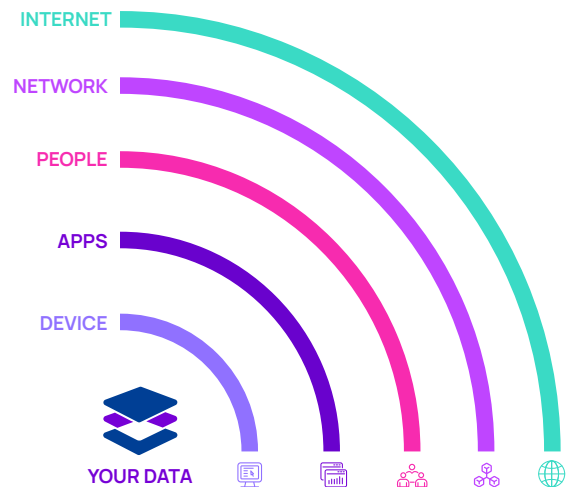


# N-able N-central Layered Security for IT Departments

Only N-able can provide a multi-layered approach to security that offers unparalleled protection and ease—all in one, simple dashboard. In addition to exceptional functionality, N-able provides industry expertise, training programs, and transformational business support that take security to the next level.

N-able delivers an impressive array of nine distinct core security capabilities to address all layers of their network and seven success capabilities to level up your business, team, and skills.



## Core Security Capabilities

- Patch management
- Endpoint Detection & Response (EDR)
- Vulnerability scanning
- Cloud-based email security
- Security manager & disk encryption
- Managed antivirus
- Password management
- Backup
- Monitoring
- Web security

## Success Capabilities

- Industry experts
- Consumer success
- World-class, 24/7 support
- Detailed training
- Automation Cookbook
- Active community
- Product feedback channels

Data is your most important asset; it's the prize most cybercriminals pursue. When you implement security technology at each layer, you're creating multiple lines of defense to protect that prize. Attackers go after data with a myriad of goals in mind. They may want to destroy the data, encrypt it, hold it for ransom, or steal it and resell it on the dark web. In every case, data is the target.

A multi-layered approach to security works to stop the attack at the outermost level—as far away from the data as possible. For example, blocking a malicious email will prevent a potential ransomware attack from even entering the network. Stopping an attack there is safer than catching it at the device level when it's already begun encrypting files.

What follows is an overview of N-able layered security capabilities, which protect data at multiple levels.

## Endpoint Detection and Response (EDR)

N-able™ Endpoint Detection and Response (EDR) provides frontline technicians with the ability to detect the latest malware—including ransomware—and to investigate and remediate any damage caused. That includes restoring endpoints to their healthy states and completing a threat incident response in just minutes, not hours.

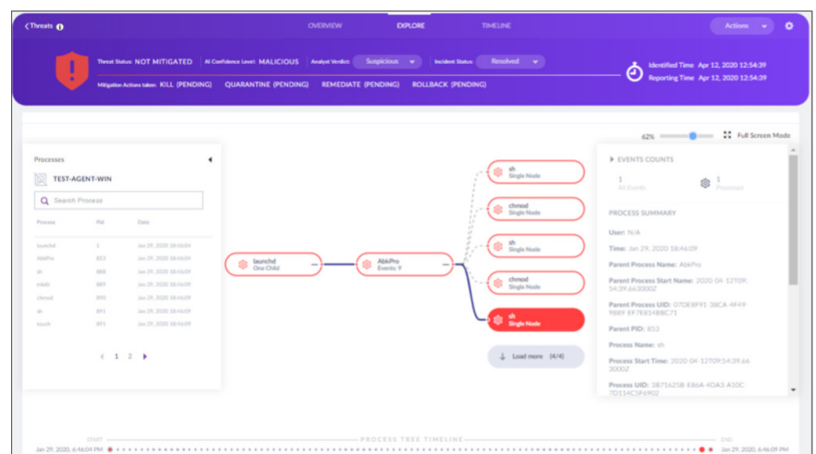
EDR is an integrated threat management software powered by SentinelOne. Combining N-central with SentinelOne's endpoint protection, EDR enables Windows devices to self-defend and heal themselves by stopping processes, quarantining the affected area, fixing any damage, and rolling back events to keep devices secure.

EDR uses process behavior to monitor multiple processes to recognize attacks as they develop and respond at machine speed. This is different from signature-based detection from traditional AV solutions, which monitor processes as they execute, in contrast to anticipating problems.



EDR provides forensic data to mitigate threats quickly, perform network isolation, and protect against newly discovered threats.

New features now integrated on N-central include the ability to deploy EDR agents, configure profiles, and monitor devices from the dashboard.

