SOLUTION BRIEF
Security
August 2019

IT@INTEL

Security Architecture Enables Intel's Digital Transformation

Intel IT's Enterprise Security architecture enables business units to focus on their goals while maintaining security standards

Executive Summary

Enterprise Security (ES) is critical to protecting Intel's intellectual property, assets, and the overall business operation. As data becomes increasingly dispersed across platforms and solutions, the threat landscape is also changing and becoming more sophisticated, requiring Intel IT to continue to make security a priority. While technology is a key part of the security model, the purpose of security is to enable the business to rapidly meet its goals in a competitive marketplace—making it safe for Intel to go fast.

Intel IT developed an integrated ES architecture using a modular, service-based design that decentralizes security and fosters a collaborative relationship with business units and their development teams. This has helped business units deploy solutions more quickly and resulted in better roadmaps and planning. It is our perspective that ES enables Information-Security-as-a-Service (ISaaS)—easy and consumable, so we provide clear guidelines and training for Agile Persistent Teams (APTs), work closely with them, and verify implementations.

With our integrated ES architecture, we have achieved the following:

- **Greater business flexibility.** We collaborate with business units and provide clear security guidelines, applying a "trust-but-verify" model.
- **Improved business enablement.** By removing many interdependencies, we make security easier and more consumable, and the modular approach allows us to rapidly respond to threats and new business demands.
- **Reduced technical debt.** The integrated ES architecture creates a framework for applications to adopt modern integration standards.

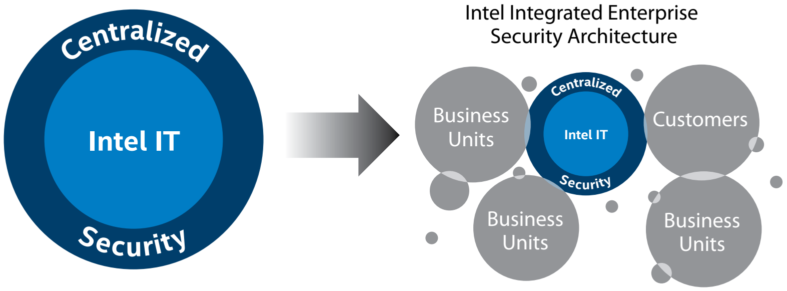


Figure 1. Integrated Enterprise Security architecture decentralizes security, giving more flexibility to business units while maintaining security standards with comprehensive guidelines and oversight.

Authors

Dennis Morgan
Chief Security Architect, Intel IT

Shachaf Levi
Cloud Security Architect, Intel IT

Jason Devoys
Enterprise Security Architect, Intel IT

Table of Contents

Intel IT Contributors

Jeff Sedayao, Industry Engagement Manager
Omer Ben-Shalom, Enterprise Security Architect, CTO Office
Eran Birk, Principal Engineer
Harish Thanneer, Principal Engineer, Enterprise Security Architect
Eric M. Monroe, Data Architect, Data Scientist
Roy Ben-Ezer, Solution Architects Manager
Sridhar Mahankali, Principal Engineer

Acronyms

APT	Agile Persistent Team
BDAT	business, data, applications, technology
ES	Enterprise Security
IAM	Identity and Access Management
ISaaS	Information Security-as-a-Service
TOGAF	The Open Group Architecture Framework

Business Challenge

In today's data-driven marketplace, Intel's continued success hinges on quickly adapting to changing security threats and new opportunities through innovation and digital transformation. Data is everywhere—in the cloud, on mobile devices, sensors, edge devices, remote assets, automation systems—and the list of sources continues to grow. The sheer volume of data continues to grow exponentially, comprising a significant percentage of Intel's assets. Securing this data in a shifting threat landscape plagued with ever-more-sophisticated hacker methodologies has become increasingly difficult.

Intel IT does not focus on technology for technology's sake. We use technology to help Intel's business units meet their goals. Therefore, changes to security technology must be associated with risk reduction, compliance, time to detection, remediation, and recovery. We recognized the need for a modular approach to information security that focused on the business and Information Security-as-a-Service (ISaaS) to better meet these needs. We also wanted to make security an easily consumable offering for business units—to get out of the way and allow them to rapidly achieve their goals while still providing solid security solutions. We moved from a traditional centralized security model to a more distributed, federated model and adopted a Persistent Agile methodology and modularized the approach to Enterprise Security (ES) architecture.

