White Paper
Information Technology
October 2025

IT@Intel: Standardizing Application Portfolio Management with Gated Resource Provisioning

Intel IT is enhancing IT governance with a standardized application portfolio management framework that enables intelligent and accurate application registration and lifecycle management

Intel IT Authors

Patrick Ballard
Information Security Manager

Omer Ben-Shalom
Sr. Principal Engineer,
Enterprise Security Architect

Richard Cardenas
Principal Security Engineer

Jason Devoys
Principal Engineer,
Enterprise Security Architect

Chris Gerk
Enterprise Security Architect

Roberto Quinones
Principal Engineer,
Enterprise Security Architect

Yaoz Talshir
Application Portfolio Management
Service Owner

Table of Contents

Executive Summary

In Intel's modern, digitized computing environment, Intel IT is tasked with lifecycle management for thousands of applications and millions of IT resources like identities, Domain Name System (DNS) records, accounts, certificates, VMs and containers, databases, platforms, and more. Tracking and managing all of these resources and their affiliated applications requires capabilities beyond those found in Commercial-Off-the-Shelf (COTS) application portfolio management (APM) solutions.

Intel IT has developed a custom APM framework to standardize how applications are managed. The foundational concept for our new framework is strict gating of the provisioning of new resources used by applications and auto-decommissioning of assets and resources upon application end-of-life. Our goal is to prevent the provisioning of any IT resources used by an application unless the application is correctly registered and the resources are linked to a specific application.

Our new approach to APM improves visibility, governance, and application rationalization. This helps to enable cost savings, creates more efficient application and resource lifecycle management, and reduces security and compliance risk. We hope that sharing our APM journey inspires other enterprises—and APM vendors—to explore new ways to enhance APM in an increasingly digital IT landscape.

Contributors

Shashi Chagam, Principal Engineer, Enterprise Architecture
Subbarao Mantha, Principal Engineer
Elena Ratner, Application Portfolio Management Business Architect
Yogesh V Shetty, Application Portfolio Management Technical Architect

Acronyms

APM	application portfolio management
BU	business unit
DNS	Domain Name System
IGA	identity governance and administration

Business Challenge: Lack of APM Governance Poses Risks to the Business

The value of application portfolio management (APM) is undisputed, and several commercial APM systems exist. However, APM systems typically rely on human input, which creates multiple categories of risk for the business. Errors can be caused by simple omissions or result from someone purposefully mis-defining an application and its lifecycle state to expedite development without meeting required security steps.

Beyond these human reliability issues, traditional APM approaches face several fundamental challenges:

- **Definitional ambiguity.** Vague definition of what constitutes an "application" leads to inconsistent registration and management practices across the organization (see the "Terms to Know" sidebar for Intel IT's definition).
- **Resource tracking complexity.** The significant technical challenges associated with tracking all the diverse resources that applications consume—including servers, databases, certificates, DNS records, and service accounts—often result in inadequate visibility.
- **Registration barriers.** One-size-fits-all registration processes that demand extensive detail upfront deter people from registering applications, particularly during early development phases (see the "Progressive Profiling" sidebar for our solution).
- **Lifecycle management gaps.** Without proper governance, applications and their resources can become orphaned, creating security vulnerabilities and unnecessary costs.

Considering technological advancements, growing security threats, and evolving business needs, enhanced APM is now more important than ever. Without a formal, comprehensive APM framework that covers all applications and their resources, organizations face several critical operational and information security vulnerabilities (see Figure 2 on the following page). Intel has experienced these challenges firsthand over the past few years, and they have limited our ability to optimize our ongoing digital transformation.

Terms to Know

Application relates to a logical set of functions and services that implement a business capability using various IT resources, including software (see Figure 1). It is possible, but very rare, for an enterprise application to be just a single piece of software. Instead, enterprise applications usually consume several resources, including multiple software components and various IT resources. For example, an application may use hosting resources to run software, "as a service" resources like storage, the Domain Name System (DNS), user accounts, and certificates.

Software is a digital implementation of a technical capability or an application function that can be used by an application or end users. Software requires an execution environment to run on, like servers, VMs, containers, or client endpoints.

Workload refers to an instance of software executing in a particular execution environment (physical server, VM, container, and so on).

Orphaned resources are IT assets (such as software, server, VM, database, or service) that are not clearly linked to an entity that owns or utilizes them and cannot be ultimately traced to a system or human that manages them. As a result, the resource is not actively supported or tracked and isn't removed when no longer required.

