opentext™

WHITE PAPER

Cracking the access management code for your business

A modern IAM infrastructure is essential yet often overlooked. Learn how to simplify secure access through a common access security layer.

Contents

As digital transformation permeates just about every aspect of business, managing secure access gets more complex. Despite this challenge, identity-based security, which ensures that only the right people have access to the right information, too often remains an afterthought, leading to "Accidental Architecture." This fragmented approach results in inconsistent, hard-to-manage access controls, raising security risks and operational complexity.

This paper proposes a strategic approach to implementing a centralized, reusable access security layer (ASL). An ASL simplifies access management across both new and legacy services and resources by delivering IAM functions as a shared service. It supports secure access for any application from any device or location while matching security controls to risk levels.

OpenText IAM solutions—such as OpenText™ Advanced Authentication, OpenText™ Access Manager, OpenText™ Identity Manager, and OpenText™ Self-Service Password Reset—can be used to build and support a robust ASL. These tools offer out-of-the-box integrations, scalable deployment, and flexible authentication methods, enabling secure, seamless user experiences across cloud, on-premises, and hybrid environments.

This paper shows that a well-designed ASL offers big paybacks to the organization in the form of reduced risk, enhanced user convenience, streamlined operations, and meeting regulatory compliance commitments. Organizations that can consolidate IAM functions into a reusable and scalable identity fabric will find that it empowers them to increase productivity while reducing vulnerabilities. When done right, a cohesive ASL creates a secure foundation for digital growth.

The Accidental Architecture

Commonly, the applications and services needed to run an organization grow over time. As digital transformation expands across businesses, delivering secure access has made a modern IAM solution a must, but too often it's treated as an afterthought. In the end, organizations are left with a slew of applications that amount to an "Accidental Architecture," where secure delivery and access control occur in ad hoc fashion and often takes an enormous effort. Not only do some customized applications lack the security layer needed to protect themselves, but as part of an Accidental Architecture, they're not within a cohesive IAM infrastructure required for central point of administration. This paper provides a perspective on how IAM can be used to build a reusable set of access management services (Access Security Layer) for both your new and existing applications. This approach simplifies access management for all your applications and digital services.

Exacerbating the security challenge is the widespread use of BYOD and other unmanaged devices by all types of users. Beyond the devices themselves, the truth is that business leaders commonly drive the purchase of applications, services, and other resources on their own, or with just the cursory involvement of IT. This approach breeds the Accidental Architecture and limits the effectiveness of IAM infrastructure. These short-sighted purchases often occur without consideration for any scalable access control or single sign-on. It's later—after access fatigue sets in—that the pains of security and the desire for convenient access rise to the top of the organization's shortlist. The people responsible for making it all work begin to tire of the critical mass of these one-off implementations. Beyond the security needs, users want a single experience where their tools are easy to find and access and the business takes a hit if they can't provide it. So, while the Accidental IAM is often the organization's default architecture, it's not the desired one.

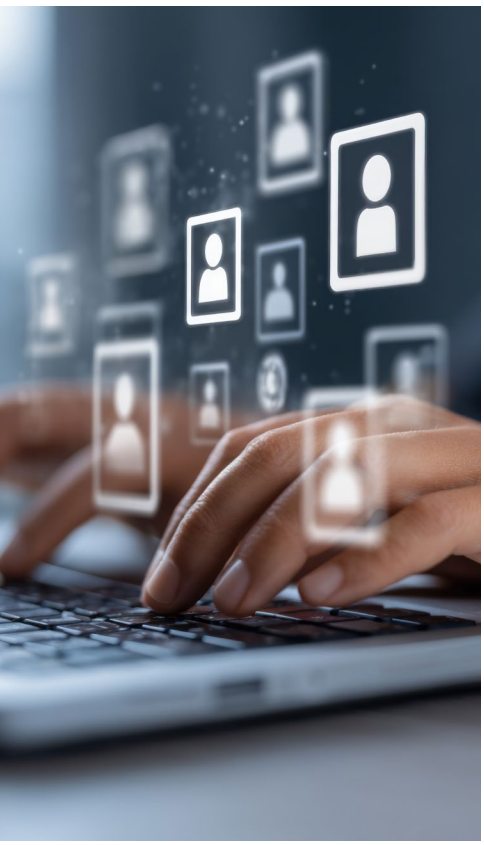
Why have an access security layer?