Solution

We developed an integrated, modularized ES architecture with end-to-end integrated reference and solution architectures. This methodical, service-based approach enabled us to integrate ES architecture and provide a better view into how deployments are connected and the impact on the overall ecosystem when one application is affected by a security threat. The modularized approach decentralizes security and provides clear guidelines so business units can move more quickly with implementations, solving problems, and achieving their goals.

Information security is a significant value stream across all of Intel's business units. Security functions include cyber defense, digital identity and access management, and compliance risk and awareness. Security capabilities at Intel are mapped to the Center for Internet Security's 20 critical security controls (CSCs) and are used to align the security architectures that comprehend business, data, application, and technology (BDAT) architecture domains.[1]

With our integrated ES architecture, we have achieved the following:

- **Greater business unit flexibility.** Through collaboration with the business units, we take a "trust-but-verify" approach by collaborating, mapping existing and future needs, and providing clear security guidelines.
- **Improved business enablement.** Standardization and modularity have removed many of the interdependencies between implementations, so we can address specific threats with less impact to other business activities.
- **Reduced technical debt.** The integrated ES architecture also decreases our overall technical debt and serves as a springboard for applications to adopt modern integration standards.

This methodical, service-based approach enabled us to integrate ES architecture and provide a better view into how deployments are connected and the impact on the overall ecosystem when one application is affected by a security threat.

Ecosystem Optimization

The modular design (see Figure 2) provides a comprehensive understanding of how deployments and processes affect each other. We use a service-based approach to replace components, such as a vulnerability scanner or logging system, without taking other processes in the architecture off-line. This approach is possible because each component is wired directly to the service bus architecture, rather than in the more traditional daisy chain configuration. Implementing new tool sets and capabilities to keep up with or get ahead of the changing threat landscape is easier and more efficient. In addition to saving time on implementation, the modular micro-service approach improves our ability to maintain services and respond to critical threats. Using various technologies, we complete security tasks such as data protection, discovery and scanning, application and service security, access control, network security, logging and monitoring, endpoint protection, compliance, and physical access.

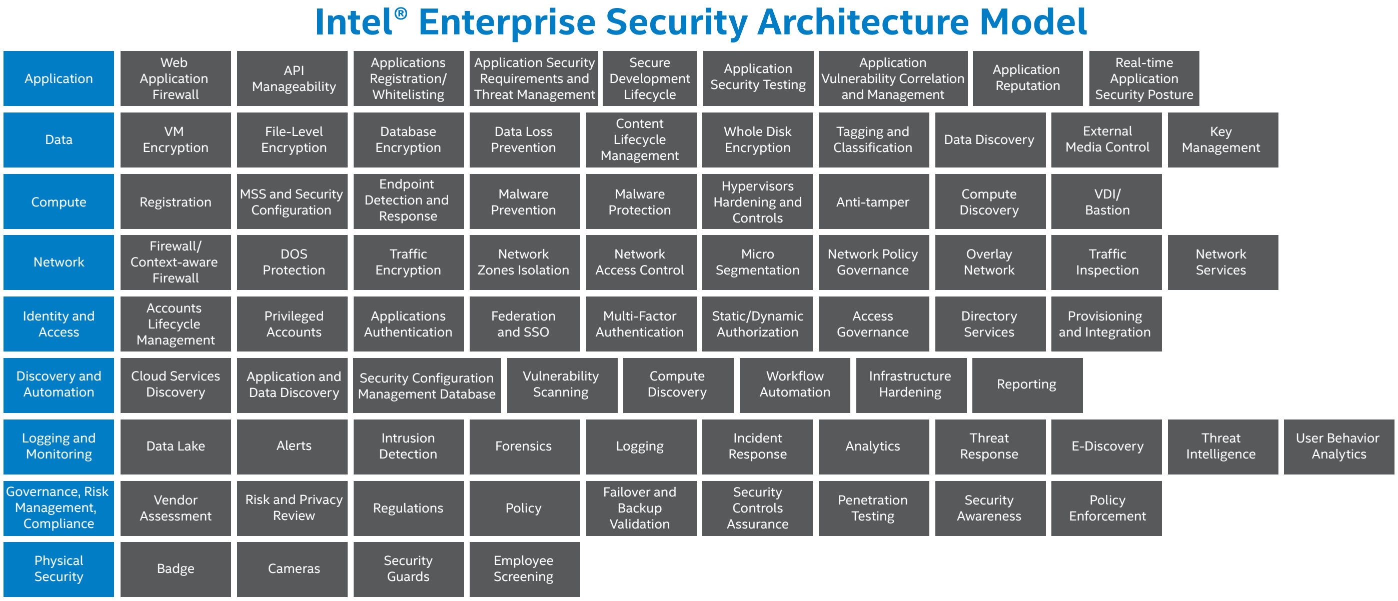
Integrated ES architecture gives business units more flexibility in their own implementations. When it comes to large-scale supplier negotiations, we have the ability to move quickly—in weeks rather than months—which improves response to requests.

