N-able N-central

Architecture and Security White Paper

N-ABLE™

Version: 1.0

Last Updated: Reviewed: 20 July 2026

Contents

Contents **2**

Executive Summary **6**

Introduction **7**

Purpose 7

Target Audience 7

Summary of Problem **8**

Problem Statement **9**

Proposed Approach **10**

Core Architecture **11**

Core Components 11

N-central Server 12

Agents and Probes (Classic) 12

Unified Agent (Modern Agent) 13

Unified Agent Communication Flow 13

N-able Ecoverse 14

How Ecoverse integrates into the N-central architecture 14

Cloud Microservices 14

Data flow and Communications 15

Typical Data Flow 15

Scalability 15

Secure Platform Architecture 16

Multi-Tenancy 16

Zero Trust Access Controls 17

Recommended exclusions for third-party AV software 17

Folders 17

Applications 17

Firewall 17

The Upgrade Process 18

Agent and Probe Upgrade 18

Software Upgrades for AV Defender 18

Key Security Features **19**

Secure Software Development Lifecycle (SDLC) 19

Access Control and Identity 19
Data Encryption 20
Vulnerability Detection 20
Network and Infrastructure Security 21
Disaster Recovery & Business Continuity (hosted only) 21
Security Profiles 21
Modern security profile 22
Compatibility security profile 22
Legacy security profile 23
Supported Compliance Standards 24
HIPAA Type 1 Compliance 24
ISO/IEC 27001:2013 Certification 24
SOC 2 Type II Attestation 24
GDPR and CCPA Support 24
Commitment to CMMC 2.0 Readiness 25
Integrations and Extensibility 26
API Capabilities and Custom Development 26
Integration with Leading ITSM Platforms 26
Flexibility to Connect with Other Enterprise Tools 26
Common Questions and Best Practices 26
Pendo UI Integration 27
Remote Control 29
Take Control 29
Ports 30
Remote Desktop 31
Other Remote Control Connections 31
Patch Management 33
Assess and Prioritize Patches 33
Deploy Patches Automatically 33
Manage Offline Patches 33
Monitor for missing patches 33
Compliance and Reporting 34
Security Integration 34

Manage Windows Updates ... 35
Windows update process flow ... 35
Direct patch data submission ... 36
Device Management for Apple ... 37
macOS security framework ... 37
Antivirus and Anti-malware ... 38
Upgrades and Updates ... 38
Product Upgrades (Major Releases) ... 38
Product Updates (Hot Fixes) ... 39
Definition File Updates (Security Signatures) ... 40
N-able Login ... 42
Centralized Single Sign-On Using Open Standards ... 42
Multi-Factor Authentication Enforcement ... 42
Federated Authentication with Microsoft Entra ID ... 42
Hardened Authentication Flows and Session Security ... 43
Compliance and Standards Alignment ... 43
Scheduled Tasks ... 44
Security Implications ... 45
Report Manager Integration ... 45
LDAP Integration ... 45
Other Security Features and Integrations ... 47
Cove Data Protection ... 47
Authorization (Access Control) ... 47
Secure communication ... 47
Encryption key/passphrase handling ... 47
Cyber resilience ... 48
Incident response ... 48
Immutable copies ... 48
Threat Modeling ... 48
Penetration Testing ... 48
Endpoint Detection and Response ... 48
Key capabilities ... 49
Analytics ... 50

How Analytics Handles Data 50
Data Collection 51
Data Synchronization 51
Data Processing and Storage 52
Visualization and Reporting 52
Security Architecture 52
Data Protection in Transit 52
Data Protection at Rest 52
Multi-Tenancy and Access Control 52
Data Residency 52
Compliance and Data Governance 53
Optional Analytics Integration 53
Conclusion **54**
Let Us Know What You Think **55**
Customer Support **56**

Executive Summary

The N-able N-central Security Whitepaper outlines the architecture, security features, and operational protocols of N-central, a Remote Monitoring and Management (RMM) platform tailored for Managed Service Providers (MSPs) and IT Pros. It emphasizes secure, scalable, and flexible IT management across diverse environments. This document details the platform's core components, deployment models, data flow, and robust security mechanisms including Zero Trust, multi-tenancy, encryption, and vulnerability management. It also highlights integrations with other N-able solutions like Cove Data Protection and SentinelOne EDR, ensuring comprehensive cybersecurity and business continuity.

Introduction

Managed Service Providers (MSPs) and IT professionals face mounting challenges in securing and managing diverse client environments. N-able N-central is a robust Remote Monitoring and Management (RMM) platform purpose-built to address these demands. It empowers MSPs and IT Pros to proactively monitor, automate, and secure IT infrastructures across workstations, servers, mobile devices, and network equipment from leading manufacturers.

Designed for flexibility, N-central supports both on-premises and cloud-hosted deployments, enabling organizations to tailor their approach based on operational needs and security requirements. Its modular architecture ensures scalability, allowing service providers to manage thousands of endpoints efficiently while maintaining high performance and reliability.

Security is foundational to the N-central design. The platform integrates advanced features such as Zero Trust access controls, multi-tenancy, encrypted communications, and vulnerability management to safeguard client systems and ensure compliance with industry standards.

N-central also plays a strategic role within the broader N-able Ecoverse—a unified, cloud-native ecosystem that brings together cybersecurity, data protection, and IT management solutions. Through shared APIs, centralized identity management, and seamless integration with tools like Cove Data Protection and Adlumin MDR, Ecoverse enhances operational resilience and simplifies service delivery for modern MSPs.

Purpose

The purpose of this document is to provide a comprehensive overview of the security architecture of N-able N-central. This document aims to inform MSPs and IT Pros about the security features, protocols, and best practices embedded within the N-able N-central solution. By understanding the security architecture, stakeholders can better appreciate how the solution safeguards client systems, ensures compliance with industry standards, and mitigates potential security risks.

Target Audience

This document is intended for MSPs and IT Pros who are responsible for the deployment, management, and support of remote monitoring and management solutions within their client organizations. The target audience includes:

- **IT Managers and Directors**: Individuals overseeing IT operations and strategy within MSPs and IT Pros, who need to understand the security capabilities and benefits of N-able N-central.
- **System Administrators**: Professionals within MSPs and IT Pros responsible for the day-to-day management and maintenance of client IT systems, who require detailed knowledge of the solution's security architecture to ensure system integrity and protection.
- **Security and Compliance Analysts**: Experts within MSPs and IT Pros focused on identifying and mitigating security threats, as well as ensuring that organizational practices meet regulatory requirements. They need to understand how N-able N-central addresses potential vulnerabilities, ensures robust system security, and supports compliance with data protection standards.
- **Technical Support Engineers**: Personnel within MSPs and IT Pros providing frontline support to customers, who need to be familiar with the solution's security features and troubleshooting procedures.

By addressing the needs and concerns of these key stakeholders, this document aims to facilitate informed decision-making and effective implementation of the N-central security measures within diverse client IT environments.

Summary of Problem

IT environments face increasing complexity and evolving cybersecurity threats. MSPs and IT Pros must manage diverse infrastructures, ensure compliance with regulatory standards, and protect sensitive data—all while maintaining operational efficiency. Traditional tools often lack the scalability, integration, and security needed to meet these demands.

Problem Statement

MSPs and IT Pros require a unified, secure, and scalable platform to manage client environments effectively. The challenge lies in balancing flexibility, performance, and security across on-premises and cloud deployments, while ensuring compliance, threat detection, and resilience against cyberattacks.

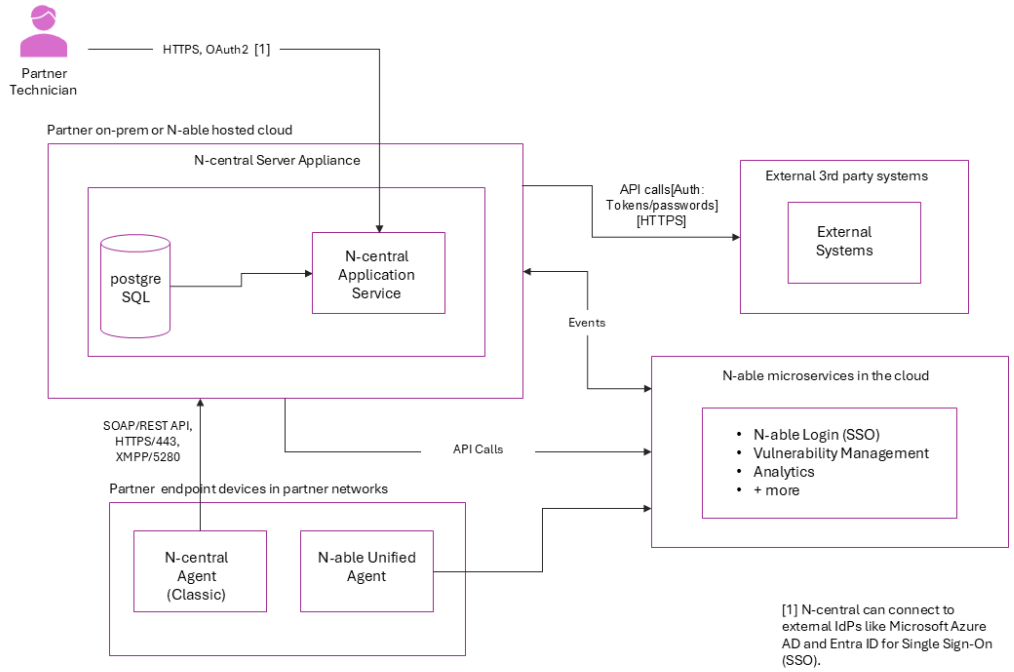
Proposed Approach

N-able N-central addresses these challenges through:

- Modular Client-Server Architecture: Supports both hosted and on-premises deployments with distributed agents and probes.
- Zero Trust Security Model: Enforces strict access controls, multi-factor authentication, and session management.
- Multi-Tenancy: Ensures tenant isolation, scoped APIs, and credential vaulting.
- Secure Development Lifecycle (SDLC): Incorporates secure coding, penetration testing, and vulnerability management.
- Data Encryption: TLS 1.2/1.3 for transmission and AES-256 for data at rest.
- Patch and Vulnerability Management: Automated patching workflows, compliance reporting, and integration with CVE databases.
- Remote Control and Monitoring: Secure remote access via encrypted protocols and session logging.
- Integration Ecosystem: REST APIs, webhooks, and compatibility with ITSM platforms like ServiceNow and Halo PSA.
- Analytics and Reporting: Real-time and historical insights into device health, patch status, and security compliance.
- Complementary Tools: Integration with Cove Data Protection for backup and SentinelOne EDR for endpoint threat detection.

Core Architecture

N-central follows a client-server architecture, where a central N-central Server communicates with various agents, probes, and client devices to provide monitoring, management, and automation services.



N-central offers two deployment options, on-premises and hosted, each catering to different organizational needs and preferences, whilst offering the same core capabilities.

- **On-Premises (Self-hosted, using AWS and Azure)**: Organizations can install and operate the N-central server on hardware within their own infrastructure. This deployment model gives teams direct control over the environment, enabling greater customization and hands-on management of the server. It suits organizations with specific security requirements or those that prefer to maintain and manage their IT infrastructure internally.
- **Hosted**: Organizations can deploy N-central using the N-able cloud infrastructure, hosted on Amazon Web Services (AWS). This model eliminates the need for on-site hardware and reduces maintenance responsibilities. N-able manages server operations, including updates and backups, allowing teams to focus on core activities. Hosted deployment offers a scalable and cost-effective solution for organizations seeking to minimize administrative overhead while maintaining reliable access to N-central capabilities.

Core Components

At the heart of the N-central functionality are several core components that work together to provide seamless IT management. These components include

- **N-central Server**: The core system that manages data and communications.
- **Agents**: Installed on client devices to collect data and perform tasks.
- **Probes**: Network devices that monitor and manage network segments and agent less devices.

Additionally, N-central features APIs and integration layers that allow it to connect with third-party tools, extending its capabilities even further.

Together, these core components form a scalable and secure IT management ecosystem that enables MSPs and IT Pros to provide proactive IT services, improve operational efficiency, and maintain high levels of service quality across multiple client environments. The following sections explore each component in detail, highlighting its role within the N-central architecture.

N-central Server

The N-able N-central server is the "brains" of the system and contains a number of components including the Web Interface, Data Management System (DMS), Database, and other core system components. In addition to providing an interface for the Agents and Probes, the DMS is also the business logic layer of the application. All rules that govern how N-able N-central deals with data are executed at this level.

The N-able N-central server operates as an appliance that communicates with agents and services over the internet. To secure this communication, organizations should apply network security best practices that align with internal policies. A recommended approach involves placing the N-central server in a demilitarized zone (DMZ) and enforcing appropriate firewall restrictions.

By default, fresh installations enable both the user interface (UI) and agent communication ports. Administrators can configure and secure these ports independently, allowing for tailored access controls and segmentation based on organizational needs. See Port access requirements for the ports that the N-able N-central server must have access to.

Agents and Probes (Classic)

A Probe is a Windows application that resides on a system within a customer's network, behind their firewall or within their private IP space. Probes provide network discovery, monitoring and management services for devices on that private network, leveraging industry standards such as WMI, SNMP, ODBC, and other protocols as needed. In addition, the probes are capable of discovery and installing agents on compatible devices when configured.

