opentext™ | Cybersecurity

Position Paper

Cracking the Access Management Code for Your Business

As the digital transformation expands across your business, delivering secure access to it has made a modern identity and access management (IAM) solution a must, but too often it’s treated as an afterthought. This position 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 of your applications and digital services.

Table of Contents

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.

As the number of unmanaged applications grows, the challenge to secure them becomes more precarious.

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 needed security layer to protect themselves, but as part of an Accidental Architecture they're not within a cohesive IAM infrastructure. This position 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 of your applications and digital services.

Exacerbating the security challenge is the widespread use 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. It is this approach that breeds the Accidental Architecture and limits the effectiveness of whatever IAM infrastructure is in place. As a result, 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. At some point, 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 at the end of the day, 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.

Figure 1. An Accidental Architecture can leave organizations with a shaky infrastructure.

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 point in 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 why the Accidental Architecture leads to access fatigue is because 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.

There are a number of reasons why organizations find themselves with an Accidental Architecture, but the result is always the same—environments that are inherently less secure while being more costly to manage.

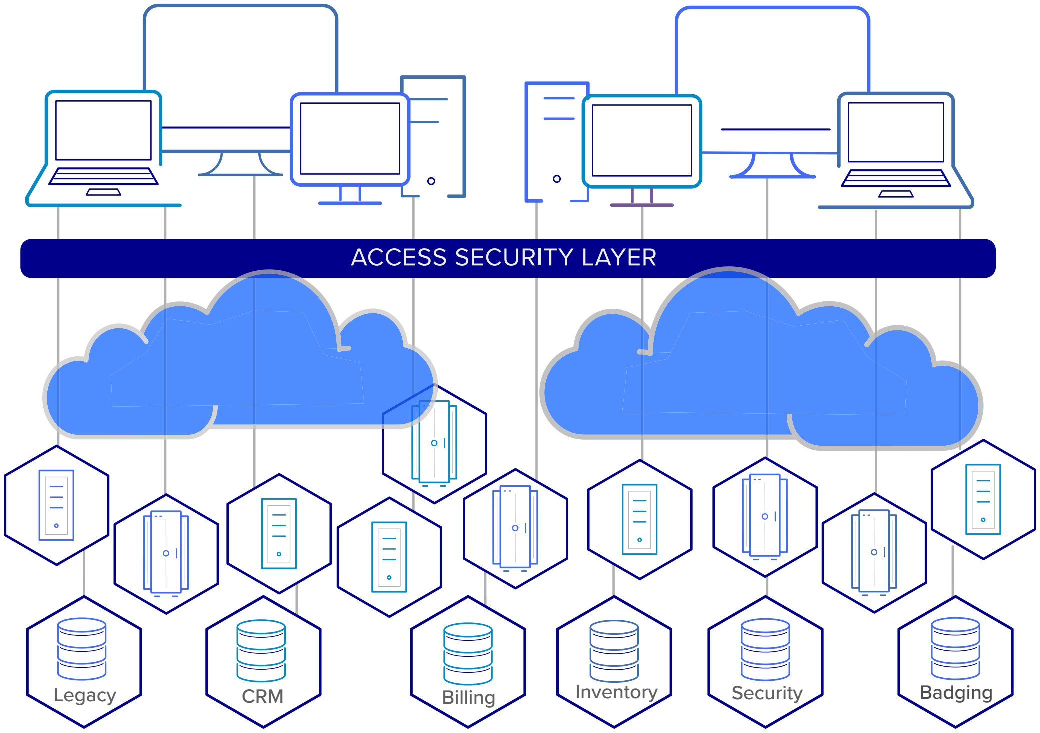


Figure 2. A properly designed Access Security Layer is flexible and comprehensive to support any user, device, and location. It spans across all cloud and legacy services.

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.

Businesses need to keep access as convenient as possible and the level of security invoked needs to match the risk at hand.

Any Device from Any Location

A well-designed Access Security Layer (ASL) provides access control and single sign-on for your applications on any device used from any location. When you stop and think about 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 keep access as convenient as possible, the level of security invoked needs to match the risk at hand. 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.