Standardization

We embraced The Open Group Architecture Framework* (TOGAF*) standard to develop a consistent vocabulary across the ES architecture, standardizing and reducing the number of definitions and references.[2] We can now reuse and adapt existing models for new implementations rather than inventing new ones. While it was a journey to build the architecture, we can now offer training and certification for architects, system administrators, and developers across the enterprise to help ensure adoption. Now that everyone is speaking the same language with a consistent vocabulary and reference designs, architects can better collaborate and align with the business units and changes can occur more quickly. For example, when building the cloud architecture, we reused definitions from the ES architecture to quickly identify the providers and the consumers of the artifacts.

Identity and Access Management (IAM) is a good example of a process we use to help business units move faster. All Intel applications require user authentication and authorization, and using industry standards promotes pluggable architecture. Once the IAM architects define all of the user access patterns (the authentication capabilities and the process), the rest of the architecture teams can reuse the artifacts and collaborate within a common set to remove duplication and gaps. We also work with our micro-services teams to develop sample code and client libraries in different programming languages that application developers can then drop into their development projects.

Standardization allows us to automate and reduce the integration points. When a service or a solution is defined in the architecture, it can be easily reused, and in-turn, the integration points are shared. For example, account-level encryption key management and launching security logs are automated when an asset is created, without the requester having to think about it. The result is that everything operates automatically behind the scenes, based on the architecture definitions.



Intel® Enterprise Security Architecture Model

Application	Web Application Firewall	API Manageability	Applications Registration/ Whitelisting	Application Security Requirements and Threat Management	Secure Development Lifecycle	Application Security Testing	Application Vulnerability Correlation and Management	Application Reputation	Real-time Application Security Posture		
Data	VM Encryption	File-Level Encryption	Database Encryption	Data Loss Prevention	Content Lifecycle Management	Whole Disk Encryption	Tagging and Classification	Data Discovery	External Media Control	Key Management	
Compute	Registration	MSS and Security Configuration	Endpoint Detection and Response	Malware Prevention	Malware Protection	Hypervisors Hardening and Controls	Anti-tamper	Compute Discovery	VDI/ Bastion		
Network	Firewall/ Context-aware Firewall	DOS Protection	Traffic Encryption	Network Zones Isolation	Network Access Control	Micro Segmentation	Network Policy Governance	Overlay Network	Traffic Inspection	Network Services	
Identity and Access	Accounts Lifecycle Management	Privileged Accounts	Applications Authentication	Federation and SSO	Multi-Factor Authentication	Static/Dynamic Authorization	Access Governance	Directory Services	Provisioning and Integration		
Discovery and Automation	Cloud Services Discovery	Application and Data Discovery	Security Configuration Management Database	Vulnerability Scanning	Compute Discovery	Workflow Automation	Infrastructure Hardening	Reporting			
Logging and Monitoring	Data Lake	Alerts	Intrusion Detection	Forensics	Logging	Incident Response	Analytics	Threat Response	E-Discovery	Threat Intelligence	User Behavior Analytics
Governance, Risk Management, Compliance	Vendor Assessment	Risk and Privacy Review	Regulations	Policy	Failover and Backup Validation	Security Controls Assurance	Penetration Testing	Security Awareness	Policy Enforcement		
Physical Security	Badge	Cameras	Security Guards	Employee Screening							

Figure 2. Intel IT's integrated Enterprise Security architecture uses a modular, service-based design that provides a comprehensive view of all deployments across all environments, making it easier to isolate threats without impacting other deployments.