Application owners are the individuals responsible for the end-to-end oversight of a specific application within an organization's IT ecosystem. They register the application, verify that its features and functionalities meet the application's business goals, and retire it when no longer needed. This role helps ensure that the application delivers value, remains secure and compliant, and aligns with business and IT strategy.

Application operational owner is responsible for the technical and operational maintenance, as well as the resource management for an application. Responsibilities include acquiring resources, patching code and updating binary images, dealing with downtime, and retiring resources used by the applications in cases where human intervention is required. In many ways, operational owners act as delegates for the application when the application itself does not directly handle these elements.

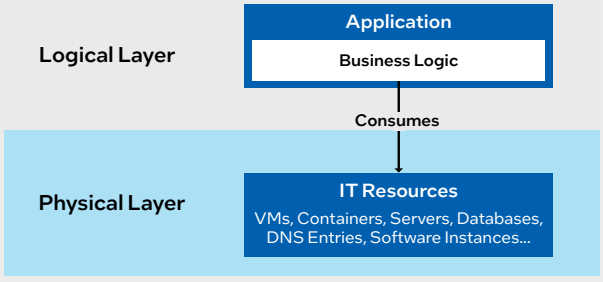

Figure 1. The relationship between an application and its resources.

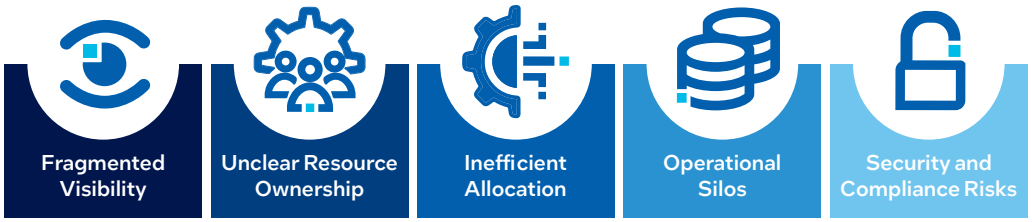

Figure 2. An incomprehensive APM framework causes a variety of problems.

Fragmented Visibility and Unclear Resource Ownership

Fragmented visibility hinders strategic planning and resource optimization, complicates operational management of applications and resources, and makes it challenging to identify security gaps such as unauthorized access.

When analyzing resource ownership in a large corporation like Intel, it is fairly easy to track the resources used directly by humans, such as their laptops, accounts, and files. However, these human-owned resources are only a small part of the total number of resources. At Intel, applications and the non-human accounts they use—such as service accounts, APIs, AI bots, and Internet of Things (IoT) devices—consume servers, VMs, containers, accounts, Domain Name System (DNS) entries, and many other resources. The association between these resources and the applications they serve depends on the accurate registration and tracking of applications, as well as the ability to link them with all their consumed resources.

Specifically, unmanaged non-human accounts can create significant security and governance risks. We must be able to effectively track and manage non-human identities associated with applications. Doing so will help to ensure secure access, compliance, and lifecycle management of these identities, their credentials, and their permissions. Tracking becomes even more critical as more resources become short-lived (or ephemeral), which is common in modern cloud environments and is a growing trend even on premises (see the sidebar, "Ephemeral Identities").

Inefficient Resource Allocation

Economic pressures demand lean IT operations. Unused or redundant applications and their resources impact the bottom line through wasteful spending, underutilization, and/or over-provisioned resources. Rationalizing and consolidating application resources can create cost savings and help us redirect funds to strategic initiatives.

Operational Complexity and Silos

The exponential growth of applications—fueled by cloud adoption and software-as-a-service (SaaS) platforms—has created sprawling IT and business unit (BU) portfolios. Unmanaged applications can lead to redundancy, lack of agility and innovation, inefficiency, and fragmented oversight. We need a better way to provide a centralized framework to catalog, assess, and optimize applications, helping to ensure alignment with business objectives.

Heightened Cybersecurity and Compliance Threats

Ransomware, phishing, and supply chain attacks are escalating globally. These threats often exploit unmanaged or outdated applications and their associated components. Applications are logical entities that encompass not just code and binaries, but also accounts, certificates, network configurations, and other interconnected resources. Consequently, any of these components can become vulnerable due to unpatched code, dangling DNS records, orphaned service accounts, expired certificates, and unmanaged VMs. We need to identify risks across all application components and interact with the appropriate owners (human or non-human) to enforce security standards like timely updates or decommissioning. This can significantly reduce the attack surface.