An Agent is a software component that MSPs or IT Pros can install on a Microsoft Windows, macOS, or Linux device to gather data specific to that local device.

- N-able N-central Probes and Agents communicate with the N-able N-central server using similar architecture and methods. The Probes and Agents leverage client-side initiated communications, where all data communications begin with an outbound call from the Agent or Probe.
- As a direct result of this architecture, there is no public IP address or port forwarding required from the Internet to the devices running the Probes or Agents. The outbound communications from the Agents to the N-able N-central server are based on SOAP and Extensible Messaging and Presence Protocol (XMPP), and are transmitted using the HTTPS protocols on the standard web ports. The nature of these communications allows for the support of standard proxies on the local network.
- After the outbound session is established over port 443, the Agent receives a session ID that is used to identify that session, and it persists until the session is closed. The Agents and Probes will open a second (asynchronous) signaling channel leveraging the XMPP protocol (on port 5280) that is persistent to allow the N-able N-central server to signal the Agents and Probes when actions are necessary (such as to initiate a remote-control session). In cases where the XMPP session is terminated abnormally (for example, by a firewall cleaning open sessions), the Agent will re-create the session automatically.
- N-able N-central leverages XMPP (Extensible Messaging and Presence Protocol) based communications for control purposes only, not for the transmission of monitored data. It plays an important role in both Take Control and Direct Support Tools by ensuring quick and efficient communication between the N-central server, technicians, and managed devices. As an additional measure, the XMPP protocol can be turned off for individual devices or globally, however, this is not recommended as this will increase system load and will cause latency on certain N-able N-central features.

Unified Agent (Modern Agent)

The N-central Unified (Modern Agent) Agent is a key part of the N-able agent modernization effort. It is designed to run side-by-side with the existing N-central agent, ensuring a smooth transition while new capabilities are developed and deployed.

Parallel Operation - The Unified Agent runs alongside the current agent without interference, allowing for a gradual transition.

Function Migration - Over time, N-central functionalities will migrate from the Classic Agent to the Unified Agent, enhancing performance and security.

Automatic Updates - The Unified Agent checks for updates during its regular operations and applies them automatically, ensuring it remains up-to-date with the latest security patches.

Unified Agent Communication Flow

The Unified Agent in N-central communicates with several components to support cloud-based functionality and endpoint management. Here's a breakdown of its communication flow:

Cloud Microservices (Ecoverse Layer)

- Sends telemetry data (e.g., device health, patch status, vulnerability info)
- Receives orchestration instructions, such as feature activation or remediation tasks
- Communicates securely through HTTPS using event-driven protocols

N-central Server

- Exchanges device registration, policy enforcement, and status updates
- Uses SOAP/REST APIs, HTTPS (443), and XMPP (5228) for communication

Patch Management Engine (PME)

- Triggers patch scans and installations
- Reports patch results and reboot status
- May use Windows Update Agent (WUA) for online scans or offline metadata

N-able Ecoverse

Ecoverse is a set of cloud-hosted capabilities that are part of the N-central cloud-native evolution, extending N-central capabilities through a modular, microservices-based architecture that supports dynamic feature delivery, secure data handling, and integration with third-party platforms.

Cloud-hosted capabilities such as vulnerability management, patch intelligence, cloud asset control, and identity services surface through components that expose cloud features within the N-central user interface without impacting backend systems or customer-managed infrastructure. Decoupling functionality into discrete services improves scalability, flexibility, and operational efficiency across managed environments.

How Ecoverse integrates into the N-central architecture

Cloud Microservices

The N-central architecture leverages cloud microservices to deliver modular, scalable, and event-driven IT management capabilities. Each microservice is a contained, independently deployable unit that performs a specific function within N-central.

Microservices operate as part of a distributed cloud layer that interfaces with:

- The N-central Server Appliance (on-prem or cloud-hosted)
- The Unified Agent on managed endpoints
- External systems, for example, identity providers such as Microsoft Entra ID, to enable SSO.

They communicate via secure APIs, event streams, and schema-driven orchestration, enabling real-time responsiveness and modular feature delivery.

Data flow and Communications

Agents continuously monitor endpoints and send telemetry data to probes or directly to the server using encrypted communication channels to ensure data security.

Typical Data Flow

Agents collect telemetry data such as system health, performance metrics, patch status, and logs, then transmit it securely via TLS either directly to the N-central server or to distributed probes across the network. Probes aggregate and preprocess data from multiple agents, cache software files (for example, patches, agents), and forward processed data to the server. The server stores this information in a PostgreSQL database, analyzes it to generate alerts, evaluate compliance, and trigger automation workflows as configured by administrators. Administrators access this data through the web-based UI or via APIs and webhooks for integrations.

Probe and Agent (Classic) Communications

Client-side initiated communications use HTTPS protocols. Probes and agents communicate with the N-central server via SOAP and XMPP, with data encrypted using TLS. This architecture ensures secure and efficient data transmission between components.

Probe as a Cache

Probes act as cache locations for software installation files, including the Agent, AV Defender, and Windows patches. Agents communicate with probes to retrieve these files, reducing bandwidth usage and accelerating software deployments.

Database Server

The database server is a critical N-central component responsible for storing all system data, including device configurations, logs, monitoring data, and reports. Using PostgreSQL as the database engine, it delivers robust performance, reliability, and scalability. This setup ensures data integrity and availability, supporting the efficient operation of N-central capabilities.

Web-based User Interface

The web-based User Interface (UI) provides administrators with a centralized console to manage and monitor devices. It offers Role-Based Access Control (RBAC), enabling multi-user access with varying permissions based on roles and access groups. The system applies the Least Rights Principle (LRP) when permissions overlap, ensuring secure delegation of tasks and maintaining control over system access. The intuitive UI enhances the user experience, providing seamless and comprehensive IT management.

Integration Layer (API & Webhooks)

The N-central Integration Layer enhances connectivity and automation through its REST API and webhooks. It supports seamless integration with third-party tools, including PSA platforms such as MSP Manager, ConnectWise, Autotask, ticketing systems, and billing platforms. This API allows administrators to extend N-central capabilities by connecting with essential business applications, creating a cohesive IT management ecosystem. Webhooks enable event-driven automation, allowing custom workflows to trigger in response to specific system events. Together, these features support dynamic, automated processes that improve operational efficiency and responsiveness.

Scalability

N-central employs a client-server architecture designed to support scalable management across IT environments of all sizes—from a few endpoints to enterprise networks with thousands of nodes. At the heart of its scalability are

distributed probes and agents, which decentralize data collection and processing. Agents send data to nearby probes, which aggregate, preprocess, and cache data—such as patch files—and then forward it to the central server. This reduces bandwidth usage and minimizes load on the server infrastructure

The PostgreSQL database serves as a robust, reliable back end, handling large volumes of device configurations, logs, monitoring data, and reports. Its support for indexing, replication, and query optimization is essential for maintaining performance at scale

N-central offers flexible deployment options, including on-premises and cloud-hosted environments, allowing organizations to tailor their infrastructure to growth demands. While virtualization is supported, N-able notes that performance variability depends on host configurations and hardware, and best performance is often achieved with dedicated server resources.

N-central is architected to support IT environments of varying sizes, from small deployments to enterprise-scale networks with more than 2,000 nodes. Its modular and distributed design enables the platform to scale horizontally and vertically without compromising performance or reliability.

A key scalability enabler is the use of distributed probes and agents for decentralized data collection and processing. Probes act as intermediaries between endpoints and the N-central server, aggregating telemetry data, caching software installation files, and reducing bandwidth consumption during software deployments. This reduces the load on the central server and optimizes network traffic in large, geographically dispersed environments.

The system's PostgreSQL database engine provides a high-performance, reliable backend for storing device configurations, logs, monitoring data, and reports. PostgreSQL's robust indexing, replication, and query optimization capabilities support large-scale data handling and fast retrieval times, even under heavy load.

N-central also supports flexible deployment options—including on-premises and hosted environments—allowing administrators to choose configurations that match organizational growth and resource requirements. Role-based access control (RBAC) and multi-tenancy ensure that scaling to manage multiple clients or large endpoint inventories remains secure and manageable.

Through this architecture, N-central can maintain operational efficiency and responsiveness in large-scale deployments, enabling consistent monitoring, automation, and reporting across thousands of devices.

Secure Platform Architecture

N-central incorporates security as a core part of its architecture and ongoing development.

Multi-Tenancy

N-able N-central is built to support secure, scalable multi-tenancy for both hosted and on-prem deployments. Multi-tenancy allows MSPs and IT Pros to manage multiple customer environments independently from a single platform instance without risking data leakage or policy crossover.

Tenant Isolation Mechanisms: Tenant data - including scripts, configuration files, reports, logs, and credentials - is stored and processed using logical data separation, ensuring each tenant's information remains isolated to prevent unauthorized cross-tenant access.

Role-Based Access Control: Tenant-specific access permissions ensure technicians can only interact with the data and devices for which they have been explicitly granted rights.

Scoped APIs and UI Contexts: All API calls and UI actions are scoped to the user's tenant context, preventing accidental or malicious data exposure.

Credential Vaulting: Credentials are stored per tenant and protected by strong encryption, ensuring compartmentalization.

Audit Logging: All actions within the platform are logged with tenant identifiers for forensic traceability and compliance purposes.

This isolation model prevents unauthorized access between tenants and strengthens regulatory compliance for service providers working with sensitive or regulated industries.

Zero Trust Access Controls

N-central never assumes trust. It authenticates and authorizes every access attempt. Micro-permissions, audit trails, and limited session lifetimes reduce attack surfaces.

Recommended exclusions for third-party AV software

N-able N-central software (agents and probes) must be excluded from third party antivirus scans in order to function properly.

N-able recommends adding the following path to the list of exclusions from security scans:

Folders

N-able N-central needs read/write access to following folders and their subfolders:

- `%Programfiles(x86)%\MspPlatform\PME`
- `%Programfiles(x86)%\MspPlatform\FileCacheServiceAgent`
- `%Programfiles(x86)%\MspPlatform\RequestHandlerAgent`
- `%ProgramData%\MspPlatform`
- `%programfiles(x86)%\MSP-agent`

Applications

N-able N-central needs installation and access to following applications:

- `%Programfiles (x86)%\MspPlatform\FileCacheServiceAgent\FileCacheServiceAgent.exe`
- `%Programfiles(x86)%\MspPlatform\PME\ThirdPartyPatch\7z.exe`
- `%Programfiles(x86)%\MspPlatform\PME\Installers\CacheServiceSetup.exe`
- `%Programfiles(x86)%\MspPlatform\PME\Installers\RPCServerServiceSetup.exe`
- `%Programfiles(x86)%\MspPlatform\PME\Diagnostics\PME.Diagnostics.exe`
- `%Programfiles(x86)%\MspPlatform\RequestHandlerAgent\RequestHandlerAgent.exe`
- `%programfiles(x86)%\msp-agent\msp-agent-core.exe`

Firewall

The Firewall must not block the following outbound communication channels:

- HTTPS communication (port 443) between FileCacheServiceAgent windows service `(%Programfiles (x86)%\MspPlatform\FileCacheServiceAgent\FileCacheServiceAgent.exe)` and sis.n-able.com server (Server-In the-sky, N-able cloud server)

For a complete list of paths to include for exclusion from security scans, see Global Exclusions in the N-able N-central Online Help. This list includes folders excluded by AV Defender by default.

The Upgrade Process

Upgrading N-able N-central involves not only upgrading the N-able N-central server but also the Agents and Probes that communicate with it. For detailed instructions on how to perform an upgrade, refer to *"Upgrading to This Release"* in the Release Notes. Refer to Upgrading to This Release.

The upgrade process for N-able N-central consists of a number of elements including:

Agent and Probe Upgrade

When Agent and Probe upgrade settings are set to Always, the server upgrade process follows this sequence:

1. The first time that the Probe connects to the N-able N-central server after it has been upgraded, the Probe will detect the new version. The Probe will be updated automatically if it has been configured to do so.
2. After being upgraded, the Probe automatically downloads the latest version of the Agent upgrade software and store it in the Windows directory `C:\Program Files (x86)\N-able Technologies\Windows Software Probe\cache`
3. If the Agents have been configured to upgrade automatically, they will:
    a. Ping all of the Probes they can communicate with to determine which Probe provides the fastest response time.
    b. Download the Agent upgrade software from the fastest Probe they can communicate with.
4. If the Agents cannot connect to a Probe, they download the Agent upgrade software directly from the N-able N-central server.

In line with best practice to avoid unnecessary strain on the internet connection, enable Probe upgrades one hour after the server upgrade. Once Probe upgrades are complete, enable Agent upgrades so Agents retrieve installation files from a local Probe.

Software Upgrades for AV Defender

Upgrades for AV Defender follow the same procedure if the probe has been enabled as the update server:

1. The Windows Probe communicates with sis.n-able.com to determine the latest upgrade software every hour. If a new version is available, the Windows Probe downloads the latest upgrade software.
2. If AV Defender installed on a device, the Agent communicates via port 443 with the Windows Probe (or Probes) on the network to determine if it is running the latest version.
3. The Agent will download the upgrade software from the Probe.

The N-able N-central server connects with sis.n-able.com on an hourly basis to check for new upgrades. If a newer version of the software is available, the appropriate service (for example, the AV Defender Status service for AV Defender) transitions to a Warning state until the software on that device is upgraded.

