TAG

UNDERSTANDING WORKLOAD IDENTITY AND ACCESS MANAGEMENT USING AEMBIT

DR. EDWARD AMOROSO,
CHIEF EXECUTIVE OFFICER, TAG

aembit

UNDERSTANDING WORKLOAD IDENTITY AND ACCESS MANAGEMENT USING AEMBIT

DR. EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG

This report from the industry analyst team from TAG Infosphere[1] explains how workload identity and access management (IAM) addresses modern enterprise cyber risk. The commercial solution from Aembit[2] is used to illustrate workload identity management in practice. Our report is intended to not just inform readers, but also to prompt immediate action by managers and developers to begin taking steps toward reducing their workload cyber risk through improved IAM.

INTRODUCTION

The importance of identity and access management (IAM) for user accounts is well-established, especially as new zero-trust based architectures have begun to transfer primary security control from the firewall perimeter to identity.[3] As such, the cybersecurity industry has seen an explosion of growth in IAM-related products, IAM platforms, and enterprise initiatives focused on protecting user accounts and access.

With this growth has come a plethora of new commercial platforms that support tasks that might be considered adjacent to IAM. For example, new commercial offers have emerged in identity governance and administration (IGA) and privileged access management (PAM).[4] These new focus areas extend IAM to related enterprise security tasks – but are still primarily focused on traditional user-based IAM.

Our attention in this report is on a different growth path for IAM – one that focuses less on human accounts and more on the protection of the workloads, applications, and software that characterize the modern Internet.[5] Specifically, we review here a new discipline known as Workload Identity and Access Management or workload IAM, which we view as having comparable benefit for enterprise protection as traditional user oriented IAM.

An important objective in this report is to help readers understand that they should start solving the problem of workload IAM. We believe this to be an urgent priority and that both security threat and compliance motivations are emerging that should prompt action by management teams and developers. Our hope is that both groups will begin to curate solutions for their existing and planned workloads deployments.

In this report, we explain workload IAM using the platform solution from commercial cybersecurity vendor Aembit as a reference to explain how such capability can be deployed into an actual enterprise. Using a live platform to explain the concept is important because it reinforces the practical nature of our guidance. That is, we view workload IAM as an actionable cybersecurity approach, one that we believe most enterprise teams should prioritize.

OVERVIEW OF WORKLOAD IDENTITY AND ACCESS MANAGEMENT

The objective for workload IAM can be understood by reviewing parallel functional and operational requirements for IAM solutions in a traditional user context. Often described in the context of vendors such as Okta and Microsoft, the deployment and use of IAM systems and infrastructure are now common across organizations of all sizes and sectors, especially ones that support on-line accounts for their customers.

User IAM	Workload IAM
Focus on employees and customers	Focus on workloads and service
Familiar, mature process	New approach to existing problem
Heavy emphasis on usability	Heavy emphasis on automation
Dominated by Okta and Microsoft	Still maturing commercial market

Figure 1. Comparing User IAM with Workload IAM

The motivation for workload IAM is that just as functions such as authentication, policy-based access control, and access governance are key objectives in user IAM, the same types of functions must now be put in place and supported for the workloads that drive modern business.[8] Our presumption is that a workload is an on-line accessible service or compute capability, often hosted in cloud, that supports some functional need for its sponsor.[9]

The technology stack for workload IAM is different from the technology stack for workforce IAM. That is, authenticating a client workload will require different steps than authenticating a user. The protocols to authenticate to a service, the management workflow ownership, and the required levels of automation and scale are different in workload IAM than supporting user IAM functions such as the movement of personnel.

In addition, the lessons for cybersecurity and compliance from user IAM have not yet been applied to workload IAM. For example, auditors don't yet demand IAM for workload authentication nor do practitioners typically experience internal or external audits for their workload credentials. Even conditional access, which is commonly reviewed for user IAM, is not typically applied to workload protection.[10]

CHALLENGES ASSOCIATED WITH WORKLOAD IDENTITIES

Readers who are familiar with the specifics of how workloads are designed, deployed, and managed with understand the many operational and security challenges that must be addressed in a day-to-day context. They will also understand the consequences of improperly managing workload identities since this can result in significant breaches to systems that rely on trusted intercommunication and sharing between systems.

