opentext™ | Cybersecurity

Brochure

NetIQ as a Service

SaaS-Delivered Identity and Access Management

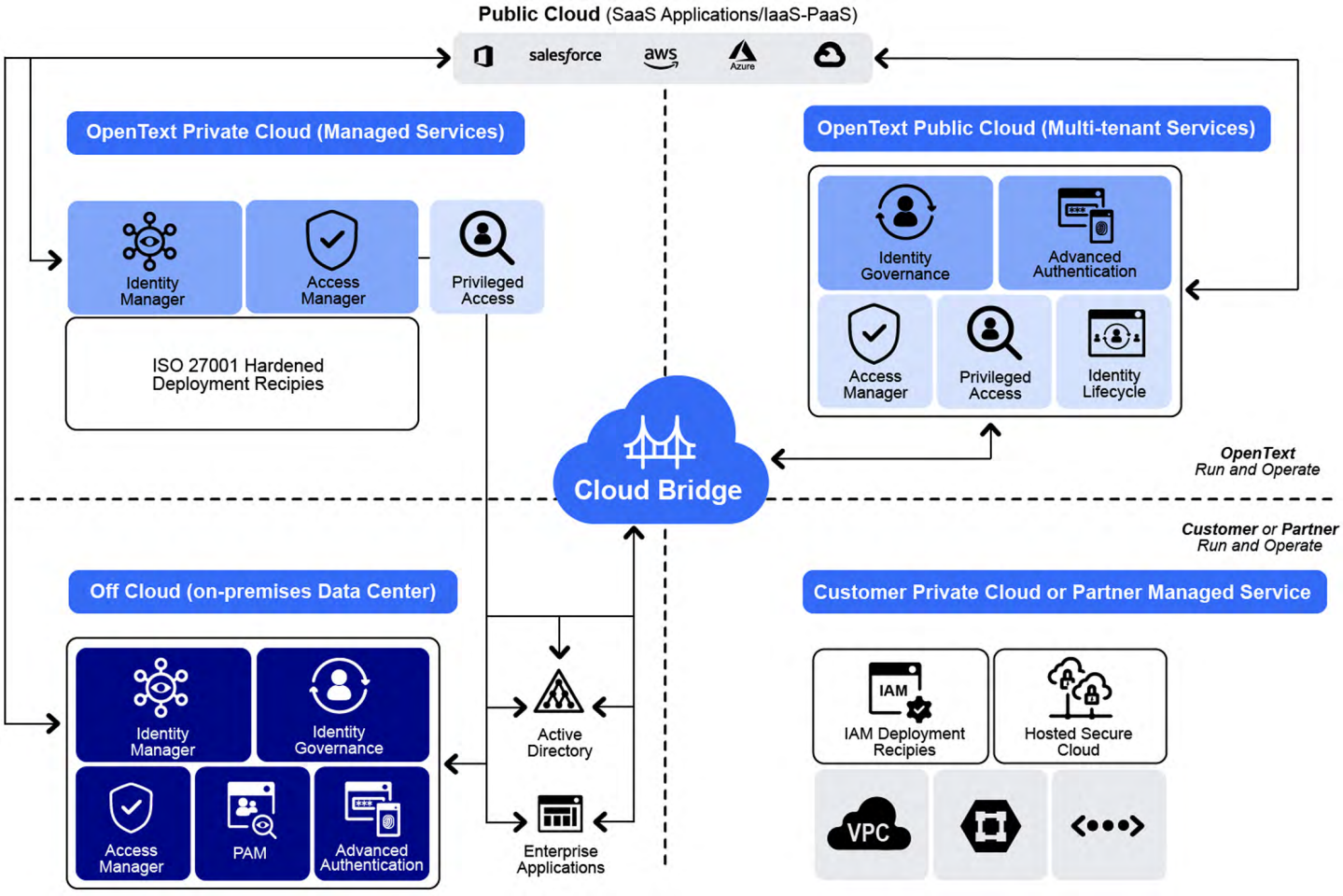
Cloud-Based IAM Solutions Are Not Created Equal. Some Force You to Live with Compromises and Limitations, Especially Organizations with Complex Environments.