If the Probe is not set up as the update server, or is unavailable, AV Defender agents retrieve their ugrades directly from the N-able N-central server (sis.n-able.com) or from external Bitdefender URLs like upgrade.bitdefender.com.

Key Security Features

N-able implements a comprehensive set of security features to protect client environments and service operations as threat landscapes evolve and regulatory requirements increase. The platform enforces multi-factor authentication, role-based access control, data encryption, audit logging, and integrated threat monitoring to support a secure and scalable IT management framework. As organizations rely more heavily on technology, the N-able security foundation defends infrastructure, protects sensitive data, mitigates threats, and supports business continuity.

N-able uses a comprehensive, multi-layered approach to ensure the security of its software platforms, aligning with industry best practices and regulatory standards. Key strategies include:

- **Secure Development Lifecycle**: N-able integrates security throughout its software development processes, adhering to the "Secure by Design" principles. This commitment is underscored by their signing of the CISA Secure by Design pledge, emphasizing proactive risk management and transparency in product development.
- **Access Control and Identity**: The system applies Role-Based Access Control (RBAC) to manage access to systems and data. It assigns permissions according to user roles, ensuring users operate within their authorized scope and reducing security exposure.
- **Data Encryption**:The system protects sensitive data using robust encryption methods, applying AES 256-bit encryption for backups and TLS 1.2 and 1.3 for data transmission to secure information both at rest and in transit.
- **Threat Detection and Response**: N-able incorporates advanced threat detection capabilities, such as Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR), to identify and mitigate security threats effectively.
- **Vulnerability Management**: The platform includes built-in vulnerability management tools that enable organizations to identify, prioritize, and remediate security vulnerabilities across various operating systems.
- **Audit Logging and Monitoring**: Comprehensive audit logs track system access and activities. These logs are monitored by trained security personnel to detect and respond to potential security events promptly.

These measures collectively contribute to the N-able robust security posture, ensuring the protection of its software and the data managed within.

Secure Software Development Lifecycle (SDLC)

N-able follows a Secure Development Lifecycle (SDLC) to ensure security is built into N-central from the ground up.

- **Code Reviews & Secure Coding Practices**: Developers follow OWASP Secure Coding Guidelines to prevent SQL injection, cross-site scripting (XSS), and remote code execution (RCE) attacks. Peer code reviews and static code analysis are performed to detect vulnerabilities early.
- **Penetration Testing & Security Audits**: Independent security firms conduct penetration tests to simulate attacks and find weaknesses. Regular internal security audits ensure compliance with industry standards.
- **Vulnerability Management & Patching**: N-able uses continuous vulnerability scanning and bug bounty programs to identify risks. Security patches and automated updates help fix known vulnerabilities quickly.

Access Control and Identity

Role-Based Access Control (RBAC) defines user permissions based on assigned roles and responsibilities. Instead of assigning permissions to individual users, N-central assigns them to roles, which simplifies access management and ensures users only access the data and tools required for their tasks. This approach enforces the principle of least privilege (PoLP) by restricting access to the minimum necessary for each role, reducing the risk of unauthorized actions. By implementing RBAC, administrators prevent accidental data exposure and mitigate insider threats.

Multi-Factor Authentication (MFA) adds a second layer of identity verification to all administrative logins and is strongly recommended for all users. MFA requires users to verify their identity beyond just a username and password, which helps prevent unauthorized access, even if credentials are compromised.

Single Sign-On (SSO) and secure password policies form part of the N-central security framework. N-central integrates with Active Directory (AD) and OIDC-based SSO providers, allowing users to authenticate once and access multiple systems without re-entering credentials. Administrators can enforce strong password policies to ensure complexity and regular updates. N-central also enforces automatic session timeouts to log out inactive users and reduce exposure to unauthorized access.

N-able Login and Entra ID provide federated SSO capabilities, allowing users to authenticate once and gain access to multiple applications without needing to re-enter credentials. This setup enhances security while simplifying the user experience.

Strong Identity and Access Management (IAM) Practices N-central supports strong Identity and IAM practices. Administrators enforce MFA for all technicians, significantly lowering the risk of compromised accounts. N-central supports MFA through authentication apps like Google Authenticator and Microsoft Authenticator, offering flexibility and enhanced security for user access.

Data Encryption

N-able ensures that customer data and communications remain private and secure.

- End-to-End Encryption
- TLS 1.2 and 1.3 encryption secures all communication between N-central agents and servers.
- Sensitive data stored in the N-central database is encrypted at rest using industry-standard algorithms.
- Secure Remote Access Controls
- Remote sessions use AES-256 or AES-128 encryption to prevent eavesdropping and MITM (Man-in-the-Middle) attacks.
- Role-Based Access Control (RBAC) ensures only authorized technicians can perform remote actions.
- Data Residency & Compliance
- N-able allows organizations to choose regional data centers for compliance with GDPR, and ISO 27001.

Vulnerability Detection

Vulnerability detection in N-able N-central is part of its built-in Vulnerability Management capability. It continuously scans managed endpoints to identify known security vulnerabilities in operating systems and applications across Windows, macOS, and Linux environments. N-central uses the Unified Agent (Modern Agent) to detect vulnerabilities across managed assets and lists them individually or by vulnerability.

Key Capabilities

- **Continuous Scanning**: Automatically detects vulnerabilities using CVE (Common Vulnerabilities and Exposures) data.
- **Severity Assessment**:Assigns severity levels (Critical, Important, Moderate, Low) and CVSS scores to each vulnerability.
- **Asset Risk Mapping**: Shows which devices are affected and how many assets are at risk.
- **Update Availability**: Indicates whether a patch or update is available to remediate the vulnerability.
- **Threat Status**: Marks vulnerabilities as Resolved or Unresolved based on remediation status.

Network and Infrastructure Security

Firewall and Intrusion Detection Systems (IDS/IPS) N-central includes firewall and IDS/IPS capabilities as part of its network and infrastructure security:

- Firewall: Filters traffic based on rules, blocks unauthorized access, and integrates with AV Defender for endpoint-level control.
- IDS: Monitors traffic for suspicious patterns and alerts administrators.
- IPS: Actively blocks threats in real time using signature and behavior-based detection.
- Security Profiles: Allow configuration of TLS versions and cipher strength to meet compliance standards (Modern, Compatibility, Legacy) 2.

Audit Logging and Incident Response are crucial for maintaining security and compliance. N-central keeps detailed audit logs of all user activities, login attempts, and configuration changes, providing a comprehensive record of system interactions. These logs help track actions, identify anomalies, and ensure accountability. Additionally, N-central allows administrators to set up notifications for monitored devices that are protected by our integrated antivirus and EDR products. This offers an additional layer of protection for those devices by leveraging the N-central notification and PSA features which can promptly alert the needed resources to respond to incidents.

Regular Security Updates and Advisory Notices are essential for maintaining system security and protecting against new threats. N-able releases regular security patches that address vulnerabilities and enhance the overall security of the system. These updates are crucial for preventing exploits and ensuring that the software remains resilient against emerging threats. Additionally, N-able publishes security advisories to inform users of potential risks and best practices. These advisories provide valuable information on how to mitigate risks and maintain a secure environment, helping users stay informed and proactive in their security efforts.

Disaster Recovery & Business Continuity (hosted only)

N-able ensures N-central remains resilient against cyberattacks, hardware failures, or natural disasters.

Automated Backups and Redundancy are essential for ensuring data integrity and availability in N-central. Data is backed up in multiple locations to prevent data loss, providing a robust safety net against potential failures. For cloud-based deployments, N-central utilizes geographically redundant servers, which means that data is replicated across different geographic regions. This setup ensures that in the event of a regional outage or disaster, the system can failover to another location, maintaining continuous uptime and access to critical data. These automated backups and redundancy measures are designed to protect against data corruption, deletion, and hardware failures, ensuring that IT management operations remain resilient and reliable.

On-Prem MSPs and IT Pros can set up their own disaster recovery following the same principles by using N-central to create automated backups and sending them to an offsite FTP.

Security Profiles

Sometimes, working with older operating systems that use older security protocols. Security Profiles in N-able N-central enable selection between modern security protocols, or legacy ones. The Modern security profile is enabled by default to block TLS 1.0 and 1.1. You can switch the network security profile to the Legacy Security Profile to use older TLS versions. To change Security Profiles, at the System level, click **Administration** > **Mail and Network Settings** > **Network Security**.

Modern security profile

- Configures N-central's Web UI, Administration UI, Agent/API, and XMPP services to support TLS versions 1.2 and 1.3.
- For all web interfaces, enables AED Key Exchange (AKE) GCM, and ChaCha20 Poly1305 based TLS 1.3 ciphers, using either x25519 or secp256r1 EC curves.
- Enables only Perfect Forward Secrecy (PFS), GCM-based TLS 1.2 ciphers, using either x25519 or secp256r1 EC curves.
- Disables weak SSH Ciphers, MACs, and KEX Algorithms.
- Will work with Modern Operating Systems (Windows 10, Windows Server 2016, OS X 10.11 (El Capitan), iOS 9, Android 4.4.2, and newer).
- Meets PCI DSS 3.2.1, Requirements 2.3, and 4.1.

The *Modern* security profile supports the following ciphers:

TLS 1.3

- TLS_AKE_WITH_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AKE_WITH_AES_128_GCM_SHA256

TLS 1.2

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Compatibility security profile

The *Compatibility* security profile sits between the *Modern* and *Legacy* security profiles. It allows you to support operating systems in their Extended Lifecycle, such as Windows Server 2012 R2, without needing to allow TLS 1.1 or 1.0.

- Configures N-central's Web UI, Administration UI, Agent/API, and XMPP services to support TLS versions 1.2 and 1.3.
- For all web interfaces, enables AED Key Exchange (AKE) GCM, and ChaCha20 Poly1305 based TLS 1.3 ciphers, using either x25519 or secp256r1 EC curves.
- For the Administration UI and XMPP services, enables only Perfect Forward Secrecy (PFS), GCM-based TLS 1.2 ciphers, using either x25519 or secp256r1 EC curves.
- For the Web UI and Agent/API services, enables GCM-based RSA ciphers in addition to the ECDHE GCM-based TLS 1.2 ciphers from the “Modern” profile.
- Disables weak SSH Ciphers, MACs, and KEX Algorithms.
- Will work with Extended Lifecycle, and Modern Operating Systems (Windows 7/IE11, Windows Server 2008 R2/IE11, OS X 10.11 (El Capitan), iOS 9, Android 4.4.2, and newer).
- Meets PCI DSS 3.2.1, Requirements 2.3, and 4.1.

The *Compatibility* security profile supports the following ciphers **in addition to** those supported by the *Modern* security profile:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

When choosing which of the weaker ciphers to make available to the **Compatibility** security profile, we looked at the security levels and theoretical/proven attacks on both non-PFS, and CBC-based ciphers. At this time, the theoretical capability to decrypt CBC-based ciphers without the private key is easier for an attacker to exploit than an attack against non-PFS, GCM based ciphers without access to the N-central server's private key.

PFS - Perfect Forward Secrecy: After negotiating the TLS connection, a new, ephemeral public/private key pair is generated for the connection, and the devices use this for encrypting the traffic. Non-PFS ciphers continue using the public/private key pair the connection was initiated with.

Legacy security profile

N-able plans to deprecate the *Legacy* security profile in a future release of N-central. As a result, we strongly recommend that you upgrade your legacy devices that may be preventing you from using a more secure security profile.

- Configures N-central's Web UI and Agent/API services to support TLS versions 1.0 through 1.3.
- Configures N-central's Administration UI and XMPP services to support TLS versions 1.2 and 1.3.
- For all web interfaces, enables AED Key Exchange (AKE) GCM, and ChaCha20 Poly1305 based TLS 1.3 ciphers, using either x25519 or secp256r1 EC curves.
- For the Administration UI and XMPP services, enables only Perfect Forward Secrecy (PFS), GCM-based TLS 1.2 ciphers, using either x25519 or secp256r1 EC curves.
- For the Web UI and Agent/API services, enables the same GCM-based RSA ciphers, ECDHE GCM-based ciphers from the "Compatibility" profile. Additionally, it enables the TLS 1.0/1.1 CBC-based RSA and ECDHE ciphers with SHA1, and the legacy CBC-based RSA cipher with 3DES as opposed to AED in all other ciphers.
- Fails PCI/DSS/HIPPA/NIST compliance requirements.
- Works with Legacy, Extended Lifecycle, and Modern Operating Systems (Windows Vista, Windows Server 2008, MacOS 10.11 (El Capitan), iOS 9, Android 4.4.2, and newer).

The Legacy security profile supports the following ciphers in addition to those supported by the *Compatibility* security profile:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Supported Compliance Standards

As organizations increasingly rely on managed IT services, regulatory compliance has become a critical component of secure infrastructure management. Compliance standards provide structured frameworks for protecting sensitive data, ensuring operational integrity, and maintaining accountability across systems and processes.

N-able N-central supports a range of recognized compliance standards that align with industry and governmental requirements. These standards—such as HIPAA, ISO/IEC 27001, SOC 2, GDPR, and CMMC—define specific controls and practices for data security, privacy, and risk management. The N-central architecture and feature set are designed to help service providers implement these controls effectively.

This section outlines the compliance standards supported by N-central, focusing on their technical relevance and the operational benefits they offer in regulated environments.

