've learned along the way, realizing that our journey is not complete and that we have more to learn.

- **With change comes risk.** CSPs have a rapid cadence of changes to security configurations. Although they test their own products, they don't necessarily test our configuration of their products, which can lead to breakage and downtime or security risks. For example, if they change an API, the data we are expecting may not arrive, which can lead to unseen vulnerabilities or delayed incident response. It could be easy to just assume the CSP is taking care of everything—that's a mistake. Success requires that we pay close attention so that nothing breaks. There is a need for a constant CSP partnership as they evolve and improve their solutions.
- **Embrace change and keep up.** Now instead of one platform, we must understand multiple solutions with different taxonomies. But if we understand the basics, that is a good foundation. Our IT teams must embrace the change, be eager to learn, and be willing to up-level skill sets as cloud security professionals. We are staging ourselves to grow with the CSPs, but for continuous improvement we need to keep up.

It could be easy to just assume the CSP is taking care of everything—that's a mistake. Success requires that we pay close attention so that nothing breaks.

- **Invest in our teams**. By adopting native capabilities and moving away from a single platform, we seized another opportunity for organizational growth and skillset development—which is always our long-term strategy. The reduction of licensing costs outweighs the increased training.
- **Continue to expand our reach and collaborate with business units.** Although the native solutions make it easier for business units to consume cloud services as well as security controls, we still need to work with business unites to encourage them to embrace our security processes and increase compliance across Intel.

It is inevitable that we will make mistakes and learn more as our journey continues—that's the eternal IT challenge. But as we learn, we'll also improve and close gaps. For example, we are still using third-party and non-native solutions in a few security domains. We are working to integrate those with the native solutions to create a comprehensive security stack.

### Intel IT's CIP

Intel IT is transforming our approach to Information Security by deploying a new Cyber Intelligence Platform (CIP) based on leading-edge technologies, including Splunk and Apache Kafka. Our new platform ingests data from hundreds of sources and security tools, providing context-rich visibility and a common language and work surface around our data. It significantly improves productivity, efficiency, and effectiveness across our entire Information Security organization. Access to real-time data, streams processing, machine-learning tools, consistent data models, and orchestration and automation capabilities decrease the time it takes to detect and respond to increasingly sophisticated threats and ultimately leads to faster insights for prevention.

Our CIP infrastructure is based on Intel® Xeon® Platinum processors, Intel® 3D NAND Solid State Drives, and Intel® Optane™ SSDs, providing the compute power our security experts need to gain faster and more intelligent insights while reducing time to pivot between security tools. For more information, refer to the first two papers referenced in the Related Content section.

## Next Steps

We completed the first and major leap of going native for cloud security. However, our work is not done. The business usage and industry will keep evolving. Some areas we are considering include the following:

- We will continue to improve the ease of integration, working with CSPs to continue to enhance user and developer experience, operational efficiency, and security.
- As cloud services constantly evolve, increase in number, and become tightly integrated, we must plan for the next level of cross-services and solutions security, which will identify exposures created by multiple service integrations.
- Our controls cover the majority of the business units' needs. In the few areas where our security solutions are not compatible or within business unit requirements, we will work to close the gaps, extend our reach, and engage with Intel's business units to bring their use cases in line with our standard cloud security architecture.

## Conclusion

Our multicloud strategy lets us use the public cloud 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, and improves the user and developer experience. Although we've had a multicloud strategy for several years, we continually try to streamline and enhance it. As the cloud industry and CSPs evolved, we saw an opportunity to do due diligence (across people, processes, and technology) and update our strategy. We will continue to do so as the industry continues to change and mature, and as we continue to learn and apply evolving best practices.

Replacing many third-party security solutions with native cloud security controls has produced significant business benefits, including reduced costs, better integration and business agility, and improved user and developer experience. In addition, the use of native cloud security controls lets Intel's business units select multiple vetted clouds for various unique business models, while helping keep Intel's intellectual property secure. Although we use multiple native cloud security controls, we also use some third-party solutions to provide defense-in-depth and to augment CSP security offerings.

Our multicloud journey—as part of the larger digital transformation for all of Intel—is everlasting, and the public cloud environment and capabilities are experiencing rapid change that we must keep pace with. We will continue on our journey, adjusting our pace and direction as necessary. We may never "arrive," since the landscape is constantly changing, but we will strive to adjust and to rapidly learn new skills to stay ahead as the business grows and evolves.

## Related Content

If you liked this paper, you may also be interested in these related Intel IT papers:

- Transforming Intel's Security Posture with Innovations in Data Intelligence
- Building a Modern, Scalable Cyber Intelligence Platform with Apache Kafka
- Building a Multi-Cloud-Ready Enterprise Network
- Securing the Cloud for Enterprise Workloads: The Journey Continues
- Intel IT's Multi-Cloud Strategy: Focused on the Business
- Security Architecture Enables Intel's Digital Transformation

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

### 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 Peer Network

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

 0121/WWES/KC/PDF 345185-001US