As with most everything, there is no single approach to achieving identity-enabled digital services that successfully allow users to engage freely and securely. Each organization has its own application and configuration and cultural requirements that make them unique. The more established the organization, the more likely they are to have specific needs requiring them to keep a set of heritage core services. So, while some organizations can run their business on a platform of pure SaaS offerings, several years of IT investments or business acquisitions push many organizations into a mix of traditional, cloud-based microservices, and SaaS-based digital resources.

Beyond securing a core of services, some organizations see their IT prowess as a competitive differentiator and invest to raise productivity and consumer engagement. This best of breed mentality frequently results in heterogeneous and often complex digital environments.

NetIQ for All Your Digital Models

Because each organization is unique and changing, NetIQ by OpenText™ offers multiple options for implementing its platform. Let's first take a quick look at the different types of IAM products and services NetIQ offers and the environments that they enable.



Cloud Bridge Enables Hybrid IAM

NetIQ's Identity and Access Management (IAM) by OpenText™ offering is unique in that regardless of an organization's digital services model, they can benefit from its full functionality. While competing solutions have different categories of capabilities, NetIQ delivers an identity platform that is equally capable across an organization's data and services model. It is a model that evolves over time and might not be congruent across different divisions and departments.

NetIQ can offer this flexibility through our Cloud Bridge solution. It serves as the focal point for delivering secure communication between the NetIQ by OpenText™ services and the entities that access it through data centers, cloud (public and private), or a variety of identity providers. Cloud Bridge enables the same type of advanced capabilities offered by traditional IAM solutions. It allows the platform to continue to be configured and extended to solve uniquely specific requirements. They can run within the customer's internal environment or be part of a cloud-based service. They are often the preferred form factor for organizations that have IAM expertise and want the flexibility to customize it to their specific requirements.

To reduce platform maintenance overhead, customers might choose to place these products on an IaaS such as AWS. Most of the NetIQ portfolio offers a Docker Container option that not only allows automated Kubernetes management, but also in-cloud configurations.

The NetIQ SaaS Offerings

NetIQ IGA's analytics and real-time responses enable organizations to provide the right level of access. It supports a diverse set of environments and is built on a solid identity foundation. NetIQ IGA by OpenText™ excels in large, complex, and hybrid environments.

NetIQ Advanced Authentication by OpenText™ provides password-less authentication technology that gives you the flexibility to implement low friction and multi-factor authentication. Its standards-based framework enables you to consolidate all your authentication silos into a single set of policies.

NetIQ Identity Governance SaaS

NetIQ Identity Governance SaaS by OpenText™ helps any organization take their risk policies to a higher level of security and productivity. It helps you achieve your compliance goals through automated compliance checks and reporting. Built to get organizations up and running in hours versus weeks or months, NetIQ Identity Governance replaces error-prone, time-consuming manual methods that expose your organization to compliance violations and risk from excessive access. NetIQ Identity Governance by OpenText™ helps you quickly identify and revoke access to resources that users don't need—such as when users change positions in a company and inadvertently accrue too many privileges. NetIQ Identity Governance collects user entitlement information across multiple systems, applications, and data into a consolidated view. These capabilities provide easy-to-understand reports for LOB managers to validate whether existing employee access privileges are appropriate and initiate immediate action to revoke any access, if necessary. NetIQ Identity Governance enables you to:

- Collect and review entitlement data across the infrastructure, including on-premises, hybrid, and cloud applications, giving you accurate visibility into who has access to what resources.
- Leverage analytics and role mining to identify commonalities in entitlements, perform "what if" analysis, and produce compliance metrics and reports.
- Conduct access certifications with campaigns that stay on schedule through automatic reminders and progress updates, including decision support for approvers and issue escalation for administrators.
- Define controls to detect and handle violations and exceptions such as SOD violations or orphaned accounts to reduce risk.
- Set business-based role and attribute authorization models to reduce the scope and duration of access certifications and access request and approval processes. This enables a focus on exceptions, ather than all entitlements.
- Close the loop on remediation, including integration with service desk solutions such as ServiceNow or Remedy for automated ticketing, or automated fulfillment via integration with Identity Manager.
- Conduct reviews prioritized by risk scoring based on attribute value, group membership, management relationship, application, permission, cost, risk, and other criteria, providing focus where it's most needed.
- Report on identity governance with out-of-the-box support for scheduling and distribution that includes entitlements, certification status, request and approvals, and policy violations to make audit reporting easier.