HIPAA Type 1 Compliance

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data in the U.S. The N-central HIPAA Type 1 compliance ensures that MSPs working with healthcare clients can manage systems and data securely.

- Enables MSPs to serve healthcare organizations confidently.
- Protects electronic protected health information (ePHI).
- Reduces risk of data breaches and regulatory penalties.

ISO/IEC 27001:2013 Certification

ISO 27001 is an internationally recognized standard for information security management systems (ISMS). The N-central certification demonstrates its commitment to managing data securely and systematically.

- Validates robust security practices.
- Builds trust with clients and partners.
- Helps meet global regulatory and contractual requirements.

SOC 2 Type II Attestation

SOC 2 Type II evaluates the effectiveness of a company's controls over time, focusing on security, availability, processing integrity, confidentiality, and privacy. The N-central attestation confirms its reliability in handling sensitive data.

- Demonstrates long-term operational security.
- Supports MSPs in regulated industries like finance and healthcare.
- Enhances credibility with enterprise clients.

GDPR and CCPA Support

The General Data Protection Regulation (GDPR) governs data protection and privacy in the EU. N-central supports GDPR through data residency options and privacy controls.

- Enables MSPs to serve EU clients legally and ethically.
- Reduces risk of non-compliance fines.
- Empowers users with data control and transparency.

Commitment to CMMC 2.0 Readiness

N-able has announced its commitment to Cybersecurity Maturity Model Certification (CMMC) 2.0 readiness for N-able N-central with expected release in 2025.

The Cybersecurity Maturity Model Certification (CMMC) is required for contractors working with the U.S. Department of Defense. N-central is preparing for Level 2 compliance, especially for on-premises deployments.

- Positions MSPs to win DoD contracts.
- Aligns with federal cybersecurity expectations.
- Provides structured security controls and audit readiness.

Integrations and Extensibility

N-central actively supports extensibility and integration across a wide range of enterprise environments. IT Pros and MSPs can connect N-central to ITSM platforms, custom-built tools, and broader business systems to streamline operations and enhance service delivery.

API Capabilities and Custom Development

N-central exposes a powerful REST API that enables developers to:

- Automate device management, alerting, reporting, and configuration workflows
- Integrate with internal systems and third-party platforms
- Enforce scalable multi-tenant operations through RBAC

Administrators can also use event-driven webhooks to trigger external workflows in response to system events such as alerts, patch completions, or device status changes, enabling dynamic and responsive automation.

Integration with Leading ITSM Platforms

N-central integrates natively and flexibly with top ITSM platforms, including:

- ServiceNow
- BMC Helix
- Halo PSA
- Custom PSA implementations via ticketing APIs and webhook endpoints

These integrations synchronize tickets, automate incident handling, and maintain continuity across service platforms.

Flexibility to Connect with Other Enterprise Tools

The N-central integration layer connects with a wide array of enterprise tools, including:

- Billing systems
- Monitoring dashboards
- Cloud infrastructure providers
- Security platforms and compliance tools

This flexibility allows organizations to embed N-central into their broader IT ecosystem and align it with business-specific workflows and data pipelines.

Common Questions and Best Practices

To support enterprise onboarding and large-scale deployments, N-central provides guidance on:

- Security and compliance protocols (e.g., ISO, GDPR, CMMC)
- Scaling for environments with 2,000+ nodes
- Deployment models and onboarding strategies
- Integration troubleshooting and support pathways

Best practices include using the MSP Developer Portal, following secure API usage guidelines, and leveraging the ReadMe Enterprise Edition for interactive documentation and version control.

Pendo UI Integration

N-central integrates with Pendo, a third-party platform that provides UI-level telemetry and in-app messaging to support product improvement and user experience analysis. This integration operates strictly within the web-based user interface and remains isolated from backend systems, agents, probes, and customer-managed infrastructure. It does not access device-level data or interact with operational components, ensuring that telemetry collection is limited to user interface interactions only.

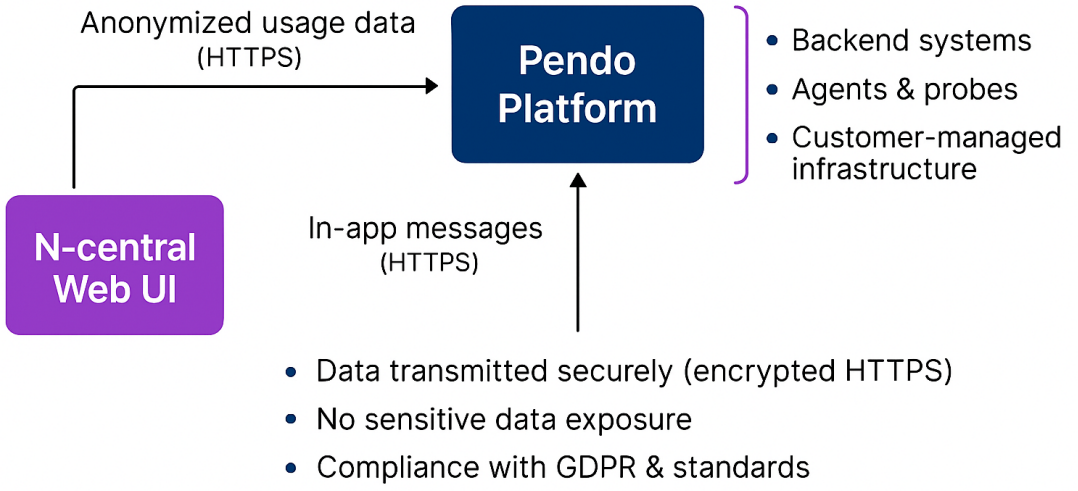
N-central integrates with Pendo to

- Collect anonymized usage data that helps N-able understand how users interact with various parts of the interface such as which features are used most often, where users encounter friction, and how frequently specific actions are performed. These insights inform interface design decisions, feature prioritization, and overall product usability improvements.
- Enable contextual in-app messaging. N-able uses this capability to deliver onboarding walkthroughs, new feature announcements, and proactive guidance, reducing the need for external documentation and improving time-to-value for users.

From a security standpoint, Pendo does not access or transmit sensitive customer data. The anonymized usage metrics and interaction patterns help N-able optimize the platform experience. All communications are encrypted using TLS, and the integration adheres to the N-central broader security posture, including RBAC enforcement and secure session management. The use of Pendo aligns with the N-able security and privacy standards, including compliance with GDPR and other applicable regulations.

From an architectural perspective, Pendo operates as a client-side service embedded in the N-central UI. It communicates with Pendo's cloud infrastructure over HTTPS (port 443), requiring outbound access from the N-central server to specific domains such as cdn.pendo.io, data.pendo.io, and pendo-static.storage.googleapis.com.

The following diagram shows how the Pendo UI integration works with N-central.



N-central Web UI

- Connects to the Pendo platform using HTTPS.

Pendo Platform

- Connects only to the N-central Web UI (no backend/agent access).
- Indicates that Pendo is isolated from:
  - Backend systems
  - Agents & probes
  - Customer-managed infrastructure

Data Flow

- Anonymized usage data flows from N-central Web UI to Pendo (via HTTPS).
- In-app messages flow from Pendo back to N-central Web UI.

Security and Compliance Notes

- How N-central meets security and compliance standards.

Remote Control

A key feature of N-able N-central is the ability to remotely control any managed device, regardless of the user's location on the Internet. Remote control in N-able N-central leverages the location of the N-able N-central server on the Internet and the outbound communications model provided by Agents and Probes.

Remote Control is available on N-able N-central servers with a Professional license.

N-able N-central uses the following methods to establish encrypted connections from the N-able N-central server to the remote control target device:

- Other remote control types use connections established through one of SSH (Secure Shell) or HTTPS (Hypertext Transfer Protocol, Secure).

Security scans performed on N-central servers may, in some cases, report vulnerabilities related to SSH based on the version string. Because the SSH version string represents a truncated, high-level value, it may not accurately reflect the presence of known vulnerabilities. Before investigating further, organizations should verify whether the reported issues have already been addressed in the specific build of OpenSSH included with the server.

Accessing a remote device requires a username and password, regardless of the protocol used.

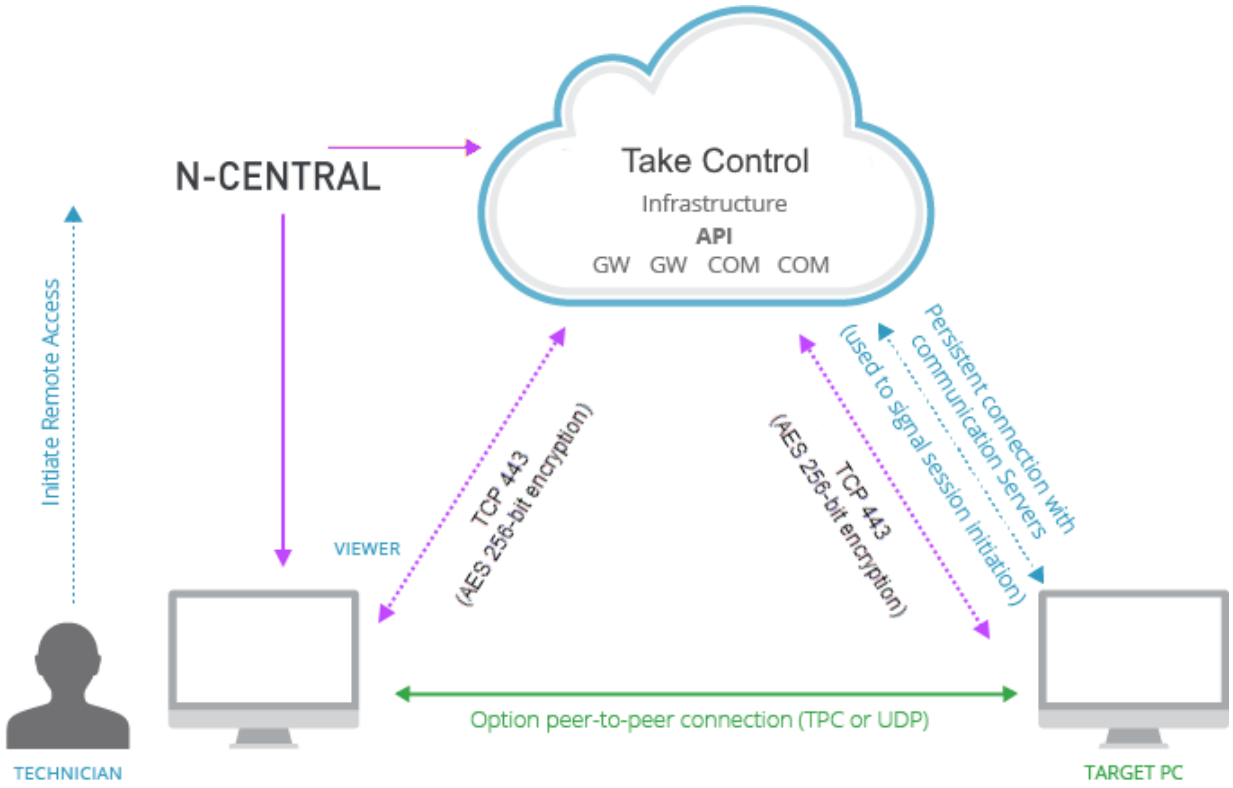
Take Control

Take Control sessions use a proprietary communication protocol with guaranteed global security, AES 256-bit encryption during session establishment and throughout the session. Key exchange is protected by SSL based on AES-CBC with TLS 1.2. All commands, including keyboard and mouse strokes, file transfers and clipboard data are digitally signed.

Take Control does not access session content. Encryption is based on end-to-end negotiation that does not intercept or decode the transferred information or the information in the gateway. Encryption keys are randomly generated for each session.

As an additional security measure, the client can configure authentication using a **Master Password** or **Windows account** and enable **pre-authorization by the machine owner** before launching a session.

Finally, all major features, including remote control, file transfer and chat conversations are logged in the session details and can be recorded as video.



Take Control traffic is secured using multi-layer authentication. Elliptic-curve Diffie-Hellman is implemented to protect our public/private key exchanges, a component step in session instantiation. All commands, including keyboard and mouse strokes, file transfers and clipboard information are digitally signed.

Take Control does not have access to session content. All encryption is based on an end-to-end negotiation that does not intercept transferred information or decode the information in the gateway. Encryption keys are randomly generated for each session.

Take Control uses servers located in large data centers around the world, and a geolocation method ensures the geographically nearest router is always used for the connection.

As public IP Addresses are dynamically assigned (outside of N-able's control) and, as internal infrastructure changes (dynamic or effective), these public IP addresses are required to manage the infrastructure (within N-able's control). **No IP Address lists or ranges can be provided**, guaranteeing that they will not eventually become invalid.

To avoid potential communication or connection problems to these global servers, we recommend you allow the following Ports and URLs in your firewall or web-monitoring software:

Ports

- 443 (TCP)
- 3377 (TCP) - used as a fall over if 443 is unsuccessful

Remote Desktop

Remote Desktop uses a Custom Protocol Handler (CPH) to facilitate the connection to an RDP session. When launching a RDP session, N-able N-central will verify if the CPH application is installed on the host device. If the system does not detect CPH, it prompts the user to download and install the application.

The handler will attempt to use a tunnel over SSH for the connection before failing over to HTTPS (443) to establish the connection. The CPH launcher opens a listening port randomly selected by N-central to start the RDP client.

