Illuminate Security Overview

Table of Contents

4Q2021

I. Introduction

N2N Services delivers a scalable cloud computing solution called *Illuminate* designed to provide turnkey APIs that allow institutions to connect new SaaS products at an affordable cost in the matter of days instead of weeks. N2N Services has architected our solutions to deliver a reliable and secure system to support the needs of your students and staff. N2N Services prioritizes the importance of safeguarding the integrity and availability of your data, and as such has built *Illuminate* from the ground up with security in mind, encompassing the utilization of hardened commercial data centers, a three-tiered application architecture and data encryption throughout the entire system. To deliver that protection, N2N employs information security practices that meet or exceed industry standard security and privacy protocols as detailed herein. N2N Services undergoes annual external evaluations of its infrastructure and practices, and has an AICPA SOC2 Type II attestation from Marcum LLP, most recently issued June, 30, 2021.

II. Physical Security

N2N Services hosts *Illuminate* in the Amazon Web Services (AWS) data center environment, designed to provide the highest level of secure services. Amazon creates an infrastructure that allows the most demanding applications to be built on top of this service, using a shared responsibility model. See https://d1.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf for information on AWS physical security. N2N Services' office at 3063 Peachtree Industrial Blvd. is always locked on the ground floor (developers and technical staff); reception and administration are on the 2nd floor which is also locked during business hours.

III. Infrastructure Security

N2N Services's network security deployment includes the use of a number of industry leading tools and services to secure the underlying infrastructure and protect against the introduction of security vulnerabilities. N2N Services uses AWS to compartmentalize, contain and protect its server resources, with a VPN connection to the server environment required for access.

We utilize AWS tools and host-based logging for monitoring access and events. Among these tools and services are solutions to detect, correlate, and identify atypical activity recorded in log data from servers and networks. Vulnerability scanning at the hardware, network, and application layer is one tool to identify and remediate potential weaknesses that can present opportunities for security breaches. N2N Services maintains its production infrastructure with a single point of ingress or egress for data, through an AWS Route 53 load-balancing environment. This provides a common point for activity monitoring and logging.

Inside Illuminate, N2N Services has also deployed Web application firewalls that provide enhanced security features including:

- ***Identification and access controls*** that decrypt and inspect SSL/HTTPS traffic, inspect TCP handshakes, enforce protocol conformity, and detect attacks (Black List)
- ***Defensive actions*** that validate input (White List), block attacks, and block user sessions
- ***Activity monitoring practices*** that block data leaks (by masking confidential data, such as Social Security Numbers), perform application-level auditing, and track user activity in applications.

IV. Data Security

N2N Services maintains a high level of security designed around the protection and security of all client and partner data. The *Illuminate* application utilizes encryption to maintain the safety of transmitted data. All data within *Illuminate* is encrypted in transit to and from the *Illuminate* servers. All web traffic is encrypted with HTTP browser encryption (HTTPS) which encodes data so that only those with the encryption keys can decode the data. Certificate-based credentials identify the source and target servers before they can communicate with each other. Illuminate has implemented specific certificate trust to ensure that the communication between the Illuminate Dataport and the Illuminate cloud environment is not susceptible to man-in-the-middle (MITM) attacks. An additional layer of transport security is through optional AES encryption of request and response data headers and data packets before the stream is sent through the SSL/TLS tunnel.

Additionally, Illuminate logs API access, which enables monitoring of what data was accessed by whom. By maintaining this level of detailed log entries, the N2N Services Information Security team can proactively monitor for potential unauthorized data access attempts.