NetIQ Identity Governance's real-time adaptive governance enables continuous risk reduction. While competitive solutions can collect entitlements at a point in time, it still leaves organizations blind to risk until the next collection. NetIQ Identity Governance fills this void by adapting to changes and events as they happen and can trigger a review as needed to ensure compliance. These cost and risk insights inform busy approvers with business-level information that make it easy to consistently make the right entitlement decisions.

NetIQ Advanced Authentication is also an intelligent and adaptive piece of technology. It can use a person's phone to leverage location information to control the type of authentication that provides the targeted level of convenience and security. It also includes other commonly used metrics to step up authentication to the type you define, based on the measured risk.

NetIQ Advanced Authentication SaaS

NetIQ offers Advanced Authentication (with or without the Risk Service) and Identity Governance as a full service. The Risk Service's behavioral analytics plug-in, based on Interset technology, is delivered as a service. Customers need only to provide credentials and the license key to enable the service, with no configuration or maintenance needed.

With a consolidated MFA approach, NetIQ Advanced Authentication is less complex to configure and maintain than other solutions. Our strength also lies in out-of-the box integrations that provide a wealth of configurable authentication options. Your entire organization benefits from the increased security and usability.

You also have the freedom to build new or replace and consolidate MFA infrastructures, enabling your organization to control costs and maximize investments. CTOs and architects have long understood the benefits of open standards. The intrinsic interoperability offers application and platform independence, as well as long-term architecture integrity. However, when an organization implements an authentication solution built on proprietary protocols, they no longer have the freedom to shop across the industry for the devices that best fit their needs at the best price. They are also subject to vendor lock-in.

NetIQ is a member and strong supporter of the FIDO (Fast Identity Online) Alliance. FIDO U2F (Universal 2nd Factor) enables organizations to support an environment where users manage their own authentication devices. NetIQ Advanced Authentication provides a solid 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 a higher level of security across other aspects of their digital life increasing their overall security posture.

IT groups should be cautious about selecting solutions that offer minimal support for today's modern authentication standards. Beyond the authentication types available in RADIUS, NetIQ Advanced Authentication offers more native methods than any other solution on the market. That matters 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 more), NetIQ Advanced Authentication offers wide applicability for your environment. In addition, the framework's broad support for a variety of authentication readers and methods provides the best option for flexibility. It provides the broadest set of native integrations found in the market and it's standards based approach protects you against vendor lock in.

NetIQ Access Manager

NetIQ Access Manager by OpenText™ is a leading provider of web single sign-on solutions for your users. It is 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 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 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 organizations that they choose to interact with, as well as the ability to self-help and administer whenever they find it convenient. If you are an organization that needs a higher level of security, NetIQ Access Manager enables you to preserve user convenience while enforcing security to match your risk.