No CPH for Mac and Linux
Mac and Linux devices still use the Java implementation for Remote Desktop. SSH and webpage require Java to run.
To manage devices from a Mac or Linux technician system, use browser-based remote control if the endpoint supports it. Launch remote sessions from a Windows-based technician machine or VM to leverage CPH.

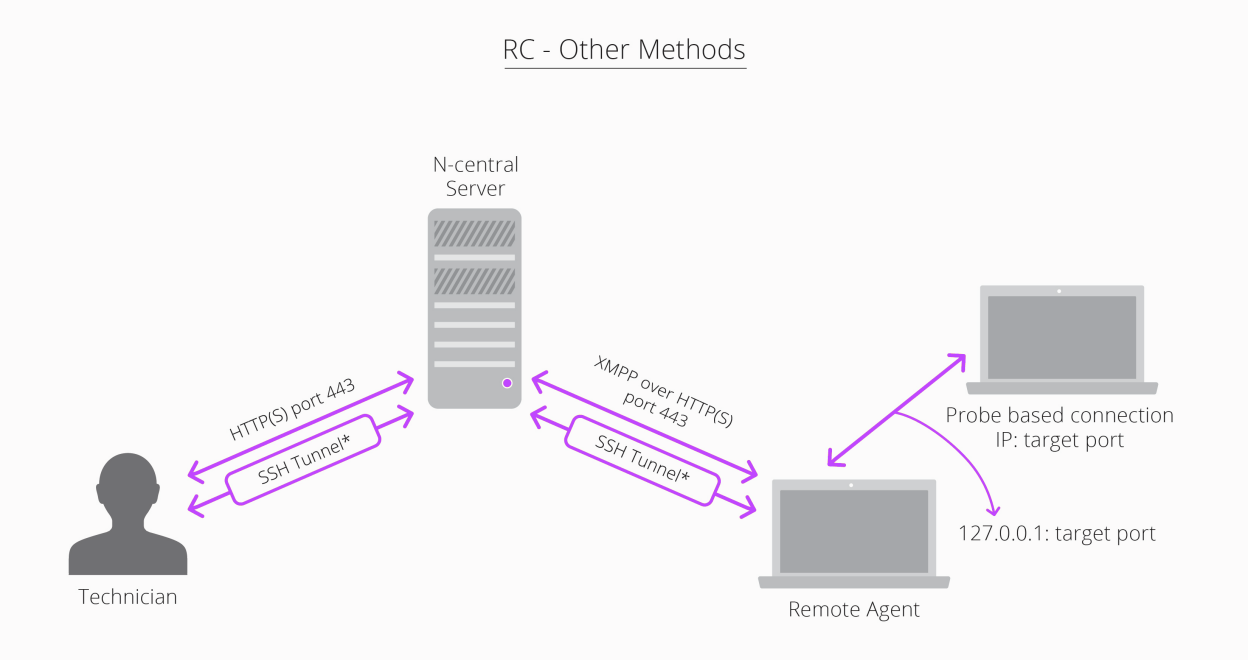
Other Remote Control Connections

For remote control types other than Take Control, the first protocol attempted will be an SSH tunnel (TCP on port 22 to N-central). Should the SSH connection attempt fail, the requesting user and the target system will again attempt to connect to each other through the N-able N-central server using HTTPS on port 443.

Port Number	Port Location			
	N-able N-central Server		Target Device	
	Inbound	Outbound	Inbound	Outbound
Port 22	√	√		√
Port 443	√	√		√

After the requesting user and the target system are connected, the remote control tools can then communicate over this encrypted connection as if they were located on the same network subnet. Since the remote control sessions originate outbound from the user's system, as well as from the device to be remotely controlled, there is no requirement for a public IP address, or inbound port forward for this remote control tool to work.

In the diagrams below, the "SSH Tunnel*" notation indicates the first protocol attempted will be an SSH tunnel (TCP on port 22).



Remote control in N-able N-central uses several layers of security. The outbound request model ensures that there are no inbound reports required.

Data passed through SSH connections is encrypted using 128-bit AES-based encryption keys.

Data is passed through HTTPS connections in combination with SSL and TLS. SSL and TLS are cryptographic protocols that provide secure communications on the Internet. HTTPS is designed for secure encrypted communication between different devices as well as secure identification and authentication of the remote device.

Patch Management

N-able N-central provides an automated Vulnerability and Patch Management solution designed to reduce the attack surface across managed endpoints. It ensures that devices remain protected by systematically identifying vulnerabilities and applying updates based on intelligent policies and insights.

Assess and Prioritize Patches

N-central evaluates detected vulnerabilities using industry-standard metrics like CVSS scores, enabling IT teams to prioritize remediation based on risk. The system provides visibility into missing patches by severity level, displays group and device-level reporting dashboards, and tags vulnerabilities as critical, moderate, or low-risk to support informed decision-making.

Deploy Patches Automatically

N-central enables centralized, policy-based automated patching for Windows and third-party software. Administrators can configure schedules, reboot options, maintenance windows, and fallback behaviors.

- Fully automated or approval-based patch workflows
- Patch caching and bandwidth control using probe-based deployment
- Post-patch reboot and rollback options

Manage Offline Patches

N-central archives metadata for a subset of system patches including Cumulative Updates, Security Only patches, SSUs, and third-party patches on, on sis.n-able.com. Probes retrieve this metadata to deliver updates to devices in offline patching mode, which operates similarly to online patching.

Communication with `sis.n-able.com` uses port 443.

Offline patching uses MSU installer files instead of the CAB installer files that are used with online patching, using the Microsoft Update server. The base URL of these files might also differ from those with online patching.

Patching data for offline devices is done through the probe using port 15000.

Monitor for missing patches

N-central monitors missing patches using the Patch Status v2 Service, which operates as part of the endpoint agent. The agent receives patch data from the Patch Management Engine (PME), which communicates directly with the Windows Update Agent (WUA) to detect available and missing patches. PME passes this information to the agent, which then updates the Patch Status v2 service. This setup allows N-central to report patch status accurately without directly performing patch scans or installations through Patch Status v2 itself.

The Patch Status service shows the following information:

Total missing patches

Displays the total number of Microsoft and supported third-party patches that the device requires but has not yet installed.

- Excludes superseded patches to avoid false positives.

Patches installed with errors

Flags patches that attempted to install but failed.

- Requires administrators to investigate and remediate through patch troubleshooting workflows.

Missing patches by category

Groups missing patches by type, such as security updates, critical updates, or feature updates.

- Allows prioritization of high-impact security patches.

Missing patches older than a user-specified number of days

Highlights patches that remain uninstalled beyond an administrator-defined age threshold.

- Highlights devices that may be out of compliance.

Patches missing but not yet approved

Shows patches identified by WUA as missing but still pending approval in N-central (manual or automatic).

- Keeps these patches in the missing list until approval occurs. These unapproved patches represent a critical blind spot in many organizations' security posture, as they may include high-risk vulnerabilities that are not yet scheduled for remediation.

Compliance and Reporting

To support compliance frameworks (for example, HIPAA, ISO 27001), N-central includes built-in reports and audit trails showing patch status and remediation timelines.

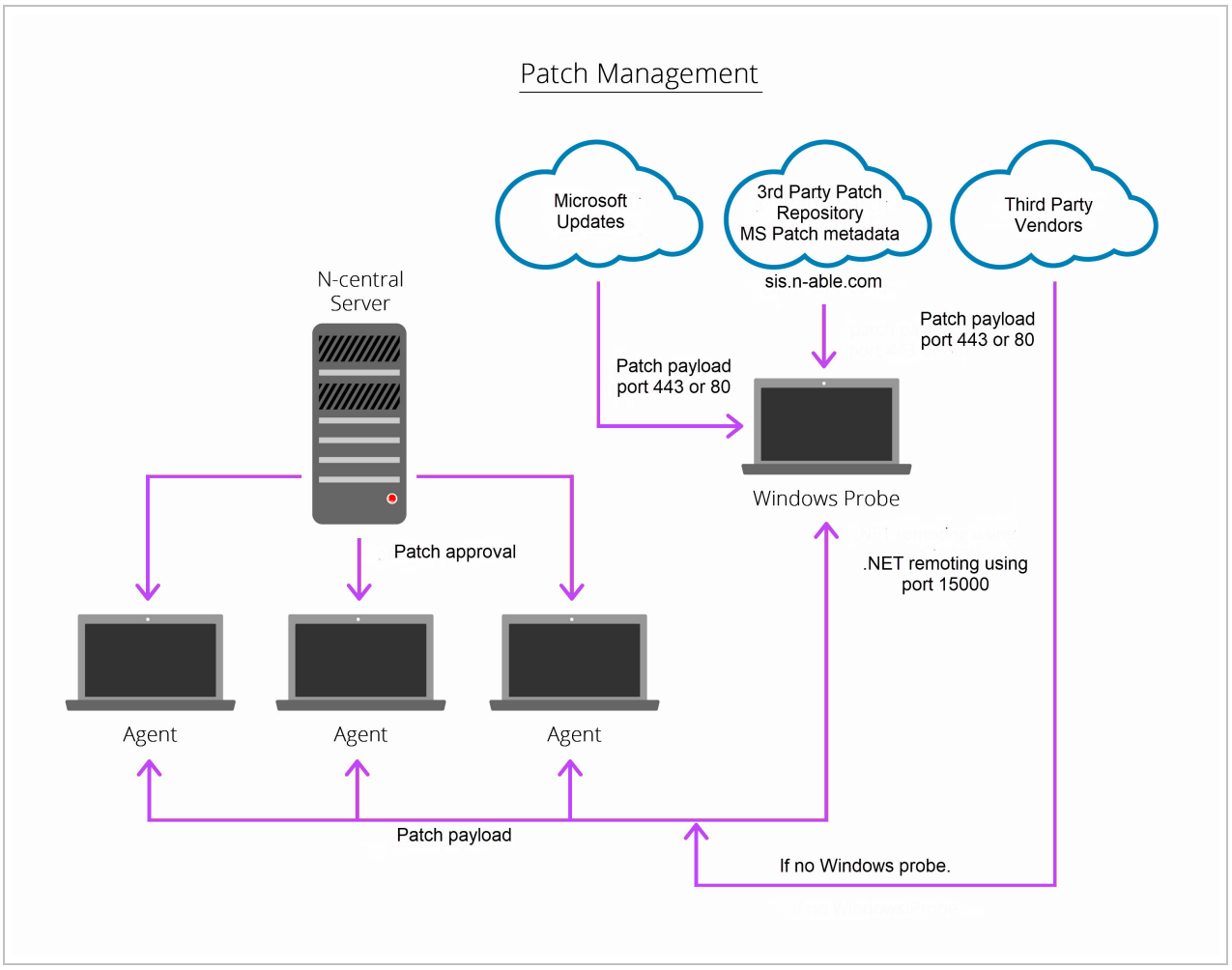
- Audit-ready patch compliance reporting
- Proof of remediation for regulatory requirements
- Executive summaries and technician-level detail

Security Integration

Patch deployment workflows are hardened by the N-central secure agent communication. All patch metadata and deployment instructions are transmitted over TLS-encrypted channels, with role-based access control (RBAC) ensuring that only authorized users can modify policies or force patch actions.

Manage Windows Updates

Windows patch management in N-able N-central uses a coordinated process between the Windows Patch Management Engine (PME) Agent, the local Windows Update Agent (WUA), and N-central components such as Probes and Agents. This process ensures that devices receive the correct updates based on administrator-defined approvals and deployment schedules.



Windows update process flow

The PME Agent queries the WUA to retrieve a list of available updates, sends this information to the N-central server, and then works through a controlled approval and deployment workflow. Once updates are approved, the PME coordinates with Probes or other Agents to download and distribute the updates efficiently, maintaining control over bandwidth usage and installation timing. This method ensures consistent and reliable patch deployment across managed devices:

1. The Windows Patch Management Engine (PME) Agent communicates with the local Windows Updates Agent (WUA) and requests a list of available updates.
2. The Windows Agent sends this information to the N-able N-central server.

   A device can send data directly through another path. See Direct data submission for details.
3. The N-able N-central administrator configures approvals for the list of updates.
4. The PME Windows Agent communicates with the Probe and/or Agent and requests the approved updates.

5. The Windows Agent downloads the required patch files directly from _sis.n-able.com_/the Microsoft update cloud.

   Alternatively, when Probe patch caching is enabled, the Windows Agent requests the required patch files from the probe. The probe then downloads the files directly from sis.n-able.com or the Microsoft update cloud.
6. The Windows Agent applies the schedule for installing updates.

Direct patch data submission

The Windows Agent sends monitoring and asset data to the N-able N-central server. However, this is not the only data submission path. Some devices can send patch data directly to our N-able cloud-based patch metadata service.

Devices selected for direct patch submissions must

- Have access to the internet.
- Connect to SIS (sis.n-able.com), the N-able Software Information Service.
- Reach AWS endpoints (*.amazonaws.com) to communicate with cloud-hosted services.

Direct patch data submission allows devices to retrieve patch metadata efficiently and optimize patch management processes through cloud connectivity.

Device Management for Apple

Device Management for Apple (DMA) is N-sight RMM's mobile device management (MDM) solution. MDM solutions are supported by Apple devices, Mac computers, iPhones, iPad tablets, and even Apple TVs, to configure devices securely and remotely.