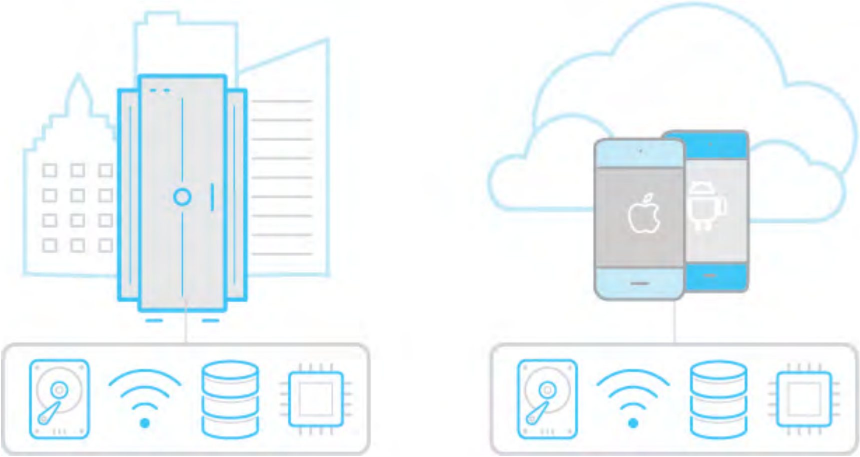


Figure 3. Access control and single-sign-on can be provided for any device or from any location with a well-designed ASL.

Not Just Anybody, but Everybody

The key to onboarding a new digital consumer (customer, patient, citizen, etc.) 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 profile or other information needed to automate their identity across your environment.
- Match user verification to the risk at hand. Don't make accessing your service harder than it needs to be. If the information at hand is low risk and you have indicators (known device, expected location, repeated access, etc.) verifying the person's identity, then 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. The goal is to attain a customized balance between delivering a frictionless user experience and applying the right amount of security.

Today you need to be expert in onboarding your digital customers

- Registration
- User verification
- Account management
- Privacy and consent management

Figure 4. Proficient onboarding of your digital customers makes it easy for them to become a known user, matching verification to need..

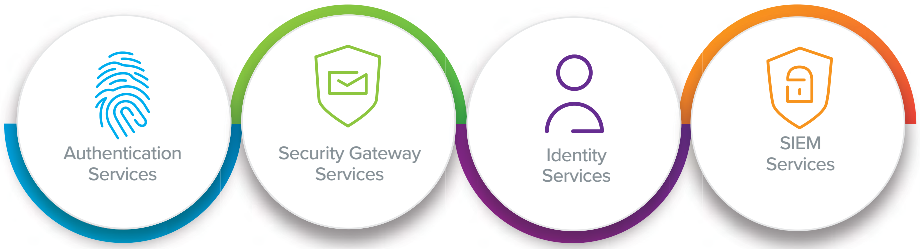
What Is an Access Security Layer?

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. The ASL consists of four areas of service.

Authentication Services

1. Federation
2. Advanced Authentication
3. Authentication Web Services
4. Identity Web Services

Access Security Layer Services:



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.

Advanced Authentication—This is becoming a firm requirement for most environments in order 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.

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.

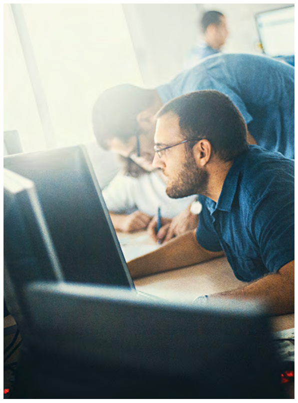
The third benefit is providing an additional layer of security. The proxy hides the various native application platforms behind a consistent, hardened interface to the outside world. This added protection can prevent exposure to vulnerabilities possibly contained in applications and services. The proxy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

Key Benefits of Security Gateway Services

- Enabling point of integration where legacy applications are protected.
- Seamless user experience.
- Additional layer of security.

