opentext™ | Cybersecurity

Position Paper

Application Security Framework for Zero Trust

Table of Contents

Executive Summary

OpenText™ Government Solutions security services is an integrated set of cybersecurity product offerings designed to enable zero trust principles at the network boundaries. Utilizing these services presents an opportunity to quickly increase the maturity of your environment by delivering advanced application security capabilities. It is an impressive set of tools and services that work independently or in concert with existing tools. Working closely with SD-WAN technology partners, our application security services not only help deliver current zero trust requirements, but also accelerate the maturity of the environment more broadly through shared enterprise zero trust services.

Key benefits to your zero trust programs:

- Apply the most advanced risk analytics to continuous access decisions.
- Enable zero trust services for user applications and data at the edge.
- Accelerate zero trust architecture (ZTA) maturity with advanced threat detection and remediation capabilities (e.g., initial access, privilege escalation, lateral movement, and many additional MITRE ATT&CK TTPs).
- Detect and protect sensitive data end-to-end.
- Create an integration path for legacy applications.

Organizations require new application security approaches in order to reach a zero-trust level of security—one where the default assumption is a hostile environment. Implementing continuous authentication at the edge creates true adaptive access by:

- Extending monitoring and control throughout the user session lifecycle.
- Detecting when the risk level has changed since the start of the session and then initiating an additional authentication request.
- Tuning (reducing or increasing) the authorization level based on the identified risk and available identity verification.

In order for the adaptive security infrastructure in your environment to be effective, edge security controls need to move beyond prescriptive risk policies and leverage deeper request context and behavior analysis. As best practices suggest, using a hybrid approach where prescriptive access policies are enforced by default but are given less weight individually as behavioral information for a specific user is the most effective. To accommodate diverse scenarios, organizations typically require a mix of strong and passive authentication methods. This enables you to apply the best fit based on the specific need and the associated risk (i.e., how sensitive the information is and the context of the request).

We welcome the opportunity to join your zero trust team and help you expedite a smooth transition to ZTA, meet existing mandate deadlines, and apply more effective security operations.

OpenText Application Security Services

Our view is that zero trust is a welcome addition to the application security stack, but it requires an underlying shift in the way access is delivered. With zero trust, neither the user's device nor the origin of the request automatically grants access to services. Rather, it requires a greater understanding of the context of the request, as well as a higher level of verification of the identity requesting it. It's a rigorous and adaptive level of security.

With continuous authentication, the system's assessment of whether access to a service should continue is repeatedly reassessed. Access metrics are continuously gathered and the risk is frequently being recalculated. As your IT security teams define the risk models that fit their mission, the zero trust paradigm is a closed-loop representation, not an open one. Not only is closed-loop monitoring and control a higher security approach, but it's conducive to behavioral analytics—which provides a level of identity-centric metrics far beyond standard risk metrics commonly used today. The grant-and-forget model of access control has its place in enforcing legacy policies, but it falls significantly short in today's threat landscape.

In addition to the security advantages of retaining access control of each session, continuous user tracking does more than enhance the ability to protect assets—it enables you to build a much larger library of user context. This repository of contextual information provides a foundation from which user and entity behavioral analytics (UEBA) can be applied to build a deeper level of risk intelligence that extends far beyond typical risk-based authentication.

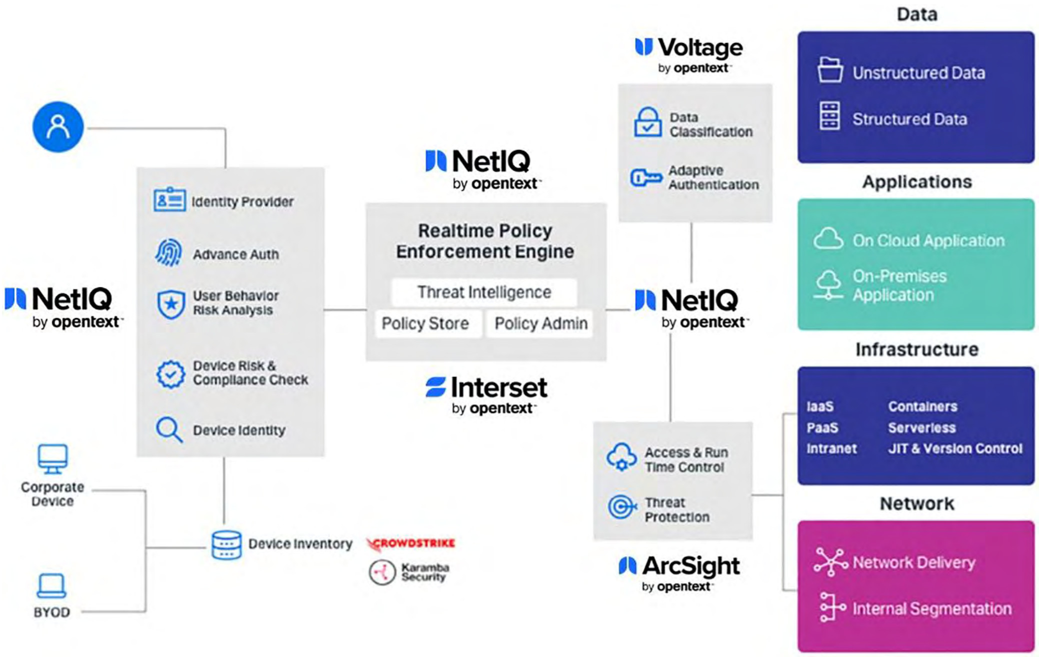


Figure 1. Zero Trust Architecture | Application Security Framework

In summary, by incorporating continuous authentication capabilities at the edge in your environment, it provides these immediate security benefits as well as more sophisticated protection, such as:

- Measuring actions to determine whether the authorization level should be changed offers better protection immediately.
- Quickly identify risky behaviors and invoke the right policy action (honor request, invoke additional authentication(s), or terminate session) justified by calculated levels of risk.
- Gathering contextual information each time protected data is accessed builds a more complete profile of the user's normal behavior.
- Continuously executing analytics on contextual data delivers a more accurate picture of expected behavior, improving the ability to identify high-risk events.
- Monitoring all the different types of input sources for risk (such as API and microservices), which account for the bulk of data movement.
- External parameters include more sophisticated contextual information, such as UEBA-based metrics.
- Continuous authentication allows for continual scoring and active session control.

Multi-Factor Authentication Framework

Because new authentication purchases typically originate within a program, they are often solved from a specific tactical perspective. This approach leaves organizations with multiple authentication silos (building access, remote access, compliance requirements, etc.). These disjointed implementations impose higher administrative overhead and inefficient processes. But, more importantly, they create vulnerabilities due to inconsistent authentication policies.

In short, authentication frameworks must:

- Drive down costs and complexity through consolidation.
- Increase security through centralized policies.
- Offer more multi-factor authentication options.

An MFA framework must also satisfy a broad set of organizational needs. For example:

- It must offer simplicity of deployment and administration for small organizations, while meeting the scalability requirements of large ones.
- It needs to be adaptable to differences across the organization, whether it's concentrated within a specific region or is highly distributed across the globe. Regardless of the shape of the organization, the framework must deliver quick response to authentication requests.
- The more methods a framework can support, the more flexibility organizations will have as they consolidate their authentication silos into one. The framework must also be able to easily expand as new authentication technologies are introduced into the market.

Your environment adoption will require providing mission partners with options and flexibility for both current and future MFA needs. NetIQ Advanced Authentication by OpenText ensures that you won't get locked into authentication silos or stuck with outdated technology. OpenText offers an open framework that aggressively updates as new technologies emerge, including compatibility with FIDO U2F-based devices.