Common issues include determining whether a central entity, system, or group is in place to manage access between workloads. Doing this manually obviously does not scale and is highly prone to human error. Similarly, organizations need to assess whether the credentials associated with workloads are long-lived and whether the management of these credentials is robust and scalable. Unfortunately, many organizations struggle with these issues.

RISKS ADDRESSED BY WORKLOAD IDENTITY MANAGEMENT

As a result, significant cyber risks tend to emerge as a result of improper workload IAM processes and infrastructure. While such risks will depend on local context and will certainly vary based on the criticality of the assets being managed or shared by workloads, some common general risks that emerge from insufficient attention to workload IAM include the following:

- **Workload-Managed Data Leakage** – A problem that can occur with poorly managed identities for workloads is that bad actors might spoof or break existing controls to gain access to key assets or resources through application programming interfaces (APIs) or other means.
- **Workload Corruption** – The potential emerges when identities are not managed, or credentials are poorly handled is that the functionality of the workload might be adjusted or corrupted by malicious actors taking advantage of the weak IAM environment.
- **Audit and Compliance Issues** – Developers, managers, and compliance experts will understand that the intensity of focus from auditors on IAM is now extending to the workloads. Being unprepared for such attention will lead to high cost of reviews and real operational challenges for compliance teams.

These risks are just a representative sampling of the types of concerns that can emerge in a given environment. The degree of consequence of any risk will be directly related to the criticality or sensitivity of the resources being managed. Readers can easily imagine scenarios, such as in operational technology (OT) or industrial control system (ICS) architectures, where the consequences could be quite grave.

CASE STUDY: AEMBIT COMMERCIAL SOLUTION

Aembit focuses its workload IAM on streamlining and securing access across heterogeneous compute environments. Most organizations today are heterogeneous, with computing supported across one or more clouds, multiple SaaS services, other cloud APIs, and possibly data centers. Securing access between workloads, both within a single environment and across environments, is both critical and complex. Aembit's workload IAM addresses this need.

At its core, Aembit's workload IAM serves as an *identity broker* between an identity for a client workload in one environment and an access credential for the target service workload in another environment. Aembit enables brokering across different environments by supporting *trust providers* to authenticate clients in various environments and *credential providers* to provide access credentials for multiple services.

Despite the fact that workload IAM is new, standards developed with users in mind can be used for workloads, so Aembit supports familiar industry approaches like OAuth 2.0 and OpenID Connect. These standards were developed for user-based federation capabilities of the major cloud providers, as well as legacy authentication mechanisms. Aembit applies these industry standards in the context of workloads.

In addition to brokering access, Aembit also helps organizations reduce their cyber risk by removing secrets (known as going *secretless*). Just as user access has become increasingly passwordless (think one-time passwords and biometrics), Aembit helps organizations cryptographically identify client workloads without secrets and migrate to access tokens instead of using long-lived API keys.

Aembit also offers the ability to specify granular authorization controls based on workload identity as well as dynamic conditions such as the real-time security posture of the workload, in addition to mapping a workload to a particular role at the service workload. This offers flexibility to dynamically grant the right level of access to specific resources, further minimizing the risk of unauthorized access and other types of potential security breaches.

Aembit Workload IAM offers centralized management capabilities, allowing system and security administrators to configure and monitor workload authentication policies across their hybrid cloud infrastructure. Aembit's centralized approach simplifies administration and helps organizations maintain compliance with regulatory requirements that are increasingly targeting workload security.

Centralization is also an important platform feature because increasingly workload access is being federated across different environments. Aembit provides a centralized Identity Broker where these trust relationships are defined, instead of creating many ad-hoc pairwise trust relationships. The reduction in complexity is welcome, especially as the number of workloads supporting an environment continues to grow.

The Aembit protocol involves the familiar cadence between the client workload, targeted on-line service (also a workload), and the interim security functional components – namely, the Aembit Cloud and the various third parties for credential and trust support.[11] By following the steps shown in Figure 1 below, you can see how familiar the protocol is for anyone steeped in modern IAM design (e.g., with vendors such as Okta).