Using Device Management for Apple, you can securely and remotely configure your Apple devices by sending configuration profiles, commands, and apps to them directly from N-sight RMM.

Device Management for Apple also supports Apple's enhanced macOS security framework to ensure our applications continue functioning with minimal user intervention.

> Device Management for Apple requires Mac Agent 3.4.0 or later. Device Management for Apple requires Mac Monitoring Agent 1.2.0 or higher.
>
> Enrollment of Virtual Machines (VMs) in Device Management for Apple is not tested or supported.

This section includes the following topics:

- Requirements for DMA
- Quick Start Guide for DMA
- Apple Push Notification service certificates
- Automated Device Enrollment
- Manual device enrollment
- Configuration profiles
- Device management
- App management

(missing or bad snippet)

macOS security framework

macOS 10.13.2 or later, includes user data protections, which are managed by Apple's expanded security framework, Transparency Consent and Control (TCC), that prevent third-party applications from unauthorized interaction with the computer. Organizations can use mobile device management solutions to remotely manage these security preferences with Apple's Privacy Preferences Policy Control (PPPC) payload.

These enhanced Apple security changes have the following implications for our applications:

- The security and privacy control settings defaulted to blocked. This forced end users to grant the required permissions for our applications to access the computer.
- These privacy and security settings are not always remotely configurable through a remote assistance tool so end users must approve each request. The number of request notifications and configuration requirements can be daunting to end users. For example, the numerous requests from new software installations or requests for re-authorization on previously permitted applications after an Operating System update can be overwhelming to end users.
- If end users do not grant the required permissions, Device Management for Apple may not run or they may run but with restricted functions.

To reduce the impact of these implications on our applications, we use our Device Management for Apple MDM solution to reduce the volume of end user notifications from our software and ensure all our installed applications have the required permissions.

Antivirus and Anti-malware

Security Manager is a fully integrated Antivirus/Anti-Malware engine designed to provide comprehensive protection to Windows Servers and Workstations. More information on this feature can be found in the N-able N-central Online Help.

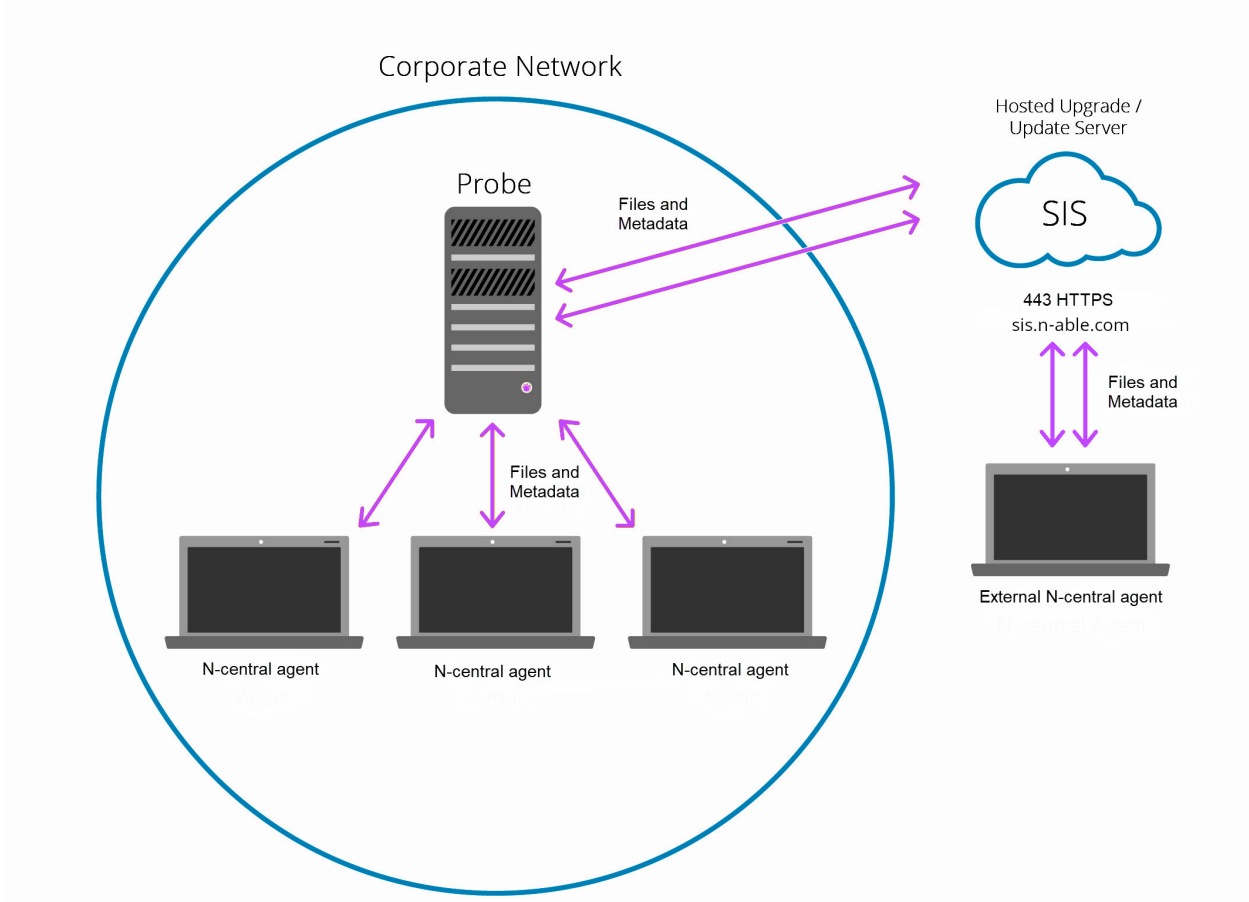
The security features of N-able N-central provide flexible deployment and updates without posing undue load on the service provider or end user networks. This is achieved through a distributed update architecture. This architecture is outlined below, and consists of the N-able N-central server, Agents, Probes, and an N-able hosted update server.

Upgrades and Updates

Bitdefender software supports three categories of upgrades and updates:

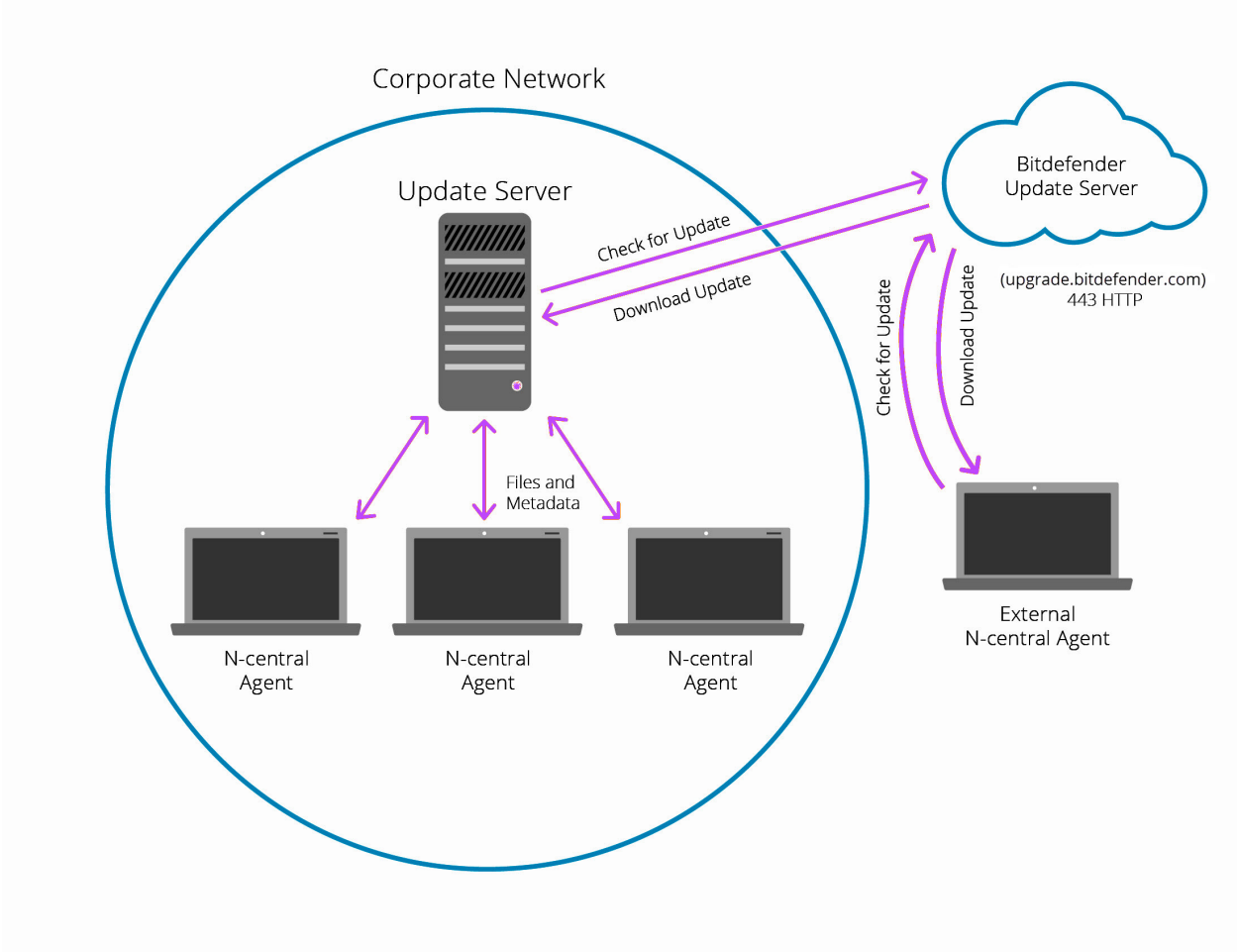
Product Upgrades (Major Releases)

- The Agent will attempt to download the catalog file from sis.n-able.com every time that is specified in the Maintenance Windows usually every hour.
- If an upgrade is available, the AV Defender Status service will transition to a Warning state to indicate that an upgrade is available.
- AV Defender will download from the probe of and apply the upgrades as defined by the maintenance Window or when configured to do so from the **All Devices View** > **Upgrade Monitoring Software**. Re-starting devices is usually needed following a product upgrade and the AV Defender Status service will indicate that a restart is required and the Agent will initiate the restart once it is permitted by the Maintenance Window.

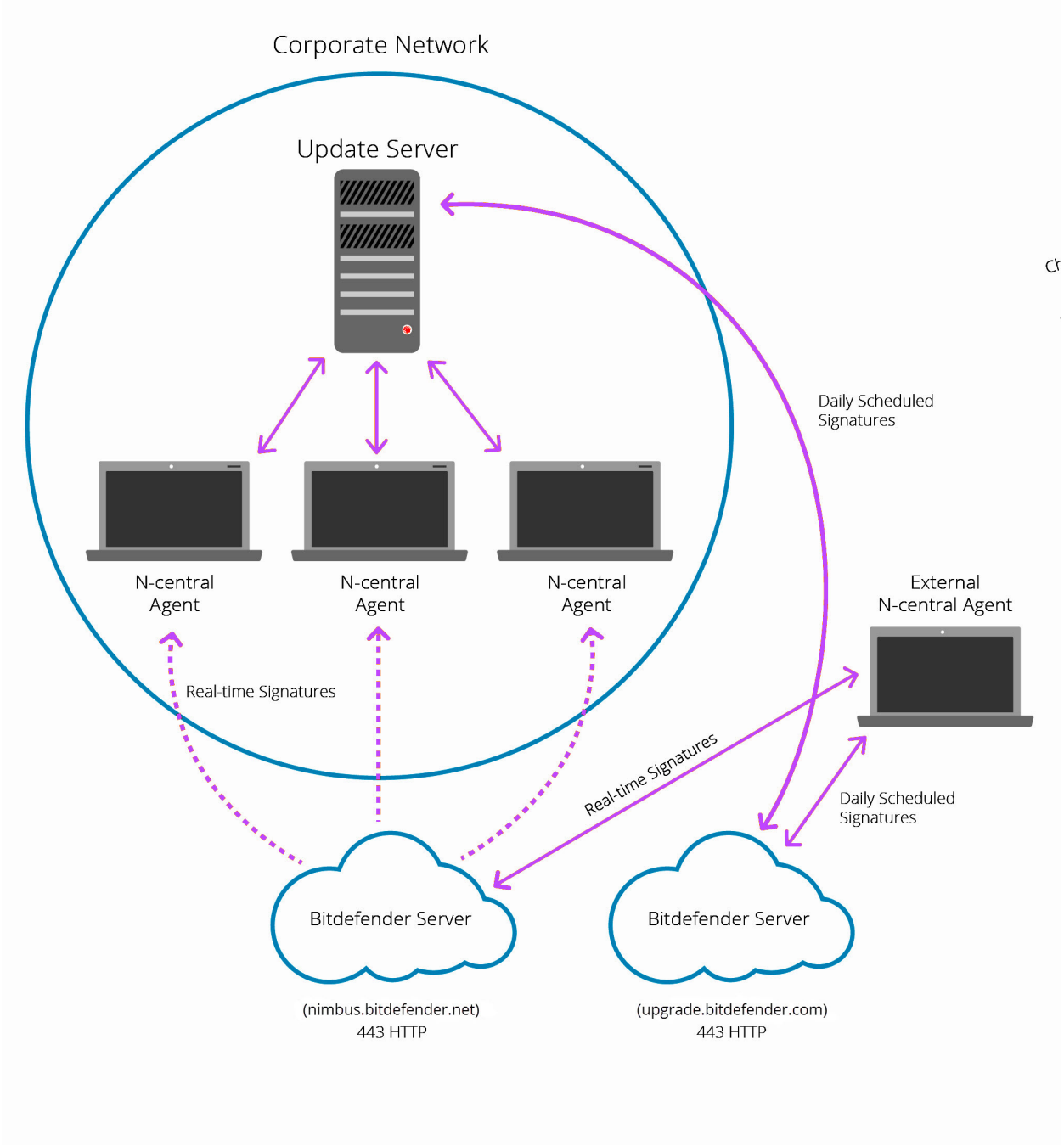


Product Updates (Hot Fixes)

1. AV Defender checks the local Update Server for updates.
2. The Update Server checks upgrade.bitdefender.com for updates every half hour.
3. Agents outside of the corporate network checks upgrade.bitdefender.com directly for updates.
4. AV Defender Status service will transition to a Warning state.
5. The update is downloaded from the Update Server or upgrade.bitdefender.com.
6. AV Defender updates are installed by the Maintenance Windows or manually.