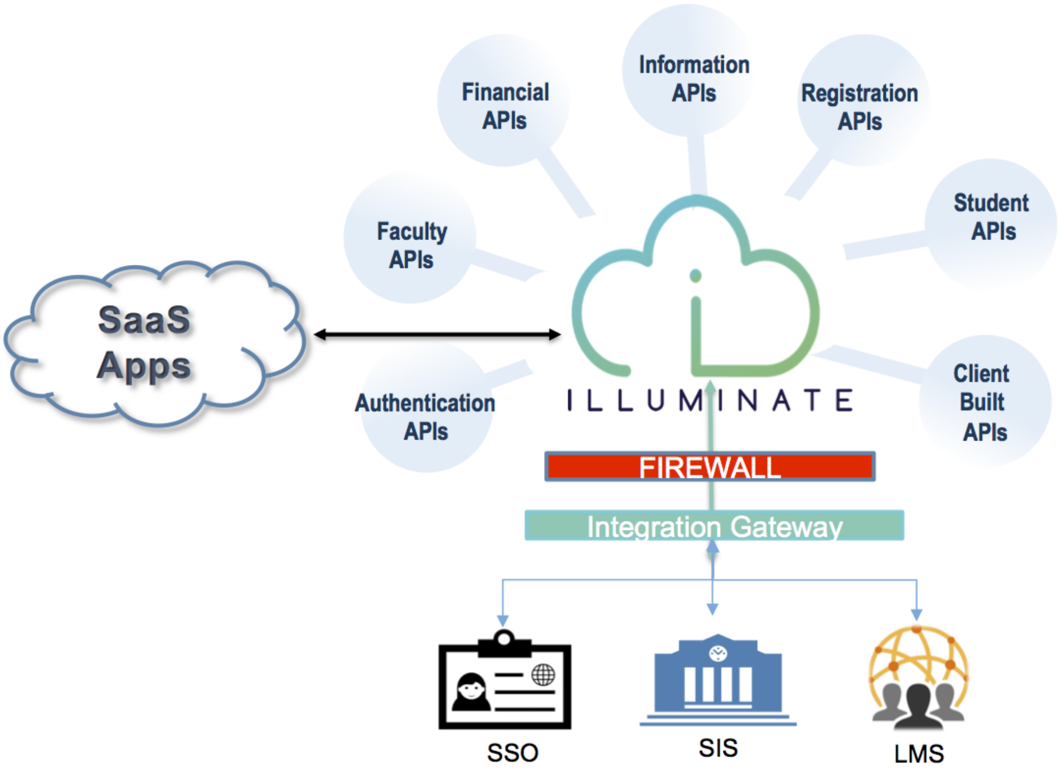
V. Security and Privacy Practices

N2N Services maintains a security program including policies/procedures, end-user workstation security, and Security Awareness Training (SAT). We run centrally managed anti-malware and anti-phishing software on our workstations, and we have a mandatory online Security Awareness Training (SAT) program. N2N Services' security and privacy policies and procedures are based on SANS templates, which are informed by common practices and frameworks, such as ISO and NIST. Awareness of N2N Services' security policies and procedures are a part of the responsibility of each employee. Each policy or procedure includes a compliance/accountability section. N2N Services performs background checks on all staff. When staff are onboarded, they are given basic access to common resources. N2N follows the principle of least access, providing access to staff on an as-needed as their duties require. Access audits for staff are performed at offboarding or upon major changes in staff responsibility. N2N Services' CISO and Operations Manager monitor compliance with security and privacy policy. Staff non-compliance is brought to an individual's manager for disciplinary action if required.

Illuminate is a transactional engine, and does not replicate data from source systems. *Illuminate* protects data as it moves between participating systems by using SSL-encrypted Web services with optional pre-injection AES encryption of the payload. N2N Services has a defined Security Incident Management process under the direction of its CISO, and well understands the responsibility of securely handling sensitive information. For example, N2N Services' executive leadership collectively has decades of experience at operational and cabinet level (VP, AVP, VC, AVC) in higher education and fully understands the nuances of FERPA and the responsibility of vendors and their software in achieving FERPA compliance. N2N does not handle PCI data in the *Illuminate* application or any of its other products. Data is normally logged using metadata. Any data stored for asynchronous transactions or error recovery is encrypted at rest in its database. N2N Services maintains a SOC2 attestation, and has annual external Web application security reviews and external penetration testing.