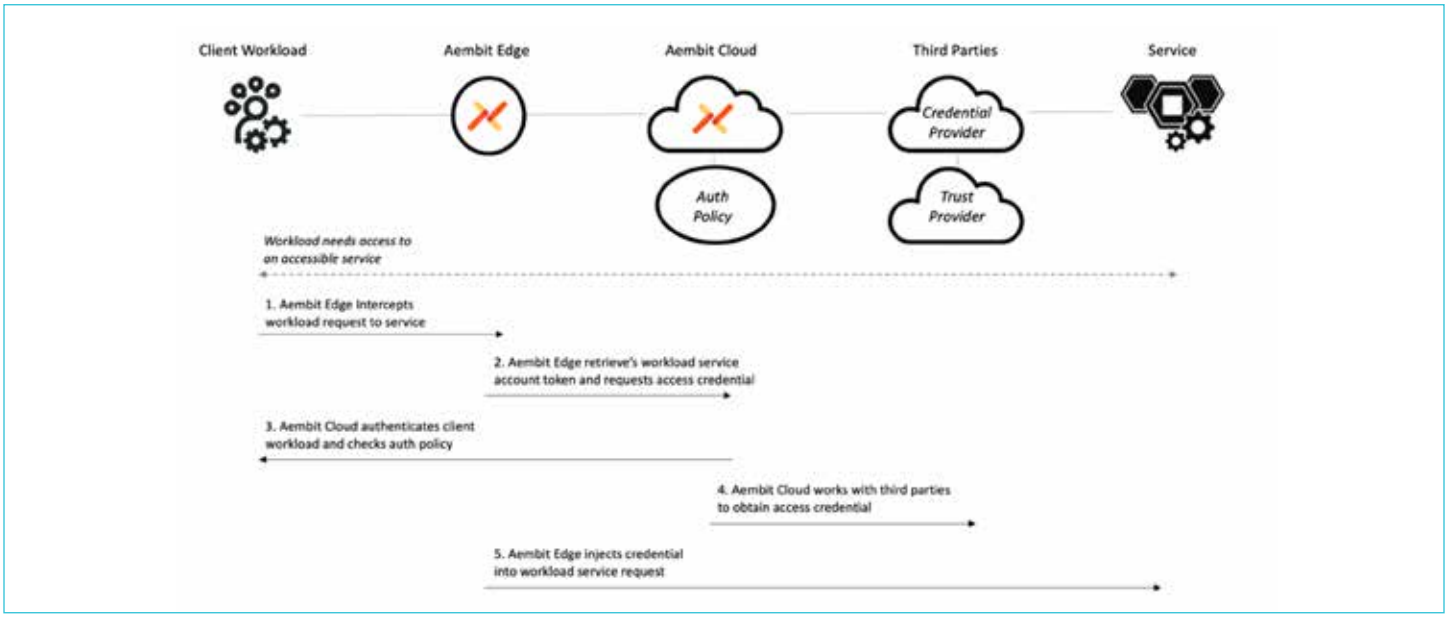

Figure 2. Aembit Protocol

AEMBIT USE CASES

Some examples can help illustrate the Aembit protocol. Consider first that the Snowflake data warehouse is often used as a centralized repository in the enterprise, with multiple applications reading, writing, and processing data in Snowflake. It is critical that those client applications authenticate to Snowflake. Today this is often done with service accounts, usernames, and passwords. Aembit allows a seamless transition to policy managed access without secrets by replacing usernames and passwords with short tokens.

Another use case example involves GitHub Actions to Amazon Web Services (AWS) which involves orchestrating automated workflows that deploy, test, and manage applications hosted on the AWS infrastructure.[12] Aembit's workload IAM system facilitates secure access between GitHub Actions and AWS services by establishing trust relationships and by managing and enforcing fine-grained access controls.

Note that in this use case Aembit federates between GitHub and AWS, Aembit IAM is able to authenticate the GitHub action, determine its access rights based on predefined policies, and issue the GitHub action a short-lived credential for access to the appropriate AWS service. This ensures that only authorized actions are performed within the environment, mitigating the risk of unauthorized access, and the risk from leakage of long-lived secrets.

As a third use-case, Aembit supports cloud identity federation, which allows workloads in one cloud to access cloud services in other clouds. By federating identities across cloud platforms, Aembit streamlines access management and enhances the user experience while maintaining security and compliance. Aembit centralizes federation, which can thus be governed and audited versus maintaining multiple federation relationships between multiple environments.