FIDO Universal 2nd Factor (U2F) enables organizations to support an environment where users manage their own authentication devices. NetIQ Advanced Authentication provides a robust framework to deliver that support to your applications without the need for development. Not only do you benefit from deferring token costs, but your users are able to incorporate an array of new alternative token options that you authorize them to use. With the deep level of support provided by NetIQ Advanced Authentication, there is no better framework from which to provide a U2F authentication environment moving forward:

OAuth2	Microsoft OATH	Kerberos
OATH authentication	NFC ISO/IEC	PKSCS7 & PKCS11FIPS 140.2
Google Authenticator	RADIUS	

Beyond the authentication types available in RADIUS, NetIQ Advanced Authentication offers more native methods than any other solution on the market—currently supporting 37 MFA methods. Why does that matter? Because both your internal and external users access sensitive information from a wide range of situations and from multiple devices. With its collection of ready-to-go application integrations (RADIUS, OpenID, OATH, FIDO, RACF, z/OS, Windows, Mac OS, Linux, Citrix, VMware, and many more), NetIQ Advanced Authentication offers wide applicability to your application security stack. In addition, its broad support for a variety of authentication readers and methods provides the next level of flexibility.

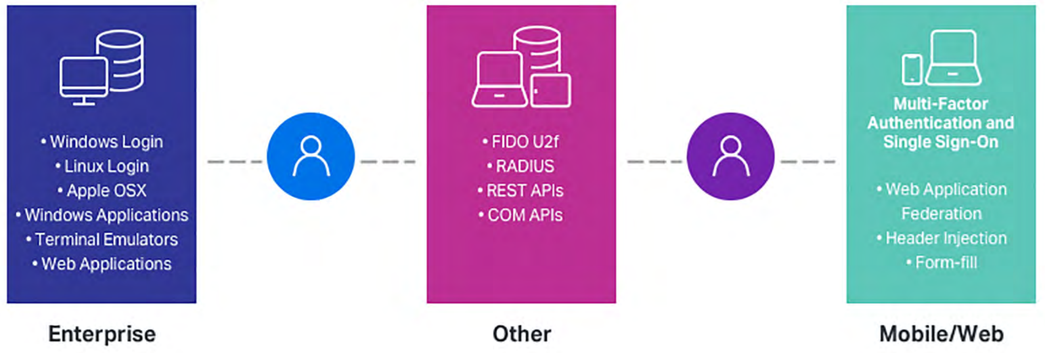


Figure 2. Advanced Multi-factor Authentication Framework

When applying zero trust to an environment from an identity perspective at the application layer, key capabilities are continuous authentication and authorization:

- Continuous authentication will re-verify an identity as many times as needed in response to a risk score that has spiked within a session. Depending on the strength of the method, one or more successful authentications might be needed to lower the risk score.
- In response to a rise in the risk score at any time within a session, an access request is subject to potential restriction or even a termination.
- The more MFA methods that mission partners have at their disposal, the better able they are to adopt a zero trust environment that doesn't decrease their productivity.

NetIQ Advanced Authentication is less complex to configure and maintain than the myriad of existing solutions. Its strength also lies in out-of-the box integrations that provide a wealth of configurable authentication options. With NetIQ Advanced Authentication as part of the enterprise application security for your environment, all of your application access will benefit from the increased security, flexibility, and usability.

Continuous Risk Services

The NetIQ Risk Service Service by OpenText organizations to deploy adaptive access control without the need for complex infrastructure. Adaptive access is a process by which context, past behavior of a user, and the sensitivity of the application are evaluated to determine the authentication required to access the application. The goal of adaptive access is to provide the appropriate risk-mitigating assurance levels for access to sensitive resources by requiring users to further demonstrate that they are who they say they are.

NetIQ Risk Service provides adaptive access through the risk assessment of user access to applications or services. It analyzes a range of indicators associated with an access activity to determine the probability that the activity is fraudulent. Factors such as the location of the user, time of access, profile and other contextual information, historic records, and behavioral data of users and entities are used to compute the risk indicator.

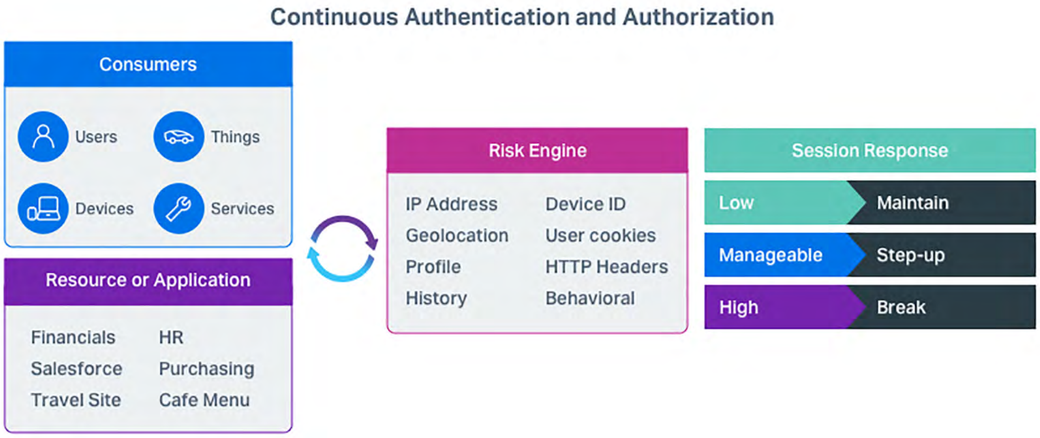
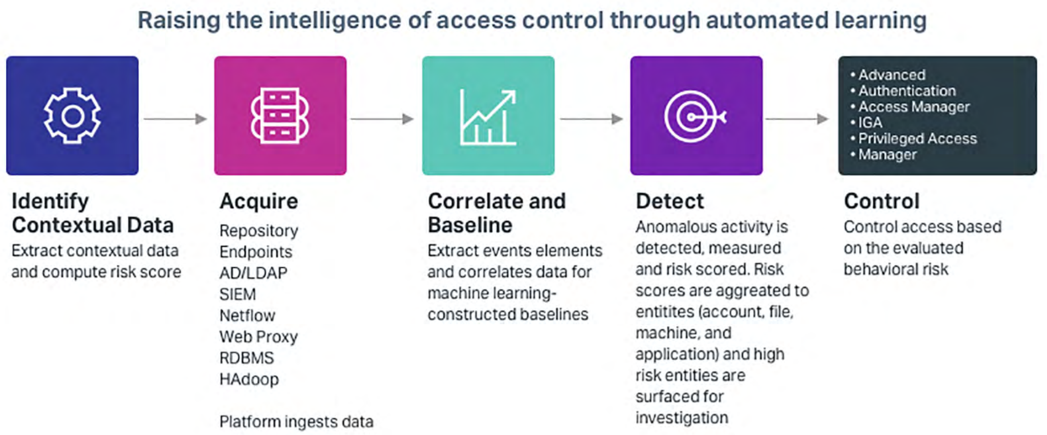


Figure 3. Applying Different Access Policies Based on Level of Riskn Framework

With NetIQ Risk Service as part of the Application Security Stack, your environment can assess the potential risk of a particular login attempt before authenticating the user. Pre-authentication risk assessment enables you to fine-tune the granular authentication factors for potential risk mitigations. It also includes out-of-the-box integration with NetIQ Access Manager by OpenText and NetIQ Advanced Authentication to provide frictionless and risk-aware adaptive and continuous authentication. Of particular importance, NetIQ Risk Service can natively ingest Interset or ArcSight Intelligence (AI) risk analysis to directly utilize behavioral analytics in a combined risk computation.