Identity Services

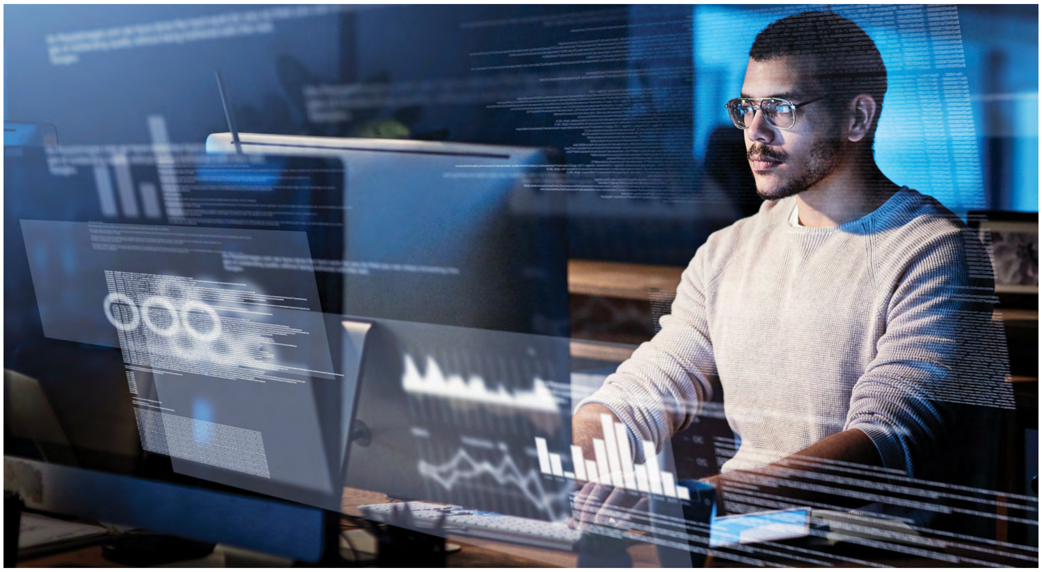
The Identity Service performs the creation, management, storage, and communication of identity information. Connection with identity stores is dependent on powerful integration tools for both internal and external objects. This includes users as well as a limitless variety of devices and their diverse 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 NetIQ to Build Your Access Security Layer
As a longtime leader in building Identity and Access Management solutions for organizations of all types, NetIQ has a suite of products that you can use to build your access security layer.

NetIQ Advanced Authentication

With its collection of ready-to-go application integrations (RADIUS, VPN, OpenID, OATH, FIDO, RACF Windows, Mac OS, Linux, Citrix, VMware, and more), NetIQ Advanced Authentication by 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. The NetIQ Advanced 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, NetIQ Advanced Authentication enables organizations to use the appliances or methods they want.
- 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.

NetIQ Advanced Authentication
Future proof your authentication environment

NetIQ Access Manager

NetIQ Access Manager by OpenText™ is a leading provider of web single sign-on solutions for your users. It's especially well-suited for mixed environments that require more than just simple federation integration. Often, organizations need a central place to control access as well as to design a particular user experience. NetIQ 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—NetIQ 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, Access Manager enables you to preserve user convenience while enforcing security to match your risk

NetIQ Access Manager

For your cloud based or on-premise applications and services

NetIQ Identity Manager

NetIQ Identity Manager by OpenText™ 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 NetIQ 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.

- Automates 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
- Provides the reports needed to satisfy audit or compliance requirements

NetIQ Identity Manager

Manage identities and their associated attributes to minimize privileges.

NetIQ Self Service Password Reset

NetIQ Self Service Password Reset by OpenText helps you enforce strong credential policies so you can reduce potential breaches as a result of poor password practices. With NetIQ Self Service Password Reset, users confirm their identity using a wealth of customizable verification techniques, including two-factor or strong authentication. NetIQ 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 to an organization's environment, NetIQ 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 question
- Administration and authentication type rules
- Account activity reports: intruder lockout, daily usage, and online log information
- Fulfills compliance requirements with detailed audit trails and workflow approval

NetIQ Self Service Password Reset

Enforce strong credential policies.

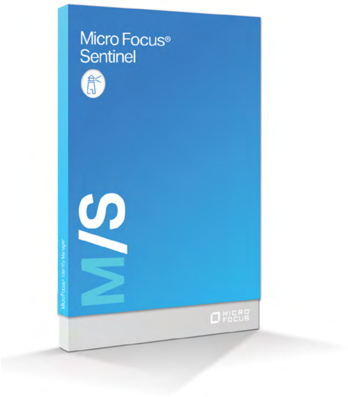
ArcSight Sentinel

ArcSight Sentinel by OpenText™ can be used for most any environment. From the simplest needs for managing data collection, storage, analysis, and management of events and security logs to a full-featured Security Information and Event Management (SIEM) solution. These different tiers of implementation can be used to match the level of deployment, administration, and day-to-day use to the level of security that you need. Sentinel provides true "actionable intelligence" in situations where security professionals need to understand their threat posture and prioritize their response.

- Log management available as an appliance for an out-of-the-box solution to consolidate distributed cloud and internal services
- Simple click driven UI to define customized reports ready for repeated retrieval
- Out-of-the-box intelligence to detect many threats
- Built-in anomaly detection automatically detects changes that can represent emerging threats

ArcSight Sentinel

Provides true "actionable intelligence."



Connect with Us
www.opentext.com

About NetIQ

NetIQ 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, NetIQ customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the NetIQ homepage at **www.cyberres.com/netiq** to learn more. Watch video demos on our NetIQ Unplugged YouTube channel at **www.youtube.com/c/NetIQUnplugged**.