NetIQ Identity Manager

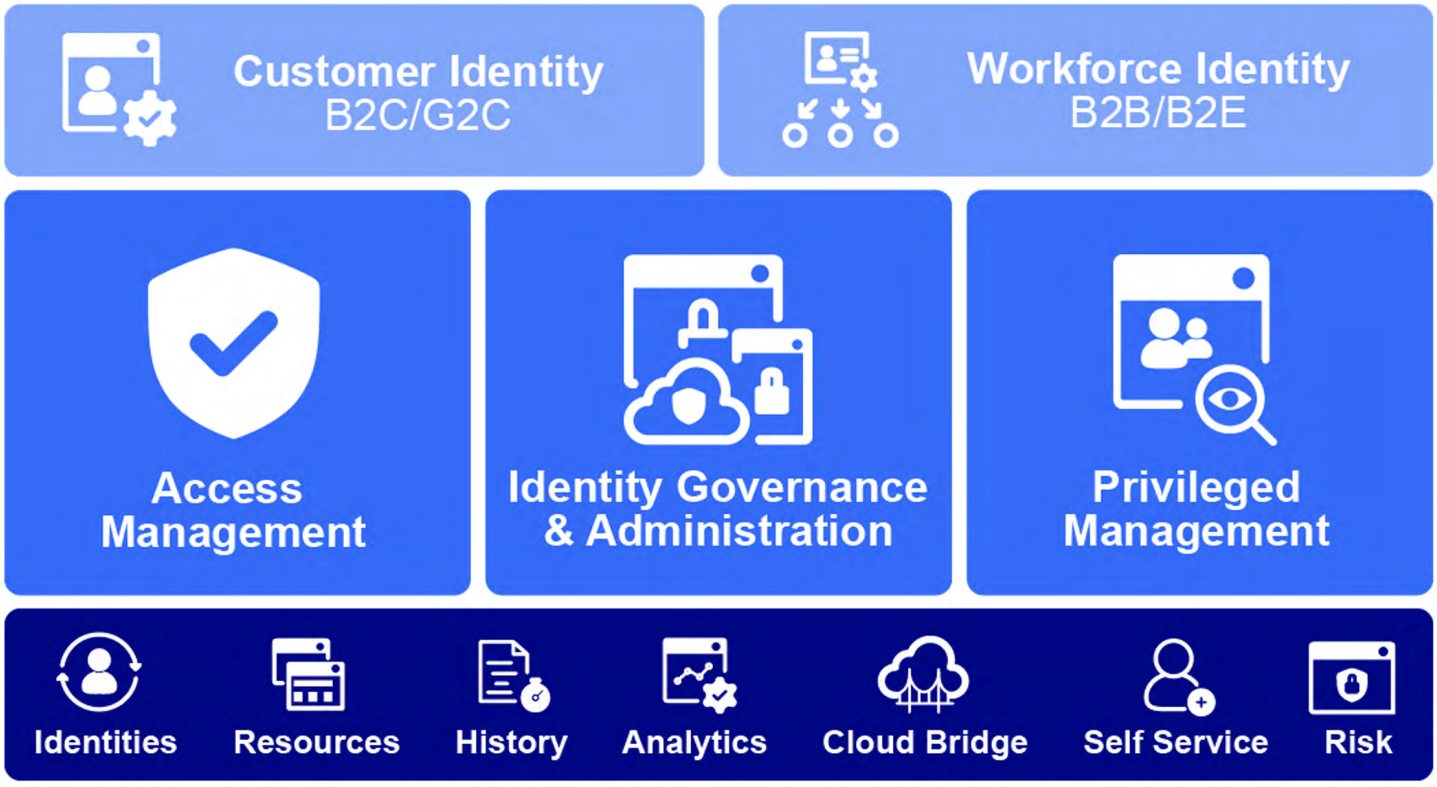
NetIQ Identity Manager by OpenText™ powers the entire identity management lifecycle by managing identities and their associated attributes to minimize privileges. This enables your organization to reduce the costs of manual account management and demonstrate compliance, while reducing the risk of unauthorized 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, deprovisioning, 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 reports needed to satisfy audit or compliance requirements.

NetIQ Privileged Account Manager

Beyond managing access for the general user base, there is a critical need to extend this type of control to the underlying systems that host that information. NetIQ Privileged Account Manager by OpenText™ fills that need by focusing on privileged access to systems and data sources across the organization. Often, the most damaging breaches are the ones that leverage privileged accounts.

NetIQ Privileged Account Manager provides the specialized level of monitoring and control needed to protect superuser access to the most sensitive information. Not only does it offer a deeper level of monitoring, but also in-depth forensic data.