Interset/AI uses unsupervised machine learning algorithms to discover patterns of user access and identify threats. Hundreds of built-in machine learning algorithms extract the available entities (individual users, machines, IP addresses, web servers, printers, etc.) from access information and log files and observe events that relate to these entities to determine what normal or expected behavior is. As new information comes through the analytics process it is evaluated against previously observed behavior, as well as dynamically measured statistical peer groups, to assess potential risk.

While Interset/AI isn't part of the NetIQ by OpenText product line, it is the OpenText Cybersecurity solution for applying state-of-the-art machine learning to create the advanced user behavior analysis. It gathers user metrics during the entire session, from which it develops fine-grained risk assessment criteria at the user level. Used in conjunction with NetIQ Risk Service's built-in engine, Interset/AI offers the unique ability to increase usability while measurably enhancing security.


Raising the intelligence of access control through automated learning

- Advanced Authentication
- Access Manager
- IGA
- Privileged Access Manager

Identify Contextual Data
Extract contextual data and compute risk score

Acquire
Repository
Endpoints
AD/LDAP
SIEM
Netflow
Web Proxy
RDBMS
HAdoop

Platform ingests data

Correlate and Baseline
Extract events elements and correlates data for machine learning-constructed baselines

Detect
Anomalous activity is detected, measured and risk scored. Risk scores are aggreated to entitites (account, file, machine, and application) and high risk entities are surfaced for investigation

Control
Control access based on the evaluated behavioral risk

Figure 4. Access Risk Service Uses Advanced Behavior Analytics

Increasingly, identity impostors are using more sophisticated tactics to defeat our digital defenses. NetIQ Risk Service protects against high-risk authentication and application access requests by initiating multi-factor step-up authentication when risk scores indicate that a higher level of identity verification is needed. Because NetIQ Risk Service offers a simple rules engine with built-in metrics, you can get started quickly with minimal effort. And in addition to user access, it offers risk-based access protection for APIs, including mobile services and microservices. NetIQ Risk Service enables you to evolve from static authentication and access to an adaptive and continuous authentication environment. And, it can consume contextual-related metrics from a variety of sources. Administrators can get started with NetIQ Risk Service using out of-the-box metrics that they can adjust and configure themselves.

Detecting Known Threats

NetIQ Risk Service computes risk information from a wide range of sources, including IP address and reputation, geolocation, user's identity, roles, and profile information, device ID, uniquely created fingerprint of the device, cookie and browser information, header information, history, pattern of access, and information from external sources. The breadth of input range allows for fine-grained risk computation, helps identify potential threats faster, and applies rules-based policies to mitigate increases in risk. These prescriptive contextual rules have become the foundation of risk-based access control. But although these access requirements are essential for enforcing government security policies, they are unfortunately not enough on their own. Over time, both insiders and persistent attackers often learn how to navigate around these static risk policies. These unknown threats require additional controls based on dynamic risk policies.

Detecting Unknown Threats

Catching crafty or persistent threat actors requires not only detecting well-known threats, but also enabling behavioral profiling of every entity. The best way to identify and protect against impostor-based or malicious insider attacks is to learn the unique normal behavior of every identity in the environment. This type of baseline enables NetIQ Risk Service to detect most anomalous and suspicious behaviors, whether they are malicious, accidental, or otherwise suspect.

NetIQ Risk Service offers an Interset/AI option that can incorporate behavioral analytics into its risk computation. Interset/AI uses unsupervised machine learning and has hundreds of built-in algorithms that discover user access patterns and activity patterns to identify priority threats from billions of events. NetIQ Risk Service can also support the creation of a database for identifying unusual user access patterns for evaluating and adapting your risk policies. The more NetIQ product line components you implement in your environment, the richer the analytics fed into to the Interset engine.

MITRE's ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a living knowledgebase of threat tactics and techniques observed in real-world attacks on enterprise networks and it plays a pivotal role in our behavioral analytics. Today, Interset/AI covers 75 percent of the ATT&CK framework that has been seen in the wild and our coverage will continue to grow. It leverages more than 450 machine learning models to baseline the behavior of every user and entity within an environment and evaluate deviations from those baselines as potentially risky behaviors. Our machine learning models are carefully mapped to ATT&CK's 219 techniques, providing effective coverage against a range of threats that can facilitate exfiltration of high-value information, fraud, and more.

To create accurate risk scores, the Interset/AI analytics engine utilizes artificial intelligence methods that include probabilistic methods for uncertain reasoning, clustering algorithms, classifiers, statistical learning methods, and neural networks. It also employs a statistical approach to compress the various anomaly probabilities into a single entity risk score—a critical aspect of meaningful, actionable security analytics.

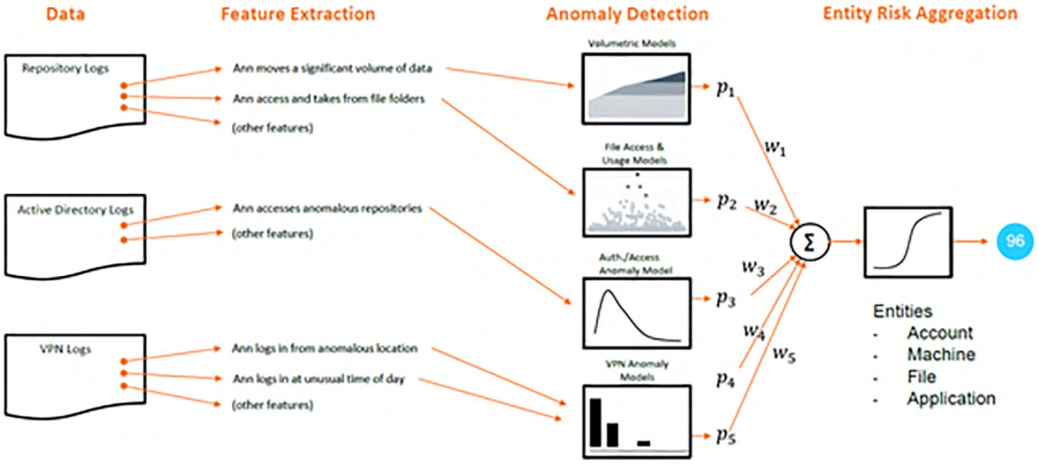


Figure 5. Analytical Framework | From Log Data to Risky Entity

A score is computed for each event to quantify the anomalies. Interset/AI aggregates these event probabilities into their associated entities, taking into consideration the entities' previous risk scores as well as outside intelligence that can affect the entity (such as employee watch lists, threat intelligence, and data from other security tools). This produces a risk score that considers all entities related to an event based on all the context that Interset/AI can gather.