Collaboration

Enterprise architecture and the Scaled Agile methodology[3] are not mutually exclusive. IT security architects work with Agile Persistent Teams (APTs) across IT and business units to ensure that our models align with the business goals, both now and in the future. All quarterly release planning sessions include IT architects, and the Information Security group has been a leader in adopting the Scaled Agile processes across IT. We can now quickly adopt new use cases and address threats, while keeping business priorities at the forefront. Within the Information Security group, architects collaborating with the APTs gather feedback and requests for changes while providing guidance. The mutual feedback helps fine-tune and prioritize execution from strategy to release planning and implementation (see Figure 3).

Clear and specific security guidelines empower business units to implement capabilities through a decentralized, federated model. We review the business implementation plans, identify vulnerabilities and, whenever possible, provide solutions that do not interfere with business unit work. We also provide feedback on how business unit products fit into the architecture. Rather than representing a security roadblock, we can now focus on meeting the business goals first, accelerating delivery of effective, scalable solutions to support Intel's digital transformation.

From a people perspective, the architecture roles empower APT members and provide a constant feedback loop and career growth discussions as part of the overall collaboration cycles. This creates a culture of sharing and mutual accountability, in addition to career growth opportunities.

Aligned Architectures Form the Architecture Runway

Architects provide direction for business and security solutions through a unified approach to security, reference, and solution architecture. This includes enterprise-wide environmental changes, new providers, new technology, new features, and assistance in prioritizing technology investments.

Enterprise Security (ES) architects create reference architectures that span business, data, application, and technology (BDAT) domains at the security capability level based on Intel's security program and portfolio management activities. Solution architectures, which are specific to security solutions and products, are then developed based on the reference architectures. These combined architectures form the "architecture runway" and establish the solution basis during the release planning sessions. Solution architects also partner closely with the Agile Persistent Teams (APTs) to ensure that project-detailed designs align to the solution architectures.

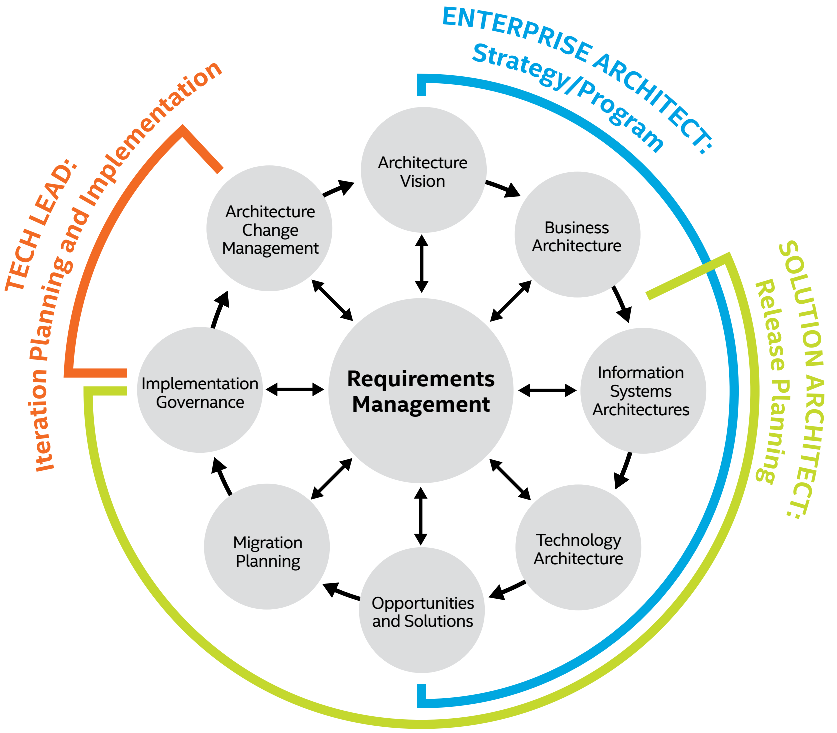


Figure 3. The Open Group Architecture Framework* (TOGAF*) standard allows us to align our security and solution architectures across all phases of strategy, release planning, and implementation.