NetIQ SaaS Practices and Processes

NetIQ secures organizations with SaaS-delivered identity and access management for workforce and customer identities. It maintains a current catalog of all resources that need to be protected and added intelligence to help ensure the right level of access to them. It also offers a robust authentication framework designed for your entire organization. NetIQ is committed to excellence in delivering these services to you.

Data Handling

OpenText employs a multi-tier, multi-datacenter data-ingestion pipeline to process data securely through network devices that can process data from multiple inputs. The data does not leave the NetIQ services and is only accessed through the application by a properly credentialed and entitled user.

The OpenText Services Platform

The NetIQ SaaS offering runs on Amazon Web Services (AWS). Cloud security is one of AWS's highest priorities. To do this, OpenText leverages AWS's infrastructure to implement strong safeguards to help protect customer privacy. All data is stored in highly secure AWS data centers, from which all the data center related portions of our compliance profiles have been completed. This allows us to maintain the highest standard of security. OpenText leverages the platform's elasticity and security design to ensure security with scaling. No matter the size of the customer, the AWS infrastructure is designed to keep data safe.

One of the key features of AWS is that it enables us to implement business continuity with replication between applications and data across multiple data centers in the same region, using availability zones. While doing so, OpenText retains complete control and ownership over the region in which our data is physically located, making it easy to meet regional compliance and data residency requirements.

To increase privacy and control network access, OpenText leverages AWS to provide security capabilities and services:

- Network firewalls built into Amazon VPC and web application firewall capabilities in AWS WAF enable us to create private networks and control access to instances and applications.
- Encryption in transit with TLS across all services.

Availability of NetIQ services is of paramount importance. As such, the OpenText team leverages services and technologies built into AWS from the ground up, to provide better resilience in the face of DDoS attacks. The team leverages the platform's ability to provide a defense-in-depth strategy to thwart attacks and use a range of tools that enable us to move quickly while still ensuring that our cloud services comply with OpenText's standards and best practices.

Compliance

Hosting our SaaS infrastructure on AWS creates a shared responsibility model between OpenText and AWS. This shared model reduces our operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer, down to the physical security of the facilities in which the services operate.

Because the AWS cloud infrastructure comes with so many built-in security features, the OpenText team focuses on the security of the NetIQ environment (including updates and security patches), as well as configuration of AWS-provided security features such as configuring and interacting with the Cloud Bridge.

Security and Risk Management

We have just reviewed in detail the OpenText compliance programs. These programs use standardized compliance profiles because these are the ways that the industry has developed to express assurances around software-based services. These NetIQ services are:

- ISO 27001:2013 certified. ISO 27001:2013 demonstrates implementation and maintenance for the highest security standards controls, assuring secure delivery of NetIQ SaaS offerings.
- ISO 27034-1 certified. ISO 27034-1 application security standard demonstrates proactive integration of security as part of the NetIQ product development lifecycle.

Security and Risk Management of NetIQ Services

The OpenText team reviews in detail the relevant compliance programs. These programs use standardized compliance profiles to achieve assurances around software-based services. These compliance profiles require a certain amount of formality and rigor around how OpenText develops and deploys its solutions and operationally runs the service. Behind this formality, OpenText has taken specific actions in the delivery of our services to fulfill these requirements. The following sections describe, in "non-formal terms," some of the actions the OpenText SaaS team takes to ensure the following:

- Systems are designed with security capabilities. They will withstand security attacks of several forms, from denial of service to vulnerability exploits to malware.
- As services are configured for a specific customer, the SaaS team builds them with professional, documented processes. Important decisions are made carefully and are documented.
- Explicit privacy of customer data is of the utmost importance and in no case will OpenText lose focus of their stewardship of it.
- The NetIQ offerings are configured for high availability. Speed and resilience is essential, so customers can count on using them when they need them. If there are unforeseen problems such as hardware or network failures, our platform team will respond and take actions to maintain identity and access capability.
- The OpenText SaaS team is of the highest integrity; everyone knows their job and knows how to expedite processes through the company as needed to deliver our services.
- The OpenText SaaS team regularly monitors and tests their systems against attacks and poor performance and to make sure preventative mechanisms are working.