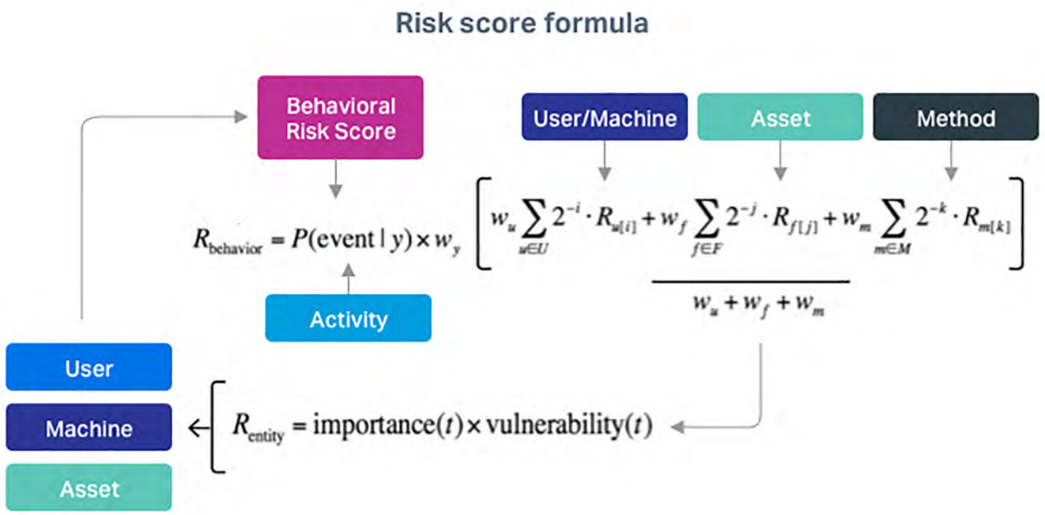

Risk score formula
Behavioral Risk Score
User/Machine
Asset
Method
$R_{\text{behavior}} = P(\text{event} \mid y) \times w_y \left[w_u \sum_{u \in U} 2^{-i} \cdot R_{u[i]} + w_f \sum_{f \in F} 2^{-j} \cdot R_{f[j]} + w_m \sum_{m \in M} 2^{-k} \cdot R_{m[k]} \right]$
$w_u + w_f + w_m$
Activity
User
Machine
Asset
$R_{\text{entity}} = \text{importance}(t) \times \text{vulnerability}(t)$

Figure 6. Mathematical Formula behind Behavioral Risk Score

As the analytics engine refines anomaly patterns, it learns which users create more risk, which files are the most at risk, and which machines are most often part of risky activities. Through statistical analysis, the engine also quantifies just how anomalous an observed behavior is. The more an entity is involved in high-risk anomalous activities, the more its risk score increases. Conversely, a risk score will decrease over time for an entity that is not involved in high-risk activities, but instead behaves normally compared to itself and other similar entities. This risk scoring is calculated for every single entity—every user, machine, IP Address, printer, web server, file share, etc. From these millions of individualized risk scores, the machine learning normalizes them in such a way that they can all be compared with each other accurately, creating a single rank-stacked list of threat leads for security teams to prioritize in terms of time and effort.

Beyond its out-of-the-box integrations, NetIQ Risk Service offers interfaces and APIs for integration with third-party SASE and CASB services for contextual attributes, risk scoring, or behavior inputs.

Unified Access Control Framework

By keeping your authentication and authorization within a single solution, you're able to secure and control access with a unified set of policies and processes. This approach is especially true with mobile users. In addition to siloed mobile apps being inherently less secure, they also create added work for developers (who should be focused on the mobile app itself, rather than its security or the systems it uses. As with desktop and laptop users, having a single access control framework eliminates redundant credential management and other disparate and often disconnected access control policies.

Key Unified Access Control Capabilities for your environment:

- Simplified application and service portal. If your organization doesn't already have a centralized place from which users find and launch their applications, NetIQ Access Manager's built-in portal provides an easy way for your administrators to configure their users' experience as they access applications and services from their laptops, tablets, and smartphones. The portal optimizes the view for each form factor to make navigation quick and easy. You can also customize and brand the portal with your own specific look and style.
- Extending SaaS and web application SSO to mobile users. For those that want to extend their dynamic cloud and web-based apps to their mobile users, NetIQ Access Manager does that for you. It supports the NetIQ MobileAccess app (found on the Apple Apps Store or Google Play), which keeps them secure and simple to access. Within the app, your users are presented with a mini corporate portal from which a single touch of an icon gives them an SSO experience. Best of all, administrators can typically port these applications in half a day.
- Mobile single sign-on. NetIQ Access Manager supports native mobile SDKs, enabling users to offload single sign-on. For delivering services through native mobile apps, NetIQ Access Manager includes an SDK for iOS, OpenID Connect, or plain OAuth.
- Onboarding your environment users. NetIQ Access Manager enables users to sign up and set up their own accounts, as well as automate the self-service onboarding and account maintenance process with the Advanced Authentication framework.
- Complete access and access policy management for your users and mission partners. NetIQ Access Manager's robust federation supports all the modern federation standards used today, with service as either an IdP or SP, enabling you to trust your partner's identity provider. You can secure access for all personnel using their mobile devices, enabling native apps or extending your existing web-based applications to them.

NetIQ Access Manager is a full mobile, web, legacy application access gateway solution with federation and single sign-on for users and mission partners. It is especially well-suited for mixed environments that require more than just simple federation and situations that require the integration of disparate enterprise applications into a single secure and consistent user experience.

NetIQ Access Manager provides reverse proxy capabilities, which serves as the application and services gateway. The NetIQ Access Gateway makes applications accessible across multiple platforms and simplifies the user experience across devices. And while it is often used to add a security layer to existing applications, you can also use it in conjunction with federated single sign-on to deliver the best user experience.

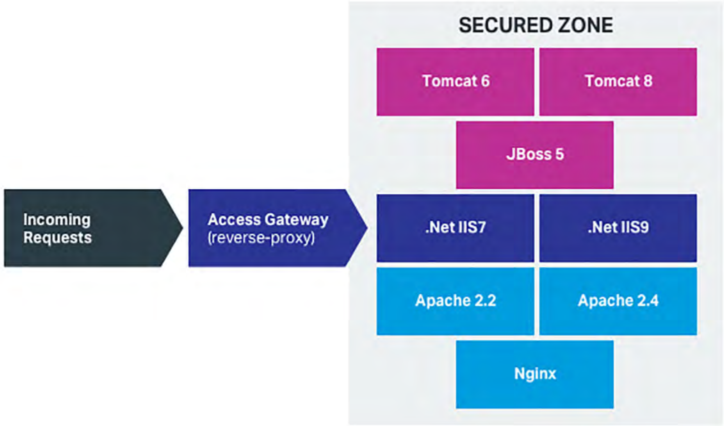


Figure 7. Application Protection with Access Gateway

The NetIQ Access Gateway reverse proxy can also be used to provide centralized access request logging, which can either supplement or replace any logging done on the backend application platform. Capturing request logs at the gateway is often simpler than trying to consolidate logs from the multiple application platforms found in most environments. The gateway logs also capture information about requests that might not be available in the application logs.

NetIQ Access Manager includes an analytics service that can be used to collect and visualize data from the access gateways and the identity providers. The following figure shows one of the out-of-the-box monitoring and reporting dashboards.

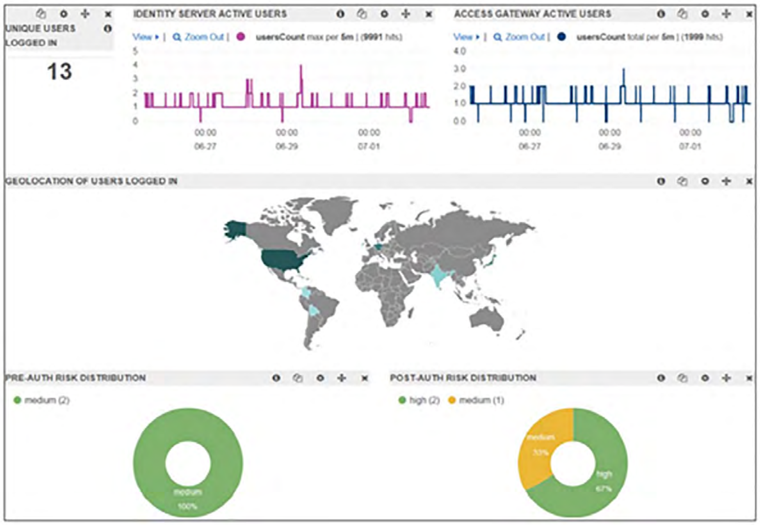

UNIQUE USERS LOGGED IN
13
IDENTITY SERVER ACTIVE USERS
View ▸ | Zoom Out | ● usersCount max per 5m | (9991 hits)
5
4
3
2
1
0
00:00 06-27
00:00 06-29
00:00 07-01
ACCESS GATEWAY ACTIVE USERS
View ▸ | Zoom Out | ● usersCount total per 5m | (1999 hits)
4.0
3.0
2.0
1.0
0.0
00:00 06-27
00:00 06-29
00:00 07-01
GEOLOCATION OF USERS LOGGED IN
PRE-AUTH RISK DISTRIBUTION
● medium (2)
medium 100%
POST-AUTH RISK DISTRIBUTION
● high (2) ● medium (1)
medium 33%
high 67%

Figure 8. Example Access Dashboard

While similar technology exists, NetIQ Access Manger's flexible and compact approach simplifies its configuration and delivers the superior performance needed for large or distributed environments. It requires fewer system resources and human resources to administer.