Next Steps

Based on considerations associated with the overall business goals, we are now developing the following embedded roadmaps that comprehend our architectures:

- **Segment-level.** This is the over-arching, integrated roadmap for ISaaS. It represents all planned information security capabilities over the next three years.
- **Capability.** These roadmaps represent specific security capabilities, such as identity management (IDM) and security incident response. They are owned by the reference architects, aligned to the segment-level roadmap, and represent planned programs and activities over the next three years.
- **Solutions.** These roadmaps represent planned implementation of specific solutions and features for a specific capability area over the next year. These are owned jointly by solution architects and the product owners and must be aligned to the corresponding capability roadmap.

We have started this roadmap process and expect it to mature over the next year. Our roadmaps align our architecture development methodology with the Scaled Agile processes and the work performed by the various APTs. We see the role of ES architecture as an opportunity for career growth. It requires a constant effort of sharing and collaborating, empowering team members, and enriching the discussion and direction.

Lastly, we have started to place increased emphasis on business architecture. Business architecture precedes the technical architecture according to the BDAT model and focuses technical work on creating capabilities that achieve the business goals with a global and local view. For security, the business value is often measured in two ways: 1) risk reduction, and therefore a reduction in the annualized loss expectancy (ALE); and 2) total cost of ownership (TCO) reduction through improved agility and user experience, and optimized security investment. As with any enterprise endeavor, establishing key processes, roles and organizations, and interactions between roles and processes is critical. All of these must align to business, IT, and information security goals.

A Closer Look at Technical Debt

Industry definitions vary—here is Intel IT's take. Intel IT defines technical debt as the following:

- Redundant applications that enable similar business processes or functions.
- Applications or data with exposure to risks (including security, compliance, copyrights, and licenses).
- Duplicate IT services for infrastructure, platforms, competing products, database solutions, and more.
- Solutions that are not consuming reusable assets.
- Technologies or solutions that have low return on investment, low cost efficiencies, or minimal usage.
- Systems and applications that run on unsupported suppliers' products or are out of compliance with Intel future-state platforms.
- Reducing/avoiding/de-commissioning custom-coded solutions and integrations that implement non-differentiating capabilities.

Conclusion

With the rapidly changing business environment, maturity of cloud solutions, and exploding data volumes, ES requires a new approach. Rather than becoming a roadblock to business goals, Intel IT developed a solution that allows business units and APTs to move more quickly on their deployments and take more ownership.

Our integrated ES architecture decentralized the security model with a modularized, service-based approach with clearly defined guidelines for APTs, which also serves as a role model for other ES architecture efforts at Intel. Not only has our ES architecture given business units more flexibility, it has provided IT with a comprehensive view of all deployments across the ecosystem and allowed us to address security issues specific to security threats without impacting other services.

Related Content

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

- Enterprise Architecture: Enabling Digital Transformation at Intel paper
- Enterprise Technical Debt Strategy and Framework paper
- Securing the Cloud for Enterprise Workloads: The Journey Continues paper
- Transforming Intel's Security Posture with Innovations in Data Intelligence paper

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.

[1] The 20 CIS Controls & Resources can be found at cisecurity.org/controls/cis-controls-list.

[2] The TOGAF* Standard, a standard of The Open Group, is a proven enterprise architecture methodology and framework used by the world's leading organizations to improve business efficiency. More information can be found at opengroup.org/togaf.

[3] More information about Scaled Agile Framework can be found at scaledagile.com.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

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 or error free, and therefore Intel makes no warranty, representation, or guarantee regarding the performance of its products, the information contained in this paper, or the suitability of its products for any particular purpose. Check with your system manufacturer or retailer.

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.

0819/WWES/KC/PDF 340009-001US