VI. Application Security

Architecture



N2N Services's *Illuminate* application utilizes a multi-tiered client-server architecture in which presentation, application processing and database functions are physically separated. This three-tier architecture enhances the level of security by limiting access to each layer to only authorized and approved entities. The Illuminate server deployment is scripted with Terraform and utilizes application containers to both encapsulate functionality and to ease the process of dynamic scalability or disaster recovery.

The *Illuminate* architecture uses application firewalls to further enhance our security approach. The application firewall layer employs multiple security features designed to protect application and client data including limiting access to server and applications to only authorized IP addresses. Any event that differs from baseline behavior triggers an alert to N2N Information Security personnel who monitor security alerts. N2N Information security personnel are trained to isolate suspicious data and correct any resulting atypical behavior.

In addition to the three tiered architecture, the web servers are protected by web application firewalls between the web servers and the internet. These firewalls block communication between Web application layers, which can reduce the vulnerability of Web applications to such attacks as SQL injection, cross-site scripting, and other types of attack.

Development Security

N2N Services understands that as important as infrastructure and physical security are, application development security is often more important. N2N Services uses an automated build and deployment process to validate code and to reduce human error in deployment to test or production servers. N2N Services' software development practices encourage the development of quality, secure software. Legacy products use a manually imposed development process leveraging dev/test, QA and Production tiers. Our current development is done with an automated build/deployment process using Jenkins. In addition, N2N Services employs an information security officer (CISO) whose role is to specifically focus on the overall security of the application and architecture of *Illuminate*.

N2N Services uses a secure source control and version control system that limits authorized access to only those requiring access during the development process. It also tracks all access and changes via audit and log files which are maintained and reviewed for security purposes. N2N Services also uses software solutions to perform security testing and vulnerability scanning of all new code prior to deployment to be sure that no vulnerabilities have been introduced.

Finally, N2N Services utilizes a rigid change control and testing process for each release of *Illuminate* that focuses on full system testing, individual unit testing, system integration testing, formal load testing, and formal use-case testing simulating common end-user actions.

In addition, all development work is done strictly in a dedicated development environment, once complete it is moved to a dedicated test environment. Once all testing is complete and the application is ready for production the development organization is required to get sign-off through N2N's Change Control Board. Once approval for the changes are logged, the changes are handed to a completely separate operations deployment team who puts the code into production. No changes are allowed in production unless they have gone through the previously defined process.

VII. Authentication

N2N Services provides two secure authentication methodologies to support our partner's utilization of the *Illuminate* application. Faculty, students, and staff using Illuminate-delivered applications can be authenticated via your campus' authentication solution, such as Active Directory, LDAP, or Shibboleth, or you may choose the *Illuminate* authentication process through your student information system (such as CAS for Banner). Where we cooperate with partners for authentication, we use JSON Web Tokens (JWT) for security assertions.

These authentication methodologies provide a reliable and robust mechanism for managing faculty, students, and staff credentials.

Illuminate internal user authentication is currently not SSO-enabled, but this is a roadmap item.

VIII. Conclusion

The N2N Services Illuminate solution has been architected from the ground up with a deep understanding and focus on protecting and securing our clients' and partners' data. From full end-to-end encryption to a multi-tiered architecture our solutions are designed to provide the highest level of confidence in our partner institutions.

Illuminate has been designed to enhance and improve the data integration process, giving you unprecedented abilities to granularly manage the way your data is exposed to other applications. The *Illuminate* platform both simplifies the data integration problem and enables you to connect more applications quickly and securely.

Illuminate Security Overview

All material in this document is, unless otherwise stated, the property of N2N Services. Copyright and other intellectual property laws protect these materials. Reproduction or retransmission of the materials, in whole or in part, in any manner, without the prior written consent of the copyright holder, is a violation of copyright law. Information in this document is provided for informational purposes only. It represents N2N Services' solution as of the date of publication and is subject to the evolving nature of security and N2N Services' solutions. The responsibilities and liabilities of N2N Services to its partners are governed by contractual agreements.

4Q2021