Credential and Endpoint Security Controls

Our well-designed Access Security Layer (ASL) delivers multi-factor authentication, dynamic access controls, and single sign-on to your applications for any authorized device used from any location. Considering this "any" doctrine, it is clear your environment requires the ability to account for a variety of remote access scenarios from which protected information is being requested. While the mission demands that you keep access as convenient as possible, the level of security invoked needs to match the existing risk at hand. A remote user requesting access from a known device from an expected location poses less risk to the mission than an unfamiliar device from a foreign or uncontrolled location.

Based on measured risk, NetIQ Access Manager can dynamically change a user's authorization to applications and services, making it possible to respond immediately to a specific threat. NetIQ Access Manager's ability to enforce an immediate multi-factor, step-up authentication with an alternative token, or deny access altogether based on real-time endpoint and user attributes, makes it an essential element for establishing an adaptive access system.

The Interset/AI analytics engine can also utilize advanced endpoint detection and response (EDR) threat data into its combined risk assessment. Through the native integration, for example, CrowdStrike Falcon EDR delivers continuous, comprehensive endpoint visibility that spans detection, response, and forensics. Interset/AI analytics can immediately use Falcon sensor data to identify risk associated with endpoint threat vectors. This adds more visibility to the rich CrowdStrike endpoint data to uncover difficult-to-find threats such as advanced persistent threats (APTs). Integration with other EDR service providers is also available.

Along with our partner Karamba Security, we have also just released our IoT SmartGuard offering, a joint security solution to advance the protection of OT networks and vulnerable IoT devices. IoT SmartGuard provides next-level IoT security, stopping malicious code execution in its tracks and providing a transparent view into high-risk devices in your organization.

IoT SmartGuard combines the efficient pinpointed log generation and deterministic protection from Karamba Security's XGuard with the powerful behavioral analytics engine fromOpenText Cybersecurity to empower the security analysts in your SOC.

This solution results in efficient IoT security that quickly detects hard-to-find threats and stops malicious execution on each IoT device. XGuard is easily deployed across a wide variety of devices and operating systems based on the XGuard platform capabilities and configuration, as seen here in Figure 9. It uses a unique cloud-device edge architecture, which optimizes security results in resource-constrained environments.

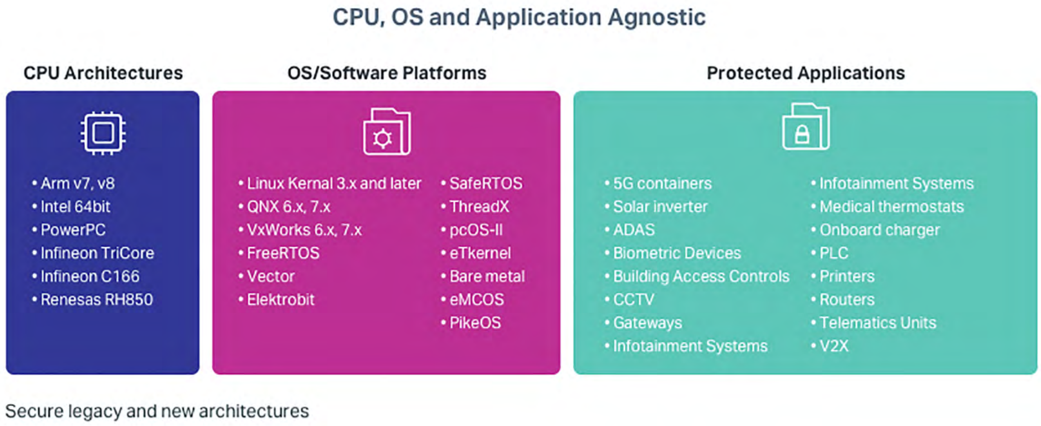


Figure 9. Native platform support offered with IoT SmartGuard

Application Security Controls

Perhaps one of the greatest benefits of deploying our application security services in your environment is unlocking a new point of integration where legacy applications that can't 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 is required for legacy applications or small, specialized services that don't contain any level of protection or access control themselves.

Another 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 do an in-flow modification of both requests and responses. The gateway provides the same type of access services regardless of the type of device being used.

By leveraging these gateway capabilities at the boundaries, your environment will be providing an additional layer of security and application checkpoint. The gateway hides the various native application platforms behind a consistent, hardened interface to the outside world. This added protection prevents exposure to vulnerabilities possibly contained in applications and services. The gateway can also do coarse-grained authorization to enhance or replace what the applications do themselves, which provides universal enforcement of application access policies.

Legacy Application Controls and Integration

The OpenText™ Host Access Management and Security Server (HA-MSS) is an application security layer for users and their devices accessing hosted IBM z/OS, Unisys 2200, Linux, Unix, and Windows-based applications. It offers user-session authorization and universal access control capabilities for those environments are provided by the HA-MSS product, respectively. Its multi-factor authentication framework offers the most native integration of methods available in the industry.

HA-MSS leverages existing IAM systems to authenticate users and authorize system access respectively, logging all activity in a central location. HA-MSS makes it possible to extend IAM authorization schemes to applications without requiring any changes to the application itself or to user workflows. HA-MSS also enables you to specify what users can or cannot do. For example, hardening their terminal emulation client: removing a user's ability to edit macros, locking down the connection settings for TLS 1.2 or 1.3, or masking sensitive application data when it is displayed on the user device.