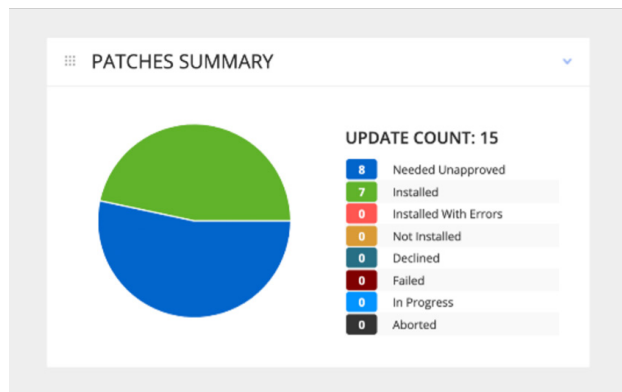
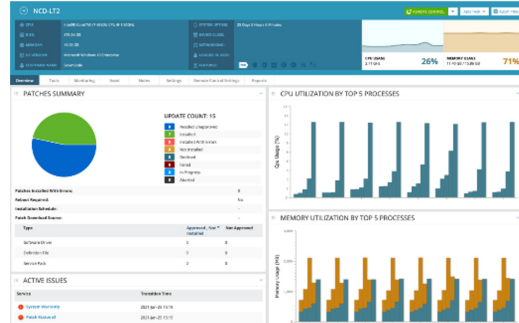


## Patch Management

Patch management gives IT managers complete granular control over when, how, and which patches are deployed across the network, devices, or groups. Patch management through N-central® also allows protection of multiple operating systems and third-party applications at once.

**N-able™ N-central Patch Management provides administrators with the tools they need, including:**

- Designate a site concentrator (Optional)
- Enable and apply patch management policies
- Custom patch management policies
- View detailed patch information, including reports
- Manage patches on individual or multiple devices
- Reprocess failed patches
- Take patch approval actions
- Uninstall Microsoft patches
- Schedule patches
- Supported applications
- Manually re-run the patch status check
- Create a patch approval lifecycle and patch identification workflows

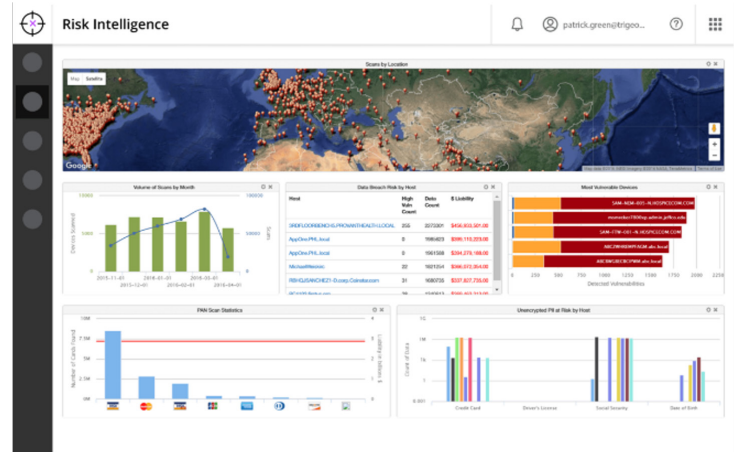


This not only allows the productivity enhancements required to effectively manage applications security, but also features easy-to-use tools for sophisticated security processes without the need for specialized security training, freeing up resources to focus on the core business.

## Vulnerability Scanning & Risk Intelligence

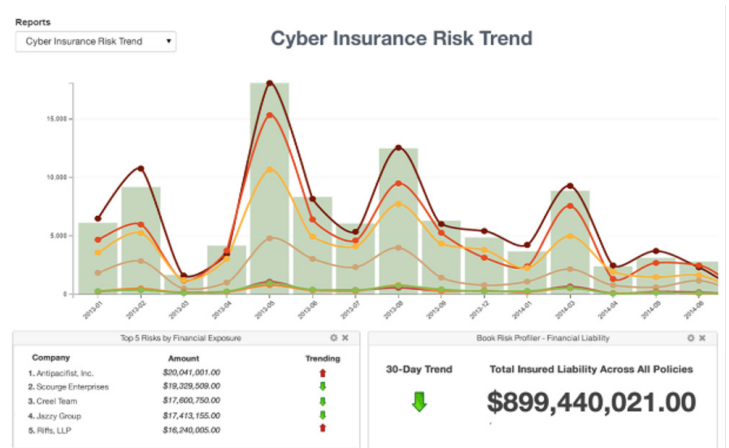
Designed to identify potential misconfiguration or open ports on the network, as well as provide historical reporting, together, these elements allow IT departments to show security progress over time.

While the N-central platform includes device network, fast reporting, and detecting and remediating patches, true risk and compliance assessments are additional, key safeguards that satisfy regulation requirements.