This reality of delivering secure access to all corporate applications is a paradigm shift for most organizations.

Historically, applications have been implemented to support discrete departmental functions, where information is tightly tied to the application platform and ultimately to a vendor. As a result, most IT organizations are saddled with an IT architecture that represents a timeline of "good" decisions that solved departmental problems at a particular time. Most of these systems, however, were not designed to integrate across a single security framework or to securely take advantage of the cloud.

The reason the Accidental Architecture leads to access fatigue is that it is labor-intensive and expensive to protect the many one-off applications while delivering secure access across all of them. Instead, the organization has silos of functionality that result in a greater amount of integration work and an increase in complexity. The root problem is the lack of a central lifecycle process for authentication and authorization.

The access security layer (ASL) approach centralizes IAM functions and delivers them as a reusable service from which applications can be integrated or protected. ASL simplifies the processes and infrastructure needed to manage identity and accelerates application implementation by providing robust integration capabilities.



Any application

Now that we live in a world where business resources can reside just about anywhere, there needs to be a scalable way to securely control access to them. And because some of these services are often specialized, IT can be faced with the task of bringing multiple applications into a single, simple user experience. The resources themselves can range from having LDAP integration, to federation support, to having nothing at all. The access security layer needs to encompass all of them.

Any device from any location

A well-designed ASL provides access control and single sign-on for your applications on any device used from any location. When you consider the risks associated with the “any” approach, it’s clear that organizations need the ability to account for a variety of remote and mobile situations from which protected information is being accessed. While the business needs to make access as convenient as possible, the level of security invoked needs to match the risk. A remote user requesting access from a known device from an expected location poses less risk to the business than an unfamiliar device from a foreign location.

Not just anybody, but everybody

The key to onboarding a new digital consumer (customer, patient, citizen) is to make it easy to become a known user. There are a few essential steps to make that happen:

- Provide a way for these users to sign up or create an account. In a world of too many credentials, people usually prefer the option of using their social (Facebook, Google, Twitter, LinkedIn, etc.) authentication. When you do this, you are lowering the threshold that many customers have for business engagement.
- Offer self-service onboarding. Customers or other users, such as patients or citizens, can enter their information to automate their identity across your environment.
- Match user verification to the risk. If the information is low risk and you have indicators (known device, expected location, repeated access, etc.) verifying the person’s identity, make it easy. Higher levels of identity verification should be reserved for situations where sensitive or regulated information might be at risk: for example, lost customer trust, financial risk, or government mandate. Deliver a frictionless user experience while applying the right amount of security.

ASL areas of service

The ASL consists of four areas of service:

Authentication Services

Federation—The authentication model of choice, where a trust is set up between the service provider and the identity provider. Most modern applications, both internal and cloud-based, now integrate with an identity provider. It is critical that the service layer supports all the current and emerging federation protocols (SAML, OAuth, OpenID Connect, etc.). The ASL can also consume external authentication sources.

Adaptive authentication—This is becoming a firm requirement for most environments to maintain security while facing increasing attacks from outsiders. The most effective way for you to manage risk while keeping access simple and convenient is to implement a risk-based authentication approach. For situations that require a higher level of user verification, advanced authentication provides a variety of options for multi-factor authentication and strong authentication. Advanced authentication is used as a single framework for multi-factor authentication, typically to comply with a mandate, as well as invoking frictionless strong authentication methods.