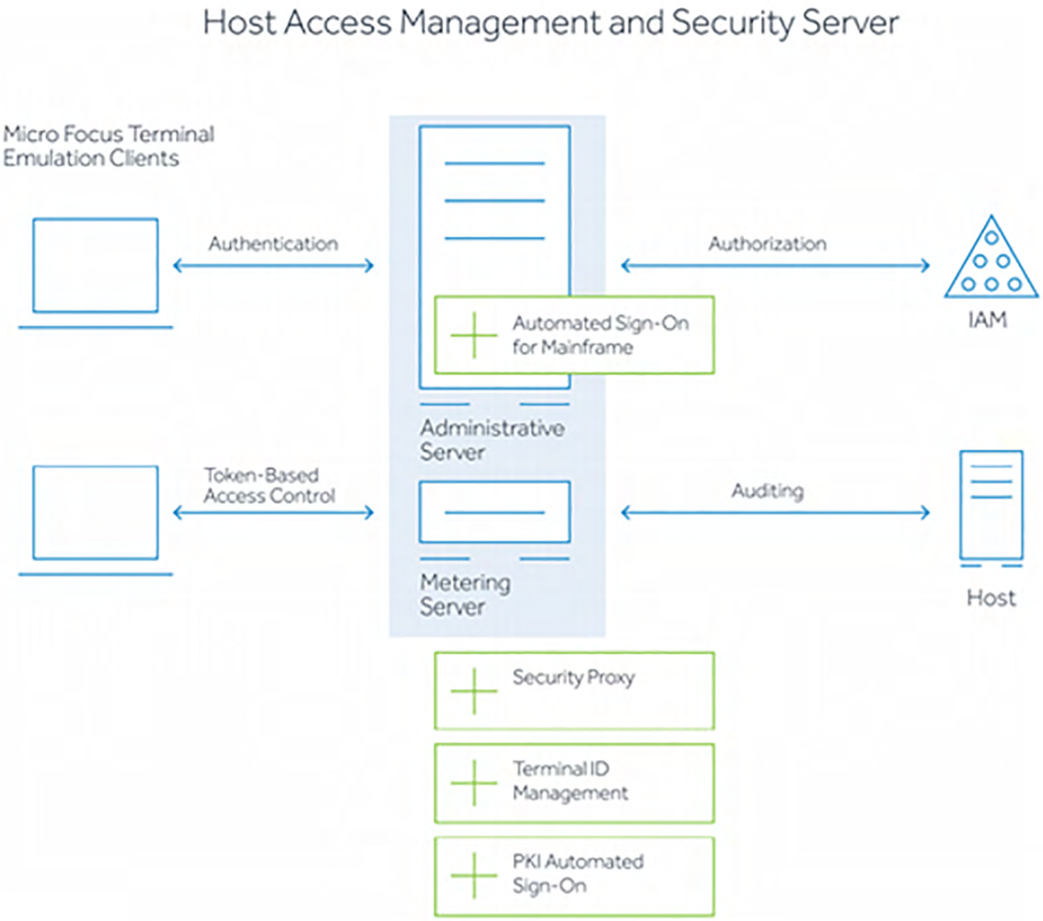
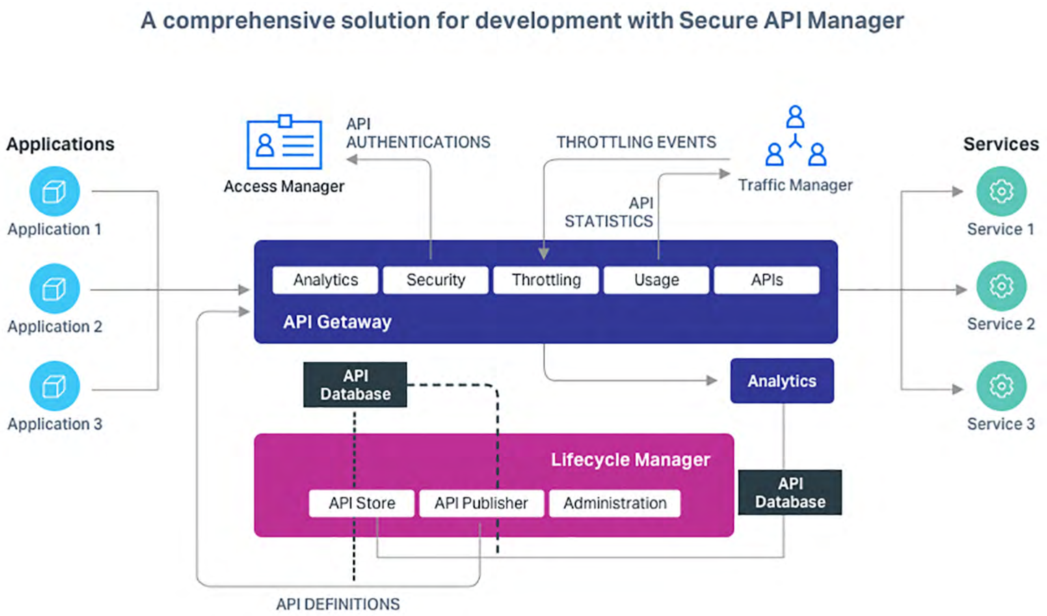

Host Access Management and Security Server
Micro Focus Terminal Emulation Clients
Authentication
Token-Based Access Control
Automated Sign-On for Mainframe
Administrative Server
Metering Server
Authorization
IAM
Auditing
Host
Security Proxy
Terminal ID Management
PKI Automated Sign-On

Figure 10. Access Control Framework for Terminal/Legacy Applications

Current releases of HA-MSS have native integration with our application security services stated here, providing a seamless integration path between your existing legacy system environments and your zero trust initiatives. This very quickly extends the zero trust capabilities being developed for your environment to legacy applications.

API Security Controls

A modern application security stack should enable you to secure API access for your mission partners and users, while also making it easy to combine multiple APIs to create new functionality without exposing your application infrastructure behind it. Introducing NetIQ Secure API Manager by OpenText a comprehensive solution for development, lifecycle management, security, integration and monitoring of all types of APIs—be it REST, SOAP, IoT or legacy custom APIs. NetIQ Secure API Manager includes a highly scalable API Gateway that provides options to secure, control, transform, and manage APIs of all types. The API Gateway allows you to control traffic while enabling secure access to the APIs from anywhere.



A comprehensive solution for development with Secure API Manager

Figure 11. Access Control Framework for APIs and Micro Services

NetIQ Secure API Manager is integrated with NetIQ Access Manager to provide API management and security capabilities that take full advantage of the robust authentication and authorization capabilities provided by NetIQ Access Manager. The same infrastructure that is used to protect cloud, web, mobile, and legacy applications can be extended to protect APIs and micro services. All of the federated authentication can also be utilized. And combined with NetIQ Advanced Authentication, you have the capability to use risk-based, multi-factor authentication with your service-based applications.

NetIQ Secure API Manager consists of two major functional areas:

- The API Gateway provides the runtime functionality to processes service requests. It enforces security, manages and limits API usage, and transforms requests and responses to and from the back-end services. As it does this, it collects data for monitoring and for analytics of API usage.

- The Lifecycle Manager is where APIs are implemented and managed. The Lifecycle Manager handles the publication of new services, controls updates to existing services, and, most importantly, enables you to manage API retirement. Lifecycle Manager also collects extensive data for monitoring and analytics.

NetIQ Secure API Manager extends your access and authentication environment to include secure API delivery for all your mission partner needs. It provides the access controls and central point of administration needed for API manageability and to improve implementation time. This delivers better security compared to traditional and existing hardening practices.

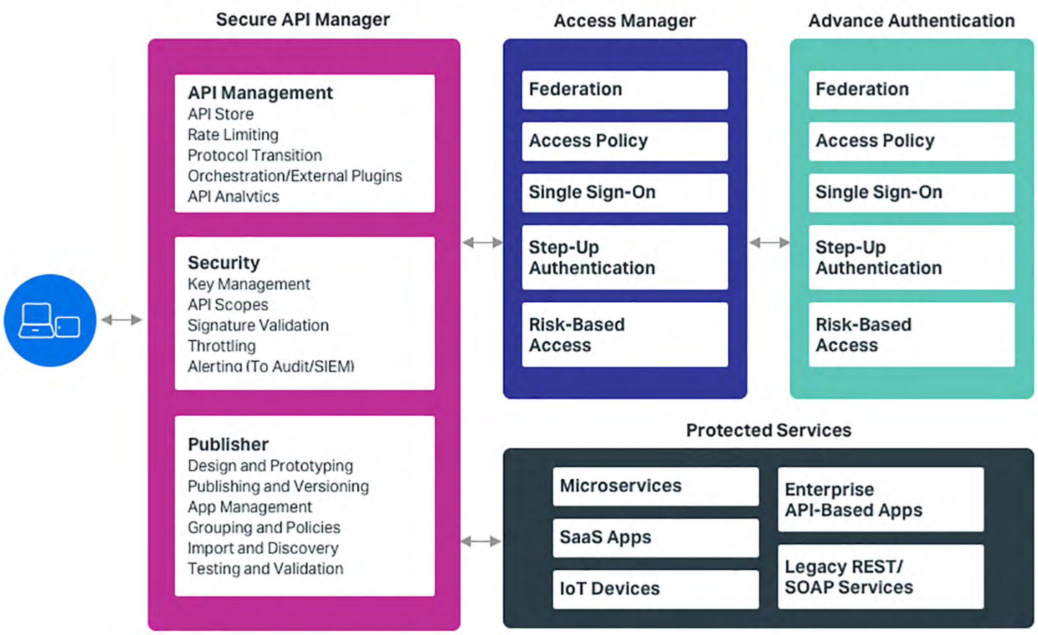


Figure 12. How NetIQ Components Work Together

With NetIQ Secure API Manager, you can limit the rate at which applications can call services. The rate can be limited per application and a total transaction volume per API can also be enforced. This can be used to prevent resources from being over utilized or it can be used to offer differentiated levels of service. NetIQ Secure API Manager can also be configured to control the flow of service calls to the back-end services. This can be used to smooth out utilization so that back-end services are not overwhelmed and users experience smooth performance. Caching information from back-end services is also possible if the data in the response is somewhat static.