Secure Software Design Lifecycle

The Security Development Lifecycle (SDL) is a security assurance process focused on software development. As a company-wide initiative and a mandatory policy, we "design in" security from the start. On the NetIQ team, the SDL is based on three core concepts: education, continuous process improvement, and accountability.

OpenText conducts penetration tests for all of its SaaS-enabled offerings. The assessment findings are remediated according to our SDLC program SLA's, critical findings are mitigated immediately, and a patch is released. In addition, the team conducts automatic scans with an internal platform called STAT.

STAT is an Automatic Security Testing platform for Agile and DEVOPS, used daily to automatically scan source code and apps and to intercept new vulnerabilities in a near-real-time manner.

The following tools are part of these scans: WebInspect, OWASP Dependency, Checker, CoreOS Clair, Fortify, and Nessus.

Access Management

Access control to the NetIQ platform is a core security measure and as such must be controlled and enforced by policy. OpenText services invoke specific processes to prevent excessive admin rights and to limit the number of administrators whose access was approved by management.

Account owners hold the root access key and that has a security impact that we take under consideration:

- Changes to accounts are monitored and reviewed.
- The number of accounts is minimal and constantly reviewed to detect orphan accounts.
- The average time to disable account upon termination.

In the context of being identity and access management experts, OpenText uses specialized cloud management tools to manage access to accounts and delegate permissions, in a way that account owners are able to manage all access.

- Account admin delegation is monitored and an alert is provided whenever a user is granted admin access.
- Any request for account admin delegation is approved by our SaaS security officer.

We create multiple AWS accounts for our organization's separate accounts—for example, production resources and backup resources. This separation enables us to cleanly separate different types of resources and provide excellent security benefits.

User Access Review Procedure

The OpenText team conducts periodic reviews for access management to ensure that necessary personnel have access to essential systems and unauthorized employees (or miscreants) do not. The process includes the following:

- Manager Reviews of Employee Profiles
- Review Employee Termination Procedures
- Automate Reviews and Compliance
- Review Administrative Groups Members
- Review Profiles with Password Never Expire

Penetration and Vulnerability Testing

A penetration test (or pen test) is a set of procedures designed to bypass the security controls of a system in order to test that system's resistance to attacks. The NetIQ SaaS offering is considered highly critical and every major release is tested. An operational penetration test is performed annually, as the infrastructure rarely changes. Vulnerability scans are conducted monthly against our internet-facing assets and the findings are remediated according to our patch management program. The OpenText NOC team monitors the remediation process and ensures that patching SLAs are met. Emergency updates are performed as soon as possible after ensuring patch stability. These updates are only applied if they fix an existing problem that the server is experiencing.

Critical updates are applied during off hours within a seven-day timeframe, after ensuring patch stability and an emergency CAB. Non-critical updates on non-critical systems are performed on regularly scheduled maintenance windows within a two-month period.

Platform Security Checks

The OpenText team uses an application that draws upon best practices learned from aggregated operational history of serving hundreds of thousands of AWS customers. This technology inspects our NetIQ environment and makes recommendations for improving system performance and closing security gaps. It checks for:

- Security groups that have rules that allow unrestricted access (0.0.0.0/0) to specific ports or to a resource.
- Unrestricted access, which increases opportunities for malicious activity (hacking, denial of-service attacks, and loss of data). The ports with the highest risk are flagged red and those with less risk are flagged yellow.
- Ports flagged green, which are typically used by applications that require unrestricted access, such as HTTP and SMTP.
- Use of AWS IAM, the root account, and warns if MFA is not enabled.
- Open access permissions that grant upload/delete access to everyone, which creates potential security vulnerabilities by allowing anyone to add, modify, or remove items.
- The password policy for admin accounts and warns when a password policy is not enabled or if password content requirements have not been enabled.