Authentication Web Services—Because these web-based services can reside virtually anywhere, there are times when communication between them requires authentication for security and nonrepudiation. WebAuthn and FIDO2 represent a modern, secure shift away from traditional passwords. Designed by the W3C and the FIDO Alliance, these standards enable strong, phishing-resistant authentication across browsers and devices. WebAuthn allows websites to register and authenticate users using public key cryptography instead of shared secrets, eliminating the risk of credential reuse or theft. When a user signs up, their device creates a unique key pair: the private key stays securely stored on the device, while the public key is sent to the server. Authentication involves verifying a signed challenge using biometrics, a PIN, or a physical security key—no passwords required.

FIDO2 includes WebAuthn and CTAP (Client to Authenticator Protocol), which enables browsers to interact with external authenticators like USB security keys or smartphones. This combination supports seamless passwordless login and multi-factor authentication with enhanced protection against phishing and man-in-the-middle attacks.

Passkeys, a user-friendly extension of FIDO2, sync credentials across devices via services like iCloud or Google Password Manager. This allows users to log in securely without needing to re-register on every device.

Identity Web Services—These services provide access to identity attributes that could come from multiple repositories. This approach allows the identity provider to supply virtualized access to its information while keeping the back-end repositories secure.

Security Gateway Services

This set of services provides three key benefits. The first benefit is that you now have an enabling point of integration where legacy applications that aren't able to consume the authentication services directly are still protected. The gateway acts as a proxy that can be a policy enforcement point and that provides integration options to send data to applications. This type of service might be needed for legacy applications or small, specialized services that don't contain any level of protection or access control.

The second benefit is delivering a seamless user experience by making multiple back-end applications appear to be a single application. This "virtualization" requires complex and powerful capabilities to route requests and to do an in-flow modification of both requests and responses. The gateway provides this same type of access services regardless of the type of device being used.

The third benefit is providing an additional layer of security. The proxy hides the various native application platforms behind a consistent, hardened interface to the outside world. This added protection can prevent exposure to vulnerabilities possibly contained in applications and services. The proxy can also do coarse-grained authorization to enhance or replace what the applications do themselves, which provides centralized enforcement of access policies.

Identity Services

The identity service performs the creation, management, storage, and communication of identity information. Connection with identity stores is dependent on powerful integration tools for both internal and external objects. This includes users as well as a limitless variety of devices and their diverse attributes, which speaks to the notion that—when properly designed—identity powers access. This service must also provide a robust workflow and provisioning engines, also making them available as web services for automating business processes. Credential management can be performed through the services' native connectors or through rich, web services interfaces for applications to implement.

Often, a rules engine is used to provide automation and enforcement of business policies. If required for internal audits or government mandates, identity services provide the core information for reporting and access governance.

SIEM Services

Monitoring a correlation report provides detail about authentication or access anomalies that might be the result of attempted breaches. Centralized logging and high-performance analysis of events are needed to identify and alert administrators, and to keep them security-aware of their ASL environment.

Using OpenText solutions to build your ASL

In that it allows you to implement all the ASL components in a synergistic, OpenText offers a collective set of solutions designed to integrate seamlessly into your existing environments. They're designed for scalability and flexibility, both of which are needed for corporate wide identity powered security.

OpenText Advanced Authentication (authentication)

Including, but also going beyond FIDO 2 support, OpenText Advanced Authentication offers a collection of ready-to-go application integrations (RADIUS, VPN, OpenID, OATH, RACF Windows, Mac OS, Linux, Citrix, VMware, and more). OpenText offers wide applicability for your environment. In addition, its broad support for a variety of authentication readers and methods provides a level of flexibility that you haven't enjoyed until now. OpenText's authentication framework is designed for high availability and internal load balancing for continuous uninterrupted operations, regardless of how large or small your environment. Replication between primary and secondary servers provides data integrity and disaster recovery (over LAN or WAN).