Another benefit of using the NetIQ Secure API Manager gateway is that it provides an easy way to centrally collect information about API usage and performance. NetIQ Secure API Manager provides several built-in analytics functions to present this information to both administrators and mission partner users.

Data Protection Framework

Traditional data security controls embedded throughout existing IT infrastructure has proven increasingly ineffective as data has become more pervasive, mobile, and cross-functional. With migration to hybrid IT and an increasing reliance on SaaS applications, organizations might not have the accessibility or development resources for API-level integration of their self-developed applications.

Voltage SecureData Sentry by OpenText protects sensitive data wherever it flows: on premises, in the cloud, and in big data analytic platforms. Voltage SecureData Sentry encryption delivers data privacy protection, neutralizes data breach, and drives mission innovation through secure data use.

Voltage SecureData Sentry accelerates time to value by enabling privacy compliance and offers consistency for end-to-end data protection. Organizations can deploy Voltage SecureData Sentry on premises and in the cloud. Voltage SecureData Sentry communicates with ICAP (Internet Content Adaptation Protocol) capable network infrastructure, such as HTTP proxies and load balancers, to apply security policies to data traveling to and from the cloud. And it intercepts JDBC (Java Database Connectivity) and ODBC (Open Database Connectivity) API calls to apply security policies to data traveling to and from the database. Wherever it is deployed, the enterprise retains complete control over the infrastructure, without the need to share encryption keys or token vaults with any other party. Voltage SecureData Sentry's inspection mode ensures that security policies can be targeted at the specific data fields and file attachments that contain sensitive information.

Voltage SecureData Sentry specializes in data protection for cloud software services as well as on-premises applications. It extends the reach of Voltage SecureData Sentry's data protection technologies to SaaS applications (such as Salesforce, ServiceNow, OpenText ALM Octane, and Microsoft Dynamics 365), as well as to commercial off-the-shelf (COTS) applications. Voltage SecureData Sentry uses dataflow interception techniques to protect sensitive data flowing through the network, ensuring that organizations remain in control of the security of their data used in SaaS and COTS applications.

Voltage SecureData Sentry intercepts data traffic between users and the target application or system where that data is used and typically stored. The goal of this protection is usually to hide sensitive information from the target application or database, without interfering with the core functionality of the target application. The user of the protected system might not even be aware that the protection has taken place. It is also possible to configure protection that deliberately protects or transforms data such that the user can identify it is protected. At a high level, content and related metadata is received by the Voltage SecureData Sentry Engine from ICAP proxies or database wrappers. Voltage SecureData Sentry uses profiles configured by the administrators to analyze the data and determine what data requires protection. Protection flows determine how data is protected and in what format the data is returned to the source application.

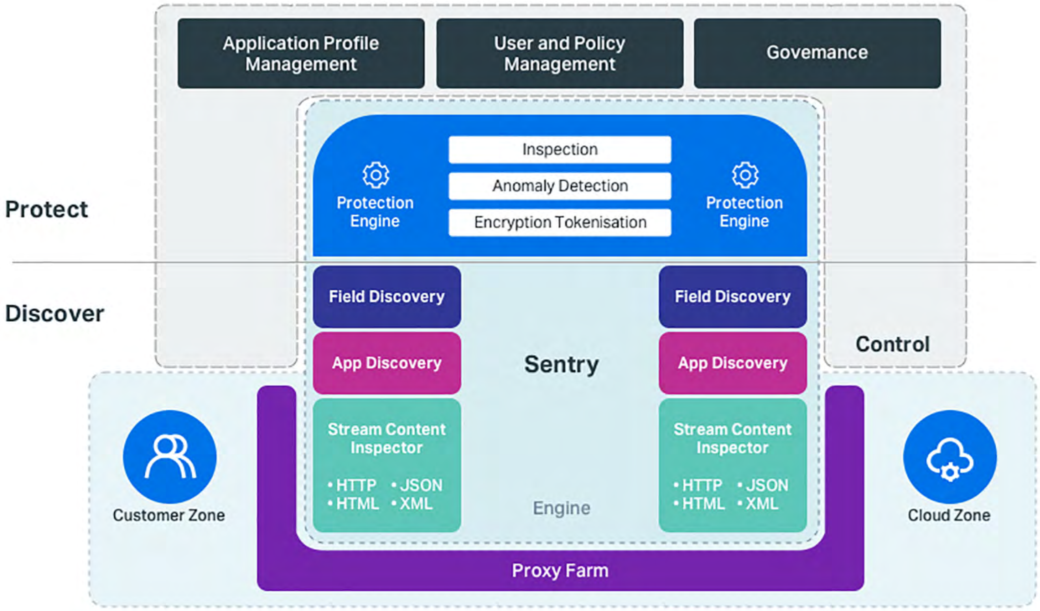


Figure 13. Data Flow in Voltage SecureData Sentry

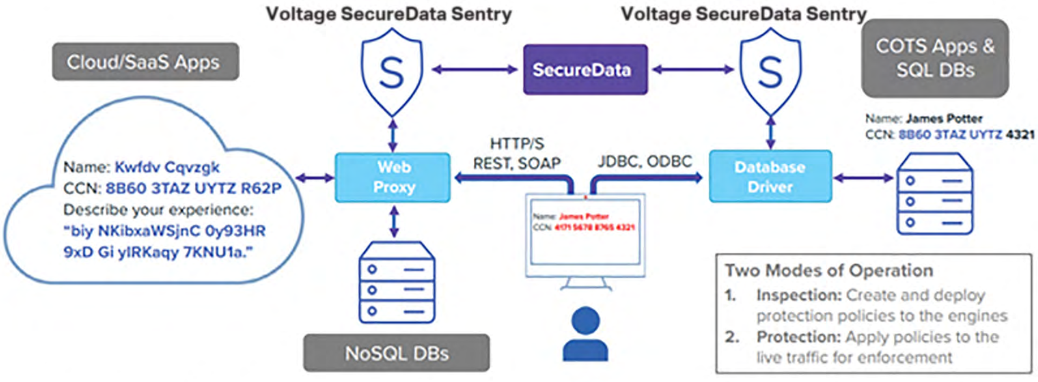
Voltage SecureData Sentry can also be used to mask data on access. The flexibility of protection flows makes it possible for Voltage SecureData Sentry to protect/mask data on access instead of decrypting them. For example, users accessing an application from abroad are not allowed to access sensitive data. When the traffic for these users is routed through Voltage SecureData Sentry, it can discover sensitive fields in the responses and protect them. The data itself is stored in the clear.