Definition File Updates (Security Signatures)



Ensuring that definition files are up to date is a critical aspect of managing AV Defender. Again, N-able N-central leverages a distributed architecture to make distribution of these files fast and efficient.

- AV Defender Profiles in N-central allow the user to configure the update frequency as well as the failover behavior.
- Local Update Servers check for updates from the Bitdefender Update Server (upgrade.bitdefender.com) on a specific schedule.
- Definition File Updates are downloaded from the Update Server if available or directly from Bitdefender all using port 443.

- If an update server is configured for a Customer or Site, then AV Defender will use the local update server. If no update servers are selected, the AV Defender Status service will transition to a Warning state.
- If the Allow Failover to External Update Server property is enabled and Immediately is selected, AV Defender will obtain Definition file updates from upgrade.bitdefender.com.
- If the Allow Failover to External Update Server property is enabled and After <x> Hours is selected, AV Defender will then try to obtain updates from local update servers after every configured interval period has ended. If it is unable to check for updates for the configured number of hours, it will obtain the next update directly from the Bitdefender update server using port 443.

N-able Login

N-able Login provides centralized identity and authentication services for N-central and the N-able ecosystem. It enforces consistent access controls, authentication standards, and session management across products, reducing credential sprawl and identity-based attack surfaces. By centralizing authentication, N-able Login establishes identity as a core security control within the N-central architecture.

Centralized Single Sign-On Using Open Standards

N-able Login provides a centralized single sign-on service for N-able products. The service uses OAuth 2.0 and OpenID Connect to enable token-based authentication across applications.

N-able Login relies on established open standards to apply consistent cryptographic handling of credentials and authentication tokens. After successful authentication, users access supported N-able applications, including N-central, N-sight, and Cove, without repeated credential entry. This approach reduces the number of active credentials and authentication events, which helps limit exposure to credential compromise.

Centralized authentication allows N-able to enforce access policies consistently across products. When N-able Login disables a user account, the service blocks access to all integrated N-able services. N-able hosts the service on AWS with a multi-region architecture and replicated data stores, which supports availability and ensures that access changes propagate across regions in a controlled manner.

Multi-Factor Authentication Enforcement

N-able Login enforces multi-factor authentication for all users. The authentication process requires a password and a secondary factor, such as a time-based one-time password from an authenticator application or a supported hardware token.

The platform enforces multi-factor authentication at the service level and does not permit users to bypass it. Recent updates require users to complete an approved recovery process before modifying authentication factors. This enforcement reduces the risk of account compromise when attackers obtain passwords through phishing or other credential theft techniques.

N-able Login supports standard authenticator applications and implements recovery workflows with administrative oversight. These controls maintain account security while supporting operational recovery needs.

Federated Authentication with Microsoft Entra ID

N-able Login supports federated authentication with Microsoft Entra ID for organizations that manage identities through Microsoft directory services.

When administrators configure federation, N-able Login redirects authentication requests to the organization's Entra ID tenant using OpenID Connect. Users with an active Microsoft session authenticate without re-entering credentials. Users without an active session complete the organization's standard sign-in process, which may include multi-factor authentication and Conditional Access policies.

Federated authentication allows organizations to apply existing identity governance and security controls when users access N-able services. N-able does not store corporate passwords for federated users and validates signed identity tokens issued by Entra ID. This design limits credential duplication and reduces exposure in the event of a security incident.

Federation also supports user lifecycle management. When an organization disables a user account in Entra ID, the user loses access to N-able services accordingly. N-able Login supports SCIM 2.0 provisioning to synchronize user creation, updates, and deactivation between directory services and N-able systems.

Hardened Authentication Flows and Session Security

N-able Login applies multiple controls to protect authentication workflows and active sessions. For non-federated accounts, the service stores passwords using one-way hashing with salting. The platform enforces rate limiting and temporary account lockouts to reduce the likelihood of brute-force attacks.

The service uses centralized session management with back-channel logout support. When a user signs out or an administrator revokes access, N-able Login terminates active sessions across integrated products. Server-side session tokens ensure that logout and revocation events invalidate sessions immediately rather than relying solely on token expiration.

N-able Login encrypts all communication between N-able products and the authentication service using TLS. The platform issues signed OAuth and OpenID Connect tokens with defined scopes and audience restrictions to limit token reuse. The service supports modern authorization flows, including authorization code flow with PKCE, and does not allow legacy authentication protocols.

N-able operates N-able Login within a hardened AWS environment that uses network segmentation and a multi-region active architecture. The service falls within N-able's ISO 27001 certified scope. N-able conducts regular security assessments, including penetration testing of authentication and federation flows.

Compliance and Standards Alignment

N-able Login operates within N-able's information security management framework and aligns with recognized security standards. N-able maintains ISO 27001 certification, which governs risk management, access control, incident response, and audit practices applicable to the service.

N-able has implemented controls that support SOC 2 requirements, including mechanisms that propagate user deprovisioning events across dependent systems. These controls support customer requirements for access governance and security oversight.

These certifications and controls enable customers, including those in regulated industries, to incorporate N-able Login into their environments with supporting audit documentation available upon request.

Scheduled Tasks

N-able N-central can create Scheduled Tasks for Windows devices. This feature enables administrators to create tasks that remotely install software, execute scripts, copy files, and perform other actions.

Scheduled Tasks are executed with the permissions used by the executing software (Agent or Probe). Agents use Agent credentials provided during discovery (or set individually on the **Properties** tab of the device) while the Probe typically uses domain administrator permissions.

Security Implications

Using N-able N-central involves several components that may interact with existing security policies and systems. Organizations should assess these elements to ensure alignment with established controls and compliance requirements.

Report Manager Integration

The following ports will need to be accessible to use Report Manager with N-able N-central:

Port Number	Port Location				Description
	N-able N-central Server		Report Manager Server		
	Inbound	Outbound	Inbound	Outbound	
80	√	√	√	√	Communication between N-able N-central and Report Manager. Port 80 must be available from the Internet to the Report Manager server to view reports.
443	√	√	√	√	Optionally used for N-able N-central to Report Manager communication. Optionally used to view reports on the Report Manager server.
1433		√	√		SQL port used to send data from N-able N-central to Report Manager.

LDAP Integration

N-able N-central will need access to the following ports to integrate LDAP to query Active Directory:

Port Number	Port Location				Description
	N-able N-central Server		Active Directory Server		
	Inbound	Outbound	Inbound	Outbound	
389		√	√		Port 389 must be

Port Number	Port Location				Description
	N-able N-central Server		Active Directory Server		
	Inbound	Outbound	Inbound	Outbound	
					available from the Internet to the Active Directory Server to query AD. Unencrypted.
636		√	√		Optionally used for N-able N-central to query AD. Encrypted (SSL).

Other Security Features and Integrations

N-able N-central provides a strong set of built-in security capabilities. Many MSPs and IT Pros want to enhance their overall security by integrating other tools and services. This section outlines additional security features and integrations that are commonly deployed alongside N-central to meet advanced operational, compliance, or customer-specific security requirements. These complementary solutions extend the platform's native capabilities and support defense-in-depth strategies across diverse IT environments:

Cove Data Protection

Endpoint Detection and Response

Analytics

Cove Data Protection

Cove Data Protection, developed by N-able, is a cloud-native backup and disaster recovery platform built for modern IT environments. It supports file-level and image-based backups for Windows servers and workstations, as well as Microsoft 365 data (including Exchange, OneDrive, and SharePoint). Unlike traditional on-premises solutions, Cove leverages encrypted, multi-tenant cloud storage and a centralized web-based console, enabling streamlined deployment, policy management, and recovery operations at scale.

Key features include block-level, incremental-forever backups, AES-256 encryption in transit and at rest, built-in ransomware detection, and bare-metal recovery capabilities. Cove also supports data seeding, retention customization, and fast restore options—making it a flexible choice for MSPs and IT teams managing distributed environments.

Authorization (Access Control)

Cove Data Protection ensures that only authorized users, systems, and processes can access data. All access requests are verified through a secure authorization process. Access is granted based on predefined user roles—Admin, User, or Guest—using Role-Based Access Control (RBAC).

To protect against unauthorized access, Cove enforces Multi-Factor Authentication (MFA) or mandatory Two-Factor Authentication (2FA). This adds a critical layer of security beyond passwords. Our password policy applies across all systems and enforces best practices. All user actions are both authenticated and authorized.

Secure communication

A Zero Trust Security model emphasizes authentication, least-privilege access, and continuous monitoring. All data backups in Cove are encrypted with AES-256 and securely transferred over TLS 1.2 to our global cloud data centers.

To protect against online threats, Cove uses Cloudflare as its Web Application Firewall (WAF). This service defends against DDoS attacks, malicious bots, and complex application-layer threats while maintaining system performance and availability.

Encryption key/passphrase handling

Data is encrypted at the source on the client side before being transmitted to the cloud. The encryption key is created during installation, whether self-managed or assisted. Cove uses AES-256 encryption for all backups (Backup Manager version 17.5+).

To install the backup agent, a one-time passphrase is required. This passphrase is generated by a Security Officer, is valid for 24 hours, and is used only once, adding another layer of access control.

Cyber resilience

Cove helps Managed Service Providers (MSPs) prepare for, respond to, and recover from cyber threats with minimal disruption. Our cyber resilience strategy supports business continuity by reducing the risk of financial loss and reputational damage.

The Cove cybersecurity framework provides a structured approach to building customized response plans that address the specific needs of each MSP.

Incident response

The Cove Incident Response Plan (IRP) is designed to help MSPs and IT Pros quickly detect, respond to, and recover from cybersecurity incidents. The plan minimizes damage by guiding MSPs and IT Pros through detection, containment, recovery, and post-incident review—helping protect data and reduce recovery costs.

Immutable copies

Cove offers Immutable Fortified Copies that safeguard backup data from ransomware and unauthorized deletion. These are read-only backups of servers, workstations, and Microsoft 365 data that cannot be altered, deleted, or accessed externally, including through APIs. This ensures reliable data recovery in the event of a cyberattack.

Threat Modeling

Cove threat modeling enables teams to communicate the security design of systems and evaluate those designs for potential vulnerabilities. This process follows a proven methodology to identify risks, recommend mitigations, and manage security improvements. Teams complete threat models for any major system change and whenever they request a penetration test.

Penetration Testing

Cove Data Protection undergoes an annual external penetration test conducted by a certified third-party provider. Internal teams also perform regular security audits to ensure compliance with industry standards. In addition, the organization conducts network penetration tests annually or after implementing significant infrastructure changes.

Endpoint Detection and Response

In N-able N-central, EDR (Endpoint Detection and Response) provides advanced endpoint protection by integrating with SentinelOne's EDR technology, offering real-time threat prevention, detection, and response capabilities. This integration enhances security beyond traditional antivirus by leveraging AI-driven threat intelligence and behavioral analysis.

Endpoint Detection and Response (EDR) is a cybersecurity solution focused on:

- Detecting suspicious behavior at the endpoint level
- Providing detailed forensics
- Allowing automated and manual responses to threats

Through its partnership with SentinelOne, N-central brings powerful EDR tools directly into its RMM (Remote Monitoring and Management) platform.