- Provides a single advanced authentication framework to protect all physical and digital assets. With support for a wide range of applications and platforms, OpenText Advanced Authentication enables organizations to use the appliances or methods they want.
- Offers a central point of administration for the management of authentication policies for users, groups, devices, or locations. Delegated administration and tracking of changes keeps policies consistent and secure.

OpenText Access Manager (authentication, authorization, adaptive access, attestation)

OpenText Access Manager is a leading provider of web single sign-on solutions. It's especially well-suited for mixed environments that require more than simple federation integration. Often, organizations need a central place to control access as well as to design a particular user experience. OpenText Access Manager is also well-suited to situations where you need to integrate multiple applications into a single user experience.

- Comprehensive secure web access management—OpenText Access Manager delivers single sign-on and access control across the enterprise. There is no need for specialized solutions for cloud-based or complex intranet environments.
- More effective partner collaboration—In addition to its robust single sign-on support, organizations can make access easy through mini portals, mobile SDKs, and even a mobile gateway. Choosing the right access management solution for digital interaction with your partners results in greater sharing of private information and ultimately more effective collaboration.
- Simple and secure access for your customers—Today's digital customers expect convenience and the flexibility to self-enroll with the organizations they choose to interact with, as well as the ability to self-help and administer whenever they find it convenient. If your organization needs a higher level of security, OpenText Access Manager enables you to preserve user convenience while enforcing security to match your risk.

OpenText Identity Manager

OpenText Identity Manager powers the entire identity management lifecycle by managing identities and their associated attributes to minimize privileges. This enables your organization to reduce the costs of manual account management and demonstrate compliance, while reducing the risk of unauthorized access. It delivers benefits for all critical stakeholders across your whole organization, which is why OpenText Identity Manager is designed to manage the complete identity lifecycle in a modular yet integrated manner, so you can address current and future needs as they come. This includes:

- Automated provisioning, de-provisioning, and account management for users and things.
- Powerful rules engine and extensive connectors for full user lifecycle management from onboarding to project level authorizations, to disabling accounts.
- Event-driven automation engine provides immediate automation based on identity and access governance requirements.
- Reports needed to satisfy audit or compliance requirements.

Why OpenText?

OpenText provides security solutions that help organizations with workforce and consumer identity and access management at enterprise-scale. By providing secure access, effective governance, scalable automation, and actionable insight, OpenText customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Resources

OpenText Identity and Access Management

Learn more ›

YouTube channel

Watch the videos ›

OpenText Identity Governance is an identity governance and administration (IGA) solution that seamlessly integrates identity governance (IG) and identity manager (IM) to elevate your organization's efficiency and protect its valuable data. Unlock the full potential of identity management by simplifying administrative tasks, boosting operational effectiveness and empowering business stakeholders to confidently manage application and data access permissions.

- Governs access to all resources across your environment, whether you choose to deploy on premises or via SaaS.
- Collects and visualizes identities and entitlements across your entire environment.
- Automates application fulfillment with a user-friendly, self-service access request and approval system.
- Reduces rubber stamping with analytics that provide business context and risks associated with each request.
- Triggers access reviews on high-risk changes, with interventions needed only for exceptions.

OpenText Self-Service Password Reset

OpenText Self-Service Password Reset by OpenText helps you enforce strong credential policies so you can reduce potential breaches because of poor password practices. With OpenText Self-Service Password Reset, users confirm their identity using a wealth of customizable verification techniques, including two-factor or strong authentication. OpenText Self-Service Password Reset is a convenient, user-friendly, web-based credential management tool that integrates with other OpenText identity and access solutions. Because users can self-enroll in an organization's environment, OpenText Self-Service Password Reset is well-suited for B2C, B2B, and other large user environments.

- Offers self-service password management.
- Provides engine and UI for challenge questions.
- Administration and authentication type rules.
- Includes account activity reports: intruder lockout, daily usage, and online log information.
- Fulfills compliance requirements with detailed audit trails and workflow approval.
- Provides reports needed to satisfy audit or compliance requirements.

opentext™