Voltage SecureData Sentry examines HTTP and HTTPS traffic between a user and a remote server for data requiring protection. This is a common scenario for protecting data sent to cloud applications and custom or on-premises web applications. Typically, a web browser or user's system prepares an HTTP request to a web application. The request is passed through an ICAP proxy to the Voltage SecureData Sentry Engine.

Alternatively, proxy chaining can be used to forward the requests to the Voltage SecureData Sentry Engine. In this case, the external proxy is forwarding requests and responses of the protected application to a parent proxy with ICAP support. The parent proxy is forwarding the requests to the Voltage SecureData Sentry Engine.

The Voltage SecureData Sentry Engine uses the headers and content in the request to decide if and how protection of the request should occur. Individual data fields in the request can be protected, such as replacing a piece of personal information with its encrypted equivalent. A complete request with protected fields is forwarded to the original proxies and then to the target web application.

Likewise, a web application will send a response back to the user and will also be directed through the proxies and presented to the Voltage SecureData Sentry Engine for analysis. The headers and content of the response are analyzed and can be protected, usually with different properties than the original request. There might also be encrypted pieces of data in the response that can now be decrypted. This is highly customizable to ensure that the desired security is maintained. A complete response with decrypted or otherwise modified fields in it will be generated and finally forwarded on through the original proxies to the end user.


Voltage SecureData Sentry
Voltage SecureData Sentry
Cloud/SaaS Apps
S
SecureData
S
COTS Apps & SQL DBs
Name: James Potter
CCN: 8B60 3TAZ UYTZ 4321
Name: Kwfdv Cqvzgk
CCN: 8B60 3TAZ UYTZ R62P
Describe your experience:
"biy NKibxaWSjnC 0y93HR 9xD Gi yIRKaqy 7KNU1a."
Web Proxy
HTTP/S
REST, SOAP
JDBC, ODBC
Database Driver
Name: James Potter
CCN: 4171 5678 8765 4321
NoSQL DBs
Two Modes of Operation
1. Inspection: Create and deploy protection policies to the engines
2. Protection: Apply policies to the live traffic for enforcement

Voltage SecureData Sentry consistent and transparent data protection, on premises and in the cloud.

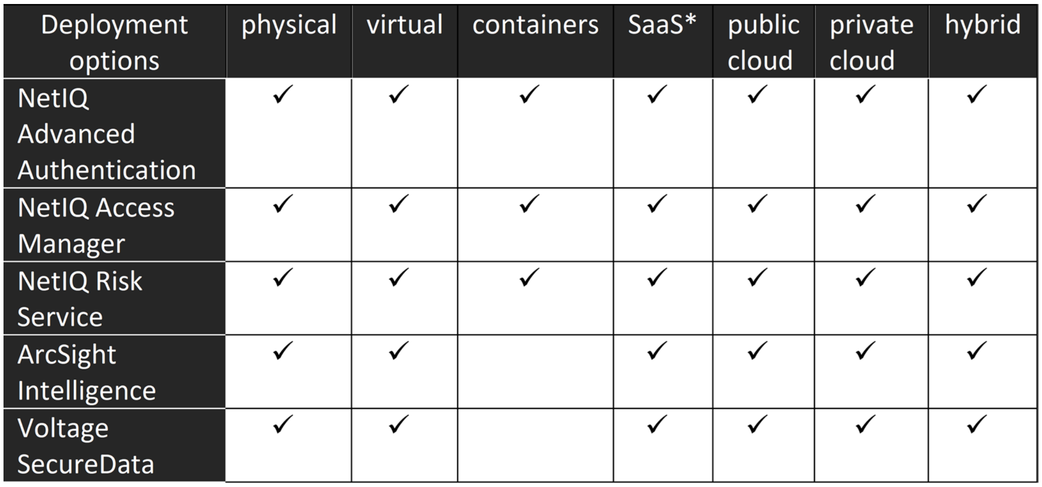
Figure 14. Hybrid application data protection at the edge

The data inserted and retrieved from SQL databases can also be analyzed and protected through Voltage SecureData Sentry. This occurs with the help of a custom driver, available for JDBC and ODBC. The custom driver is responsible for forwarding queries and related parameters to the Voltage SecureData Sentry Engine. Depending on the profiles active at the Voltage SecureData Sentry Engine, the queries and parameters are analyzed and protected—for example, encrypting the data values that will be input to the database. Modified queries and parameters are returned to the driver again, which can combine them into new database calls that deliver protected data to the database.

The reverse is possible for retrieving values from a database. Values can be forwarded to Voltage SecureData Sentry to be protected again, which would usually decrypt them. The decrypted values are then ready to be presented back to the user.

Flexible Deployment Options

While we expect teaming arrangements and mission priorities to dictate which options are best suited for deployment, rest assured that OpenText provides the broadest range of technology options available to ensure successful mission outcomes.



Deployment options	physical	virtual	containers	SaaS*	public cloud	private cloud	hybrid
NetIQ Advanced Authentication	✓	✓	✓	✓	✓	✓	✓
NetIQ Access Manager	✓	✓	✓	✓	✓	✓	✓
NetIQ Risk Service	✓	✓	✓	✓	✓	✓	✓
ArcSight Intelligence	✓	✓		✓	✓	✓	✓
Voltage SecureData	✓	✓		✓	✓	✓	✓

Figure 15. Deployment Options to Fit the Mission

Shared Zero Trust Services at the Edge

OpenText Application Security Services can not only help third-party SD-WAN solutions meet your environment requirements, but also accelerate the maturity of both the selected SD-WAN solution and your environment more broadly through these shared zero trust services offerings:

- Dynamic multi-factor authentication service: 30+ MFA methods, step-up authentication.
- Continuous risk analytics service: Combined attributes and behaviors risk policies.
- Advanced entity behavior analytics service: MITRE ATT&CK and EDR threat analytics.
- Application and API security portal: User self-service, single sign-on, central management.
- Application data protection service: Prevents sensitive data leaks, detects and protects field-level data.
- Share key access intelligence data with security operations: Risk dashboards, access data feeds, and priority threat alerting.

Summary of Key Benefits

OpenText Application Security Services is an integrated set of product offerings designed to address zero trust at the edge and presents an opportunity to quickly advance the maturity of your environment by delivering advanced enterprise application security capabilities to the edge and beyond.

Here are the unique benefits that these Services provide:

- Apply the most advanced risk analytics to continuous access decisions.
- Enable key zero trust services for user applications and data at the edge.
- Accelerate ZTA maturity with advanced threat detection capabilities (i.e., initial access, privilege escalation, lateral movement, and other TTPs).
- Detect and protect sensitive data end-to-end.
- Legacy application integration path.
- Most flexible hybrid deployment options with proven scalability.
- Lowest risk and cost associated with integrating the application security stack; a single vendor with the broadest set of zero trust capabilities.
- Well-established and trusted software manufacturer for US Government organizations with past performance and government references.
- Zero trust subject matter expertise, experienced engineers in government, and a well-established partner ecosystem.

OpenText Government Solutions welcomes the opportunity to join your zero trust team and actively contribute to achieving mission objectives as quickly as possible to expedite a smooth transition to ZTA and more effective security operations.

About NetIQ by OpenText

OpenText has completed the purchase of Micro Focus, including CyberRes. Our combined expertise expands our security offerings to help customers protect sensitive information by automating privilege and access control to ensure appropriate access to applications, data, and resources. NetIQ Identity and Access Management is part of OpenText Cybersecurity, which provides comprehensive security solutions for companies and partners of all sizes.

Connect with Us
www.opentext.com

OpenText Government Solutions
Rockville Office
One Irvington Center
700 King Farm Boulevard
Suite 125
Rockville, MD 20850-5736
USA
Tel: +1-301-838-5000

Additional contact information and office locations:
www.microfocusgov.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

762-000088-002 | O | 11/23 | © 2023 Open Text