Data Encryption

NetIQ SaaS security involves techniques for protecting sensitive data stored within the services:

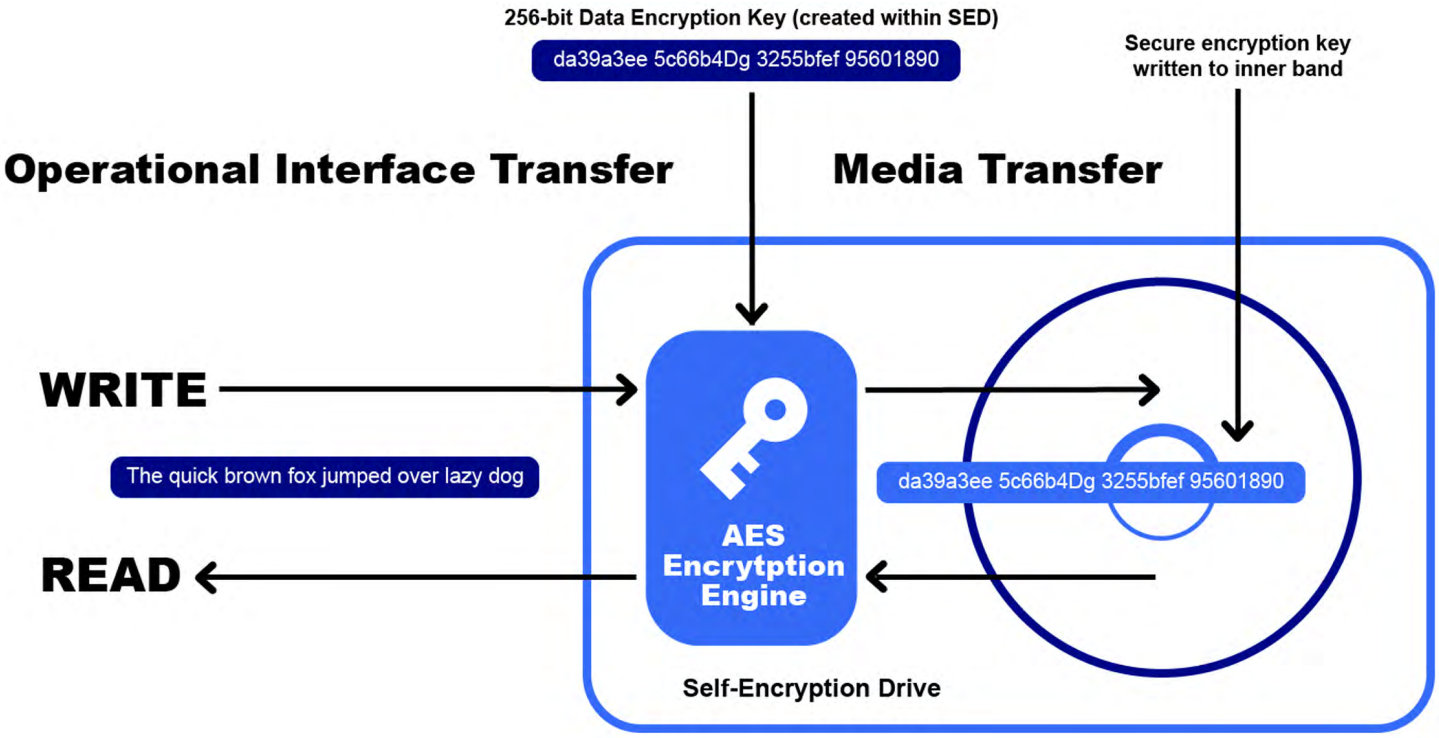
- Define approved cryptography.
- Define encryption architecture and insecure protocols guidelines.
- Data in transit encryption.
- Data at rest encryption.

Data Encryption for Both Transit and Rest

OpenText uses TLS1.2 for data in transit encryption (browsers) and HPE 3PAR devices for storage. All data written to each FIPS 1402 disk uses Full Data Encryption. All data encryption is handled at the drive level and no external software or hardware is needed to encrypt data. The benefits from Full Data Encryption are:

- Government Standard-based encryption—industry-wide standard.
- Uses AES-256.
- Dedicated engine for full speed encryption contained on every drive.
- Encryption key is unique and protected on the media.
- Encryption key itself is encrypted and stored on the media.