In addition to needing to guard against cybersecurity threats, IT is under increasingly stringent global and regional regulations that require robust governance of IT assets. Examples include the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and System and Organization Controls 2 (SOC 2). Non-compliant application resources, such as software and unmanaged non-human identities, can lead to penalties or reputational damage. We must verify that applications and their resources are compliant with standards and provide audit trails and governance controls.

Ephemeral Identities

An application is a logical entity whose logic is implemented using code. In contrast, a workload is an instance of that software running in an execution environment—it is the digital entity that uses resources to effect change. That is why our new application portfolio management (APM) framework tracks resources used by an application. Application identity is shared between workloads and is persistent. On the other hand, workload identities, especially in the cloud, are usually ephemeral, but often act on behalf of the application's identity. This is the key difference, for example, between managed identities assigned by a cloud system and managed identities assigned by end users. Tracking ephemeral workload identities back to the parent application is an interesting topic, but is beyond the scope of this white paper.

Solution: APM Governance through Resource Gating

Managing Intel's vast array of resources and their consumers has been a challenge that we've been working on for several years. Governing 430,000 compute servers, 984 PB of storage, about 11,000 commercial software installations, more than 1,700 applications, and nearly 200 horizontal platforms—not to mention thousands of VMs and containers and millions of unique identities—is a monumental task. We are leveraging key learnings from our past APM efforts to create a comprehensive, automated APM framework that exceeds the capabilities of commercially available solutions.

Resource Gating Is Key to APM Success

Within our new APM framework, the foundational model to enable resource linking and tracking is to control the creation of new resources, which we call gating. The rationale is that if all resources are properly attributed to applications when they are created, they are then strongly linked to the application, which allows lifecycle management for these resources. Our ultimate goal is to make sure that application-related resources cannot be allocated unless they are linked to a specific application.

This strong link between applications and resources helps ensure that applications are registered correctly regarding their attributes, such as type and lifecycle state. Incorrectly registering an application will prevent it from receiving the necessary resources to make it fully functional.

Another critical value of resource gating is that it links resources to the application itself rather than to the human who requested the resources (likely one of the application's operational owners). This approach eliminates the need to track individual human employment changes like job transfers or terminations. When personnel changes occur, they are handled upstream in human resource systems, affecting groups like application operational owners rather than requiring updates to potentially hundreds of thousands of individual resources used by an application.

Early Gated Resource Provisioning Efforts

In 2015, we used an early version of our APM platform to gate resource provisioning of SSL certificates from our enterprise Public Key Infrastructure (PKI). This ended years of ambiguous ownership that prevented expiration notifications from reaching the appropriate interested parties or wasted efforts on lifecycle management of non-essential certificates. It also drove many application owners to declare and register previously missing application entries. This approach established a model for controlled resource allocation, influencing other systems to provide clear ownership and accountability for resources:

- **Privileged access management and secrets management.** The following year, we began gating the provisioning of secrets vaults, helping to enhance storage security and manage privileged accounts and sensitive credentials. This addresses the problem of orphaned secrets and accounts by establishing clear ownership and accountability.
- **Identity governance and administration (IGA).** Around the same time, we also began gating the provisioning of non-human accounts, entitlements, and roles within identity and access governance systems, helping to ensure controlled access and compliance with security policies. This helped address the problem of orphaned accounts, roles, and entitlements.
- **Cloud subscriptions.** As Intel expanded our execution in the public cloud in about 2020, we started gating cloud subscription provisioning, helping to ensure controlled allocation and management of cloud resources in alignment with organizational security and governance policies. It helps address the problem of orphaned cloud resources and provides accountability for cloud resource cost, which leads to cost savings by removing orphaned resources and right-sizing underutilized resources.
- **Domain Name System (DNS).** Until recently, our DNS record management was suboptimal, with no defined ownership of domain names. This created risks of DNS takeover due to untracked or mismanaged records. Stale records often persisted because of uncertainties that removing them might disrupt services. Starting in 2022, we now gate the provisioning and lifecycle management of DNS records, helping to ensure secure and controlled configuration, updates, and retirement of DNS resources.

Taking Resource Gating to a New Level

However, these isolated gated provisioning efforts were not enough. To achieve reliable application registration, we needed a forcing function. Our new approach to APM makes it difficult—if not impossible—for an application to be unregistered or mis-defined and still operate successfully.

Our strategy is to gate all systems that allocate resources related to applications. This will help ensure that resources cannot be allocated without relating them to their associated application, as well as validating that the application type and state authorize that application to acquire these resources. Once the resource creation events are tied to the application accurately, other lifecycle events (such as rotation/renewal of resources and closure/elimination of resources when they are no longer required) become easy and can be automated with confidence. This helps create disciplined resource management that aligns IT operations with strategic, operational, and security objectives.

Our gating strategy supports Intel's strategic goals—such as cost efficiency, innovation, and digital transformation—and addresses the pain points discussed in the Business Challenge section:

- **Visibility.** We will map resources to applications for strategic and operational clarity.
- **Accountability.** Explicit ownership of resources helps ensure governance and security.
- **Efficiency.** Optimized resource allocation can help reduce costs and waste.
- **Simplicity.** Integrated systems reduce operational complexity.
- **Security and Compliance.** Security by design, with auditable records, mitigates risks and helps meet regulatory requirements.

Our new APM system is both scalable and practical because it integrates with existing resource management systems, such as identity and access management tools, infrastructure provisioning platforms (such as cloud orchestration tools), and IT service management systems. It also integrates with our existing software asset management (SAM) and hardware asset management (HAM) systems (see Figure 3); one signal from the APM system can cascade across all resource management systems. This widespread integration reduces operational silos, streamlines lifecycle management workflows, and provides a unified view of resource dependencies. It also helps ensure that all application resources are tied to a specific application. This integrated approach enables us to scale out the solution across Intel's global operations without completely overhauling existing investments in infrastructure.

Our APM system requires robust computational power to handle enterprise-scale integration of resource management systems, process large-scale application and resource data, and support real-time tracking and analytics. Intel® Xeon® processors provide high-performance computing, enabling efficient processing of APM workflows, resource provisioning, and audit trails.

Our comprehensive approach to APM demonstrates how a standardized APM framework with a gating mechanism can transform resource management for enterprises and help deliver measurable business value in efficiency, security, and strategic IT alignment with the business.

Progressive Profiling Encourages Application Registration Compliance

Our early application portfolio management (APM) attempts took a one-size-fits-all approach to application registration. We asked for the same information for a new application that was just starting development as we did for a mature application entering production. Having to provide a high level of detail (such as identifying application operational owners and segment architects) for a simple, small proof of concept made registration difficult, and people often opted not to register their applications.

We considered alternatives, such as only asking for the bare minimum information (which means that as an application matures, we don't have the information we need for effective APM). Instead, we instituted a progressive profiling model, similar to what is used for customer identity profiling in marketing. For a new application, we ask for only a few details, such as the name of the person registering the application, the application owner's name, and the application type. As the application progresses toward production, we gather details about the application's technologies, request a full code scan, ask for the operational owner's name, and so on.

For the progressive profiling approach to work, we need to ensure owners actually "progressively register" and don't just use the minimum "new app registration" profile and then never update the registration. To avoid this scenario, we gate the resources that an application can obtain based on its lifecycle registration. If the registration is not updated when an application moves from "new app" to "pilot" to "production," we do not make the necessary resources available. Resource gating forces correct and progressive application registration while making it easier for application developers to register their early efforts.

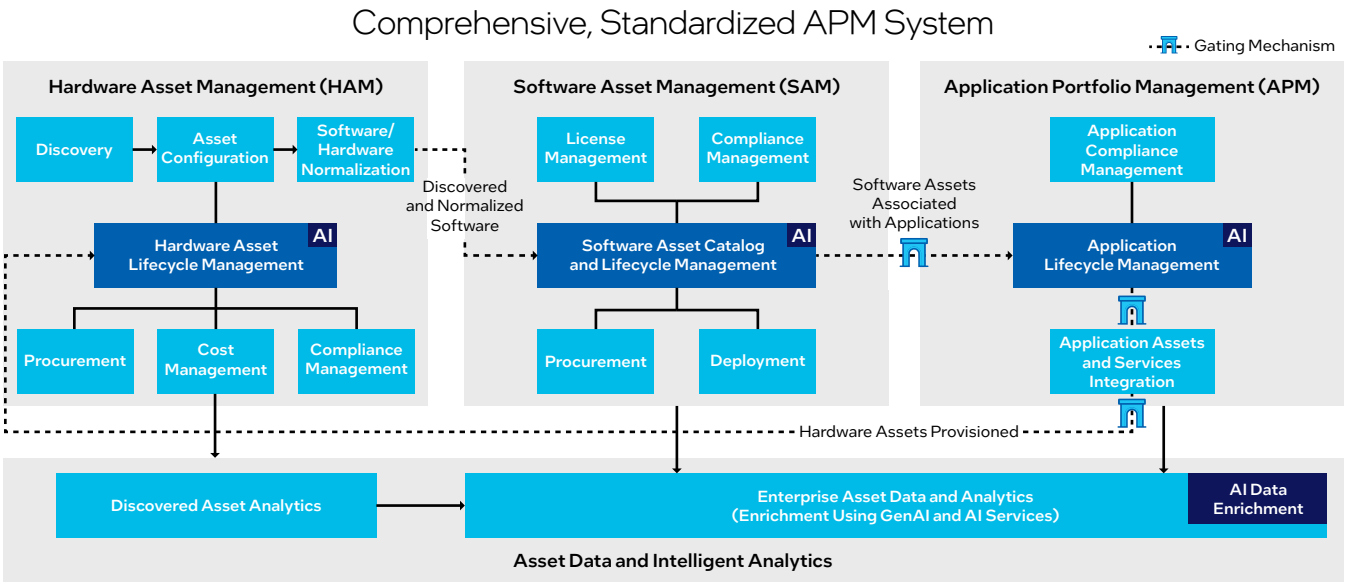

Figure 3. Our comprehensive and automated APM system integrates application registration with hardware and software resource allocation.

How Our APM Governance Works

Our new APM framework is fairly simple, consisting of five steps (see Figure 4):

- **Step 1: Application registration.** Every application must be registered to provision resources. This enforces a centralized registrar for all applications and, as their maturity progresses, all their resources. The gating mechanism provides control and visibility into both the application state/lifecycle and its use of IT resources. See "A Closer Look at the Registration Process" for additional information.
- **Step 2: Resource entitlement determination.** Based on the application's registered type and lifecycle state, the system determines what categories and types of resources the application is authorized to request. For example, a "new application" in development may be entitled only to basic development resources, while a "production application" can request production-grade infrastructure, certificates, and service accounts. This step establishes the boundaries for what resources can be provisioned without actually allocating them yet.
- **Step 3: Provisioning validation and resource linking.** Resource requests, such as a new account or VM, are automatically validated against predefined criteria including the application's type, owner, tier, and lifecycle state. The system knows what the application is entitled to and approves requests that meet these criteria, while rejecting unauthorized requests. Upon validation, each approved resource is allocated to the application and explicit ownership is assigned, while metadata captures resource dependencies (such as which identities or servers are allocated to the application). This clarifies accountability, supports governance, and mitigates security risks from unowned resources. It also significantly reduces the likelihood of orphaned resources, because each resource is linked to an application and, therefore, to specific owners—for example, that application's operational owner's group. Provisioning is achieved through integrated identity and access management or infrastructure platforms, which collect and store ownership and tracking metadata.
- **Step 4: Continuous auditing.** The gating mechanism continuously tracks resource usage, ownership, and dependencies, and generates auditable records of resource provisioning. These records include who or what requested the resource, which application the resource supports, and the owner of the application. We can use this data help with compliance audits and security monitoring. Automated governance strengthens our ability to comply with regulations like GDPR and SOC 2, and reduces vulnerabilities such as unauthorized access or unpatched assets.
- **Step 5: Cleanup.** We clean up application resources once the status of an application reaches end-of-life. For example, we can retire resources such as VMs, containers, and DNS records and delete accounts and identities. When an application is no longer active, cleaning up resources reduces costs by retiring unnecessary resources and improves security by reducing the attack surface from unnecessary accounts, permissions, resources, and data.

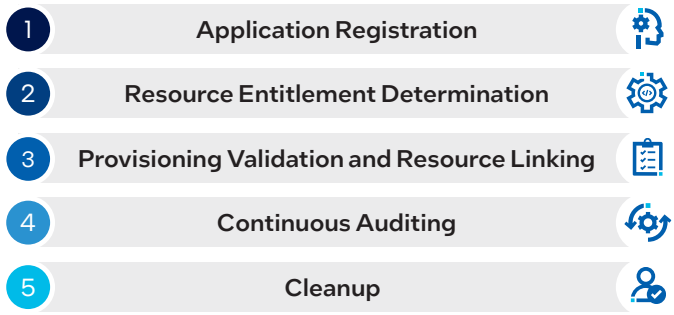

Figure 4. Five steps provide simple but effective APM.

A Closer Look at the Registration Process and Software Taxonomy

As we developed our new APM framework, we discovered that even with a clear distinction between "application" and "software," nuances still existed that we needed to account for during the application registration process. Table 1 on the following page provides our software taxonomy, while Figure 5 shows how that taxonomy affects application registration.

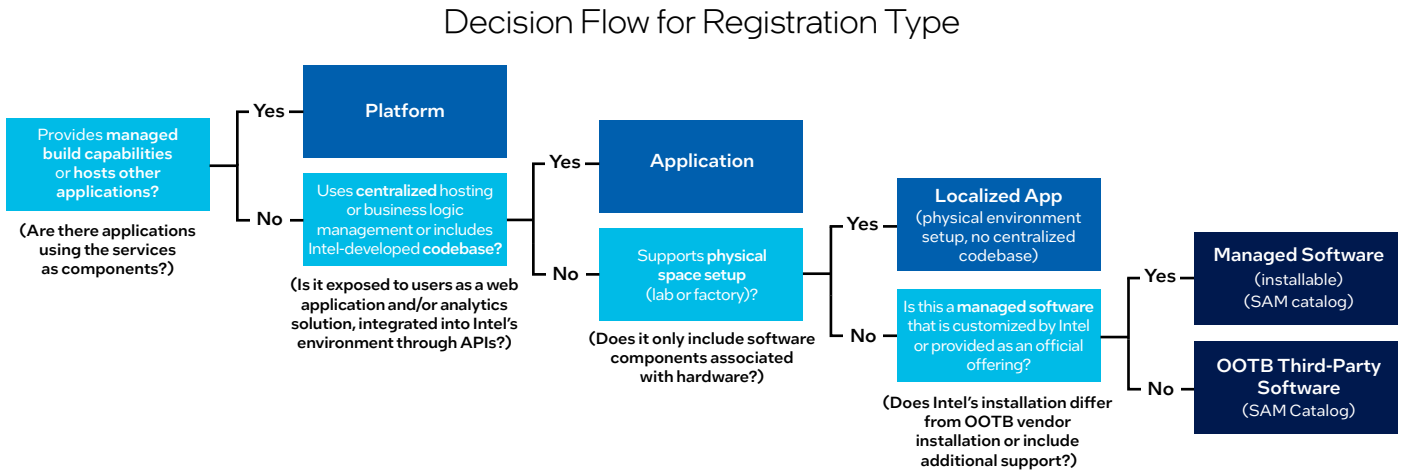

Figure 5. We have defined a software taxonomy that guides the application registration process.

Table 1. Software Taxonomy

Registration Type	Data Definition	Hosting	Used By
Third-Party Software (SAM Catalog)	▪ Commercial-Off-the-Shelf (COTS) or open-source installable software (no customizations) developed by a third-party solution provider and used by Intel. ▪ Limited to formal company software sources.	Enterprise servers or devices	Users/ applications
Managed Software (SAM Catalog)	▪ Subset of third-party software. ▪ Intel's implementation of software (customizations and/or configurations, not involving custom code) that provides technical capabilities or a utility/productivity tool, which is used within the context of a single user/single device (not hosted/managed centrally) and does not support business process execution. ▪ Primarily includes development frameworks, system utilities, operating systems, and end-user applications. ▪ Limited to formal corporate software sources.	N/A (local installation, no centralized hosting)	Single user/single device (per installation)
Application (APM System)	▪ A business solution that supports Intel's business process execution and enables business capabilities. It can be custom software developed by Intel or an Intel-specific deployment/ customization of a third-party software that is usually centrally hosted and exposed to users as a web application. ▪ Requires assets, resources, and services supported by Intel.	Enterprise, software as a service (SaaS)	Multiple users/ multiple devices (per deployment)
Platform (APM System)	▪ Managed solution implementation (custom or COTS) that provides build/host capabilities and services to enable enterprise applications' continuous development/deployment lifecycle. ▪ Must be used by other applications.	Enterprise, SaaS	Applications
Localized Solution (APM System)	▪ Non-reusable, team- or area-scoped solution with minimal risk, cost, and architectural complexity, with limited business impact and low support level. ▪ No enterprise business dependency on the localized solution and its data.	Enterprise (hardware only or localized low-code scripts not executed centrally)	Limited team usage

Challenges to Implementation

As we work on implementing our new APM framework, we have encountered both technical and organizational challenges.

From the technical perspective, the first challenge was realizing that most industry-standard APM tools aren't mature enough to handle the level of granularity and governance we require. We had to build our own APM system by writing custom APIs to integrate disparate resource management systems into a cohesive whole. As we designed the system, we had to determine how to enforce mandatory application registration to gate resource provisioning without disrupting existing workflows. We must also balance security and compliance requirements with operational efficiency to avoid introducing resource allocation bottlenecks.

From the organizational perspective, we realize that change is rarely easy, especially when application developers' and BUs' methods of interacting with the IT landscape are deeply ingrained. We had to obtain buy-in from diverse stakeholders (including the CIO, IT managers, the CISO, and architects) to adopt the gating mechanism across Intel's global operations. We have also educated the BUs and architects about what constitutes an "application."

Enterprise Benefits

We are shifting the paradigm of application compliance from reactive enforcement to built-in compliance by design. As we implement APM and its gating mechanism, we are realizing significant enterprise-wide benefits for Intel, which include, but are not limited to, the following:

- Cost savings
- Operational efficiency
- Enhanced security and compliance
- Reduced technical debt
- Strategic alignment of IT resources and business goals

We also hope that our success story can influence industry standards and solutions so that eventually, we can retire our custom solution and deploy a commercial solution that meets our needs.

The Critical Role of Application Portfolio Management in Zero-trust Success

Today, the IT industry is focused on the infrastructure elements of zero-trust architecture, such as software-defined perimeter (SDP), secure access service edge (SASE), and secure service edge (SSE). However, access decisions based on missing or inaccurate data can be a potential weak point of zero-trust architecture, limiting fidelity and often prohibiting the use of the advanced authorization involved in true zero trust.

Application portfolio management (APM)—done correctly—can provide a strong, trusted, and accurate source of context and attributes about applications, as well as the resources they consume. Unfortunately, many commercially available APM systems rely on human-entered data, reducing both the scope of data and data quality. Intel IT's approach to automated APM with strict application registration and gating mechanisms helps improve the accuracy of access decisions. It also addresses other security challenges resulting from orphaned resources being used to impersonate or take over trusted entities by harvesting and using account credentials or no-longer-required privileges. In other words, a standardized, automated APM system is crucial in establishing a successful zero-trust environment.

Next Steps

As we scale our new, standardized APM framework with a gating mechanism, we are rolling out a comprehensive, cross-functional APM implementation program that brings together IT, security, and architecture teams to deploy the gating mechanism enterprise-wide and integrate the APM system with all of our resource management systems. Activities that we are working on include:

- We are conducting an application and resource inventory audit to establish a baseline, which identifies unregistered or orphaned assets. These resources will be mapped to applications to clean up our existing environment, while all future provisioning will adhere to the gating mechanism.
- We are establishing policies to institutionalize the gating mechanism. These policies are embedded into our IT and security workflows to ensure consistent governance and compliance and long-term adherence to the gating mechanism.
- We are working on embedding our standard IGA administrative access model into our APM framework so that when a new application is registered, all the relevant administrative roles and permissions are automatically set up and assigned to the right people associated with the application.

Conclusion

APM is critical today due to the overwhelming number of applications, AI systems, and rising cybersecurity threats, combined with cost pressures and regulatory demands. Intel IT's standardized APM framework with gating mechanisms transforms IT governance by ensuring every resource is registered, owned, and tracked, shifting from reactive enforcement to built-in compliance by design. This approach delivers comprehensive visibility, governance, and optimization, empowering Intel to achieve significant cost savings, reduce risks, enhance security, and drive innovation in an increasingly complex digital landscape.

Related Content

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

- IT@Intel: Enterprise Architecture: Accelerating Intel's Business Transformation
- IT@Intel: IT Resiliency Drives a Resilient Enterprise
- IT@Intel: Prioritizing Investments and Maximizing Security Using Capability-Based Planning

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 on **X** or **LinkedIn**.

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