Key capabilities

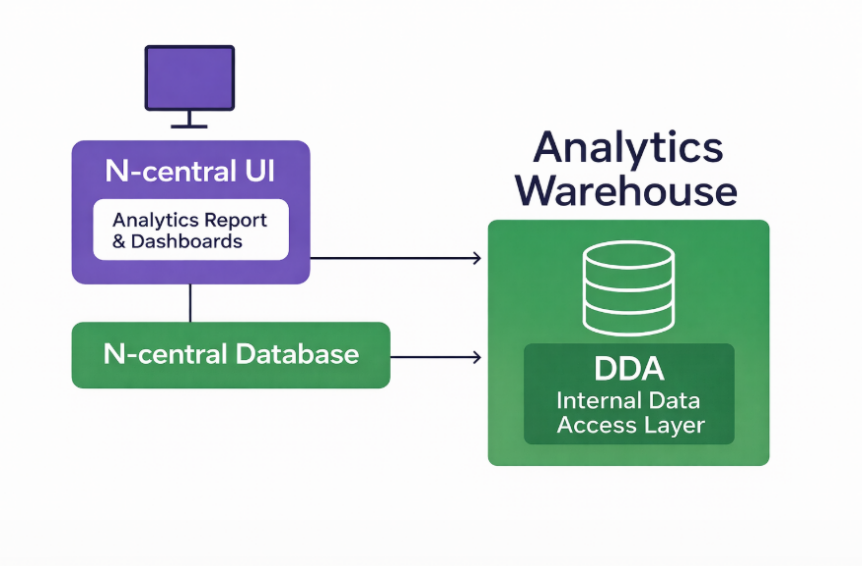
- **Behavior-Based Threat Detection** EDR identifies both known and unknown threats, including malware, ransomware, fileless attacks, and exploits. It relies on machine learning and behavioral analysis to detect malicious activity without depending solely on signatures.
- **Automated Remediation & Rollback** When a threat is found, EDR can automatically quarantine it, kill malicious processes, and roll back system changes made by ransomware (on supported Windows devices with Volume Shadow Copies enabled).
- **Real-Time Alerts and Dashboards** Alerts appear directly within the N-central interface, offering a detailed view of each incident, including type, scope, and affected systems.
- **Deep Forensics and Timeline Analysis** Security teams gain access to a detailed attack timeline that visualizes how threats entered and propagated, helping with root-cause analysis and compliance audits.
- **Cross-Platform Protection** EDR supports endpoints running Windows, macOS, and Linux. Deployment and management are handled through the N-central platform.
- **Policy-Based Management** Administrators can define EDR settings such as detection sensitivity, response automation, update cadence, and alerting—all from within N-central's policy engine.

Analytics

N-central uses a dedicated, cloud-based architecture to protect operational data throughout its lifecycle. This architecture governs how Analytics collects data from N-central, how it transmits and stores that data, and how it enforces encryption, tenant isolation, access control, and data residency requirements.

Analytics processes data on a scheduled basis and stores it in a centralized analytics environment designed for historical analysis and reporting. Because Analytics retains and aggregates data over time, it operates within the scope of the N-able security and compliance programs. These programs define the controls that protect Analytics data in transit and at rest, limit access to authorized personnel, and support regulatory and contractual obligations.

Here is how Analytics data flows out of N-central for reporting:

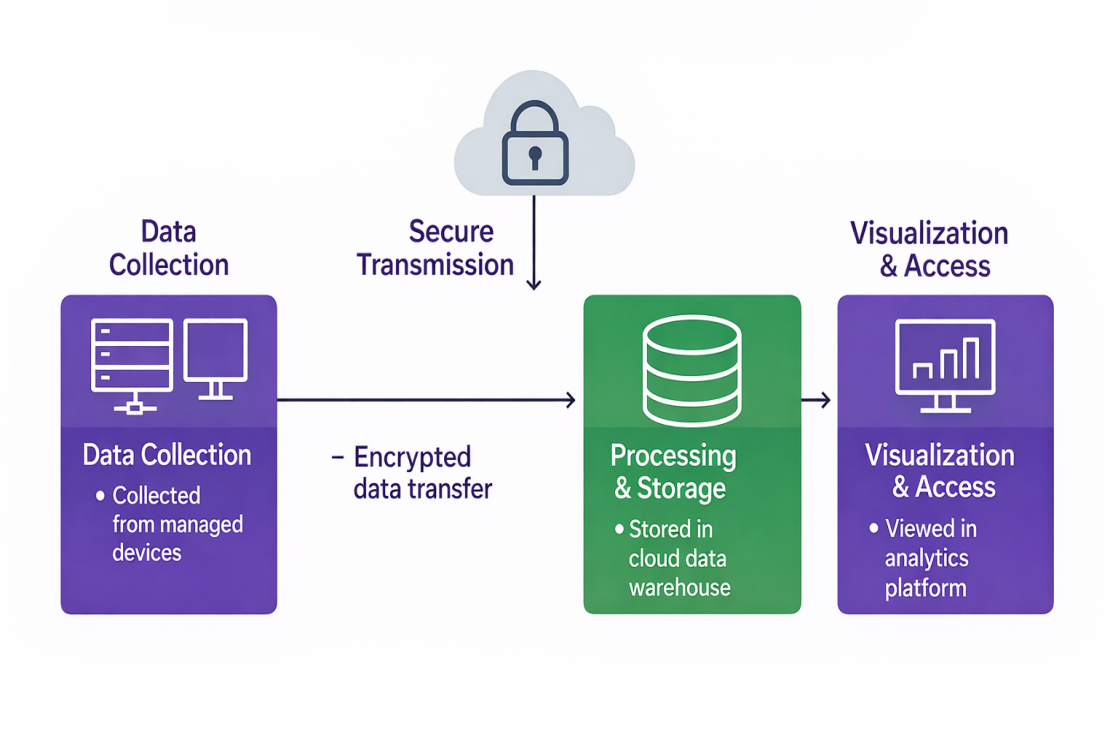


- N-central generates and stores live operational data in its primary database, which is optimized for running the product, not reporting.
- DDA provides a controlled way to extract and expose that data for Analytics, without direct reporting queries hitting the live database.
- The Analytics Warehouse stores, aggregates, and structures the data so it's suitable for historical analysis, dashboards, and reporting.
- The N-central UI pulls analytics data from the warehouse to display reports and dashboards, keeping analytics workloads separate from core product operations.

How Analytics Handles Data

N-central Analytics follows a secure, multi-stage data pipeline that collects, processes, stores, and visualizes operational data from managed devices.

This diagram illustrates how N-central Analytics collects operational data, transmits it securely, processes and stores it in a centralized analytics environment, and makes it available to authorized users. Security controls apply at each stage of the data lifecycle.



Data Collection

The N-central server collects device and operational data from managed environments using agents and probes. This data includes:

- Device attributes such as operating system, hardware manufacturer, CPU, and memory
- Installed services and applications
- Patch installation history and approval status
- Remote access and remote control activity

N-central does not collect sensitive information like personally identifiable information (PII).

Data Synchronization

The N-central server transmits collected data to the Analytics platform over encrypted channels. Data synchronization frequency depends on the Analytics subscription model:

- Free Analytics: Data synchronizes every 24 hours.
- Paid Analytics: Data synchronizes every 4 hours.

During initial onboarding, the first data export can take up to 24 hours, depending on the size of the N-central environment. After the initial export, data propagation across the Analytics can take up to approximately four hours before dashboards begin displaying results.

Data Processing and Storage

Analytics parses, transforms, and normalizes raw data before storage. This process ensures consistency across device types and monitoring sources and enables accurate analysis and comparison across environments.

Analytics stores processed data in a Snowflake data warehouse hosted on Amazon Web Services (AWS). Snowflake serves as the system of record for Analytics data and supports large-scale analytical queries and historical analysis.

Visualization and Reporting

Analytics uses Microsoft Power BI, hosted on Azure, to visualize data stored in Snowflake. Power BI renders dashboards, charts, and reports that allow users to:

- View aggregated metrics across customers or environments
- Filter and drill down into customer-specific or device-specific data
- Analyze historical trends for operational review and planning

Power BI processes each tenant's data within a dedicated workspace to ensure logical separation and access control.

Security Architecture

Analytics applies security controls at every stage of the data lifecycle.

Data Protection in Transit

Analytics encrypts all data transmitted between the on-premises N-central server and the Analytics platform using TLS 1.2. Encryption applies across the entire data path, from collection through ingestion and visualization.

Data Protection at Rest

Analytics protects data stored in Snowflake using an end-to-end encryption model based on AES-256 encryption. Snowflake encrypts all data by default and does not allow users to disable encryption.

Encryption controls include:

- A hierarchical key model backed by cloud-based hardware security modules (HSMs)
- Encryption of individual data elements using different keys
- Automatic key rotation every 30 days

Multi-Tenancy and Access Control

Analytics uses a multi-tenant architecture with strict logical isolation between tenants:

- Snowflake enforces row-level security to segregate tenant data.
- Power BI processes each tenant's data within a dedicated workspace.
- Analytics enforces a least-privilege access model. Only authorized N-able personnel approved to maintain and operate the solution can access Analytics data.

Data Residency

N-able meets data residency requirements by storing Analytics data in-region Snowflake data warehouses hosted on Amazon Web Services (AWS) infrastructure. Customers cannot select their data region; we assign them to a region based on their organization's location at onboarding. Data remains encrypted both in transit and at rest within the selected region

The following table lists the supported regions, AWS region codes, and physical data center locations for N-able Analytics data storage.

Supported Region	AWS Region Code	Physical AWS Region Location
US	us-west-2	Oregon, United States (AWS US West – Oregon)
EU-Central	eu-central-1	Frankfurt, Germany
EU-West	eu-west-1	Dublin, Ireland
APAC	ap-southeast-2	Sydney, Australia

N-able assigns data regions and does not offer flexibility in region selection. Organizations with specific jurisdictional requirements, such as Canadian partners seeking to avoid US storage or EU partners requiring EU residency for GDPR compliance, should review their assigned region before onboarding.

Compliance and Data Governance

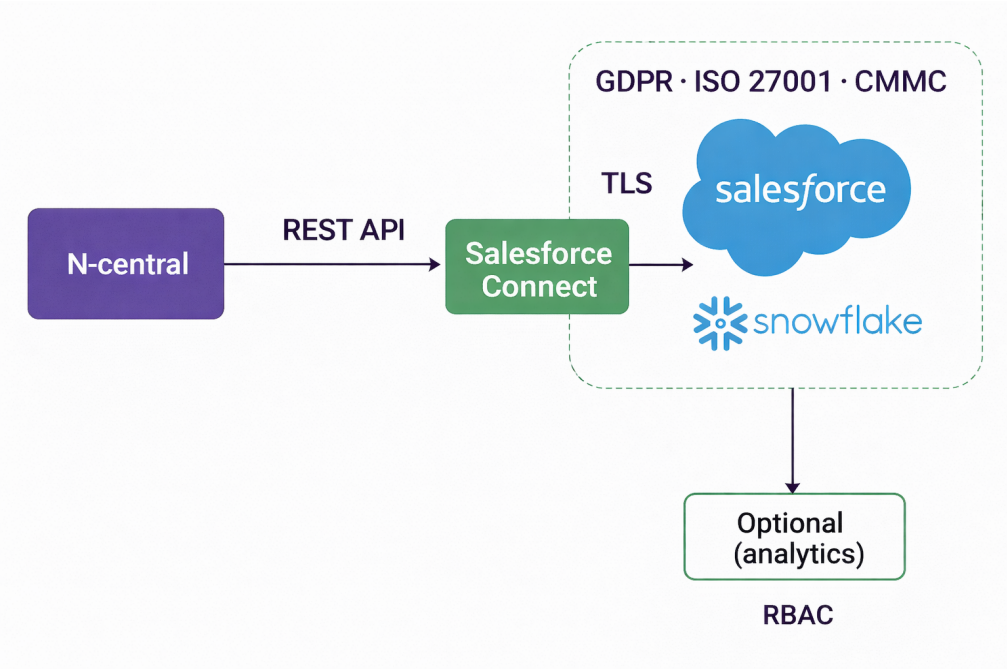
N-able holds ISO/IEC 27001 certification and maintains a formal information security management system. The organization is also progressing toward SOC 2 Type I certification.

All data, files, and information submitted or transmitted in connection with N-able services remain the property of the partner, as defined in the Software Services Agreement. The partner acts as the data controller, and N-able acts as the data processor.

Partners may export Analytics data using JDBC or ODBC connections. Upon termination of services, N-able deletes partner data in accordance with applicable regulatory requirements.

Optional Analytics Integration

Analytics also integrates with other systems, such as Salesforce, to provide controlled access to selected data. These integrations retrieve data on demand and do not store, process, or retain Analytics data. So they do not define the Analytics security posture or data governance model.



Conclusion

N-able N-central is a comprehensive RMM platform built with security, scalability, and flexibility at its core. It empowers MSPs and IT Pros to manage complex IT environments securely and efficiently. Through its layered security architecture, robust integrations, and proactive threat management, N-central ensures data protection, regulatory compliance, and operational resilience. The white paper serves as a guide for stakeholders to understand and implement best practices for secure IT service delivery.

Let Us Know What You Think

We're committed to continuous improvement, and your feedback helps us refine the clarity, depth, and relevance of our content.

If you have suggestions for enhancements to this document, need more detailed information, or have any other feedback, please let us know via our online feedback form.

Your insights and suggestions are invaluable.

Customer Support

Web Page:	https://www.n-able.com/
Technical Support Self- Service Portal:	https://me.n-able.com/
Phone:	Toll Free (U.S./CAN): 1-866-302-4689
	International: +800-6225-3000
	Local: (613) 592-6676, select option 2 for support

About N-able

N-able fuels IT services providers with powerful software solutions to monitor, manage, and secure their customers' systems, data, and networks. Built on a scalable platform, we offer secure infrastructure and tools to simplify complex ecosystems, as well as resources to navigate evolving IT needs. We help partners excel at every stage of growth, protect their customers, and expand their offerings with an ever-increasing, flexible portfolio of integrations from leading technology providers. n-able.com

The N-ABLE, and other N-able trademarks and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. and may be common law marks, are registered, or are pending registration with the U.S. Patent and Trademark Office and with other countries. All other trademarks mentioned herein are used for identification purposes only and are trademarks (and may be registered trademarks) of their respective companies.

©2026 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.