On SED drives, data is always encrypted on the storage medium; no license is necessary. Enabling encryption on the array protects the SED drives from any malicious intent by locking the disks to the array in which encryption is enabled. Per industry-wide standards, the same array encryption-locking key is used for all disks within the same encrypted storage array.



OpenText leverages AWS's server-side encryption, which encrypts data on our behalf "after" the API call is received by the service, leveraging AWS KMS. Amazon S3 or EBS supports server-side encryption (SSE) of user data. Server-side encryption is transparent to us. Our database uses EBS storage, so all database storage is encrypted in this way. AWS generates a unique encryption key for each object and then encrypts the object using AES-256. The encryption key itself is then encrypted, using AES-256-with a master key that is stored in a secure location. The master key is rotated on a regular basis.

Logging and Monitoring

Logging and monitoring are key components in security and operational best practices, as well as requirements for industry and regulatory compliance. Understanding the changes made to our resources is a critical component of IT governance and security. It is equally important to prevent changes and unauthorized access to the log data.

OpenText records AWS API calls made on our account and delivers log files to an Amazon S3 bucket that is specified. It records important information about each API call, including the name of the API, the identity of the caller, the time of the API call, the request parameters, and the response elements returned by the AWS service. This information helps us to track changes made to our AWS resources and to troubleshoot operational issues.

Near-real-time alerts to misconfigurations of logs detailing API calls or resource changes is critically important for effective IT governance and adherence to internal and external compliance requirements. Because it's imperative that logging is configured properly to oversee the activities of administrators and resources, OpenText technology is used for log management and monitored by the Security Operation Center team.

Network Zero Trust Practices

Network architecture consists of separate VPCs for management and other services. OpenText uses IPS to prevent attacks on the network, as well as periodic vulnerability scans:

- FWs performing deep packet inspection, TCP session state and anti-spoofing.
- Managed dedicated active directory with strict group policy.
- Patch management process is in place to ensure all components are up to date.
- In transit and at rest encryption for client data.
- TLS version 1.2.
- Malware detection agent is installed on all servers and workstations.
- Backups for both data and configurations.
- SOC team monitors incidents and keeps track of service availability.

The Intrusion prevention system detects and blocks brute force and spoofing attacks. System configurations consist of:

- The effectiveness of this system is being tested annually based on attack history.
- IPS is being updated constantly for new attacks signatures.

Incident Management

OpenText's incident response leverages AWS's wealth of information in the form of logs and metrics to quickly identify potential security incidents. To isolate any security events, response to any indication of compromise includes modifying security groups attached to that instance. The security team can take this one step further by creating a new subnet to isolate the concern while they do further investigation of the potential threat source, vulnerability of the configuration, or other potential risks. OpenText's incident response strategy includes the following phases: anticipate, deter, detect, respond, and recover.

OpenText has also defined incident response and notification processes to meet contractual requirements and applicable regulations. Once an incident has been detected and the CSM notified, the SOC team provides an update to the CSM every 12 hours, or as soon as new information is available, until the incident has been resolved. A root cause analysis is sent to the customer within five business days of resolution. This program is audited annually as part of the ISO27001 certification.

Business Continuity & Disaster Recovery

Business Continuity (BC) ensures that the organization's critical business functions continue to operate or recover quickly in case of an incident; it might also be referred to as High Availability (HA). OpenText has multiple data centers around the globe, so our BCP relay on data and configuration backs up to a remote location. The operational teams follow a program that tests and validates these backups.

Conclusion

Despite the trend of organizations moving their IAM services to a SaaS model, their needs haven't diminished or simplified. In fact, digital transformation has increased dependencies on a solid IAM infrastructure. At the same time, their increasingly complex environment imposes unique requirements onto IT and security teams. NetIQ's SaaS design allows organizations to secure more with fewer compromises.

To learn more, check out NetIQ's website.

Connect with Us

www.opentext.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.

763-000012-002 | O | 11/23 |