Many other practical use-cases emerge for deployment and use of Aembit workload IAM including the following:

- **Data Warehouses** – Securing access to sensitive data in many types of data warehouses beyond Snowflake (e.g., Databricks, MySQL, Amazon S3).
- **SaaS APIs** – Enforcing secure access to SaaS APIs (e.g., Large Language models (LLMs), Salesforce, Stripe, MS Graph)
- **Secure CI/CD** – Providing support for secure CI/CD pipeline development and delivery (e.g., GitHub, GitLab, Terraform)
- **Secure Vault** – Offering support for secure vault access and usage (e.g., HashiCorp, GCP Secret Manager, AWS KMS)
- **Multi-Cloud Federation** – Enabling multi-cloud federation for workloads (e.g., On-Premises, AWS, GCP, Azure)

ACTION PLAN FOR ENTERPRISE

Our team at TAG strongly recommends that enterprise teams begin the planning, if they have not already, to create an effective means for performing the types of IAM tasks for workloads referenced above. Our observation is that most CISO-led teams in both industry and government will tend to neglect this function, perhaps relying on a shared secret model or other ineffective and difficult-to-maintain approach.

In the past, we would have prioritized teams heavy in the provision of applications, workloads, and services, but it seems awkward today to suggest that any modern company or agency is not fully deployed in these areas. As should be evident from our comments above, TAG strongly endorses the use of Aembit for this type of task, but our Research as a Service (RaaS) customers are encouraged to contact us for source selection assistance if this is required.

---

[1] TAG Infosphere is a New York City-based research and advisory firm founded in 2016 and focused in the areas of cybersecurity, artificial intelligence, and climate science/sustainability. TAG provides analyst reports such as this one as a general service to the industry with unbiased and expert judgment focused on the needs of enterprise and government practitioners. See https://www.tag-infosphere.com/.

[2] The workload identity and access management platform from commercial cybersecurity vendor Aembit is explained in detail on the company's public website: https://aembit.io/. The Aembit team including David Goldschlag, co-inventor of onion routing, and Kevin Sapp, a pioneer in zero trust network access, supported the development of this report and were helpful in assisting with the technical content.

[3] ISACA (the industry's most prominent security auditor collective) reports on this important control shift from the perimeter to identity in this article: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-21/identity-as-a-new-security-perimeter.

[4] TAG Research as a Service (RaaS) customers can request information on IGA and PAM from our analyst team, including guidance on the most suitable vendors for their local environments. Companies such as Sailpoint and CyberArk, have been particularly successful in each of the two areas respectively – but neither focus on workload identities as discussed throughout this report.

[5] Readers should recognize that application architecture is changing with data center-hosted monolithic apps shifting to distributed services that consume cloud, SaaS, and legacy resources. Handling this transition demands a new approach to supporting IAM.

[6] See https://www.okta.com/ for more detailed information on how leading commercial cybersecurity vendor Okta supports user-oriented identity and access management for enterprise customers.

[7] See https://www.microsoft.com/en-us/security/business/solutions/identity-access for information on how Microsoft addresses user identity and access management with emphasis (interestingly) on their multi-cloud support.

[8] It is worth mentioning that while the process might be familiar, the underlying technology requirements are significantly different. This helps to explain why user IAM platforms cannot just be used to cover workload IAM needs.

[9] It turns out that defining a workload is a more awkward task then one might expect. Many experts equate workloads with services and applications (as we have basically done), and in most cases, this works out just fine. NIST offers a stilted definition that we have found less useful: "A logical bundle of software and data that is present in, and processed by, a cloud computing technology." We find this to be a truly awkward definition of workload, so we generally do not use it. See https://csrc.nist.gov/glossary/term/cloud_workload.

[10] A good way to reinforce the point is to explain applications today are not monolithic. Instead, workloads interact with each other and such interactions cross governance boundaries. Furthermore, the interactions are often autonomous – that is, not related to a user action.

[11] Aembit often thinks of credential providers as being associated with services (on the right side of the diagram in Figure 1), since the service needs to trust credentials provided by the credential provider. In addition, the trust provider is associated with the compute environment of the client workload since the trust provider authenticates the client workload to Aembit. Readers interested in diving more deeply into the protocol design can contact Aembit directly for more information: https://aembit.io/contact/.

[12] See https://aws.amazon.com/blogs/devops/integrating-with-github-actions-ci-cd-pipeline-to-deploy-a-web-app-to-amazon-ec2/ for more information about GitHub Actions.

ABOUT TAG

TAG is a trusted research and advisory company that provides insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, project consulting, and personalized content—all from a practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Edward Amoroso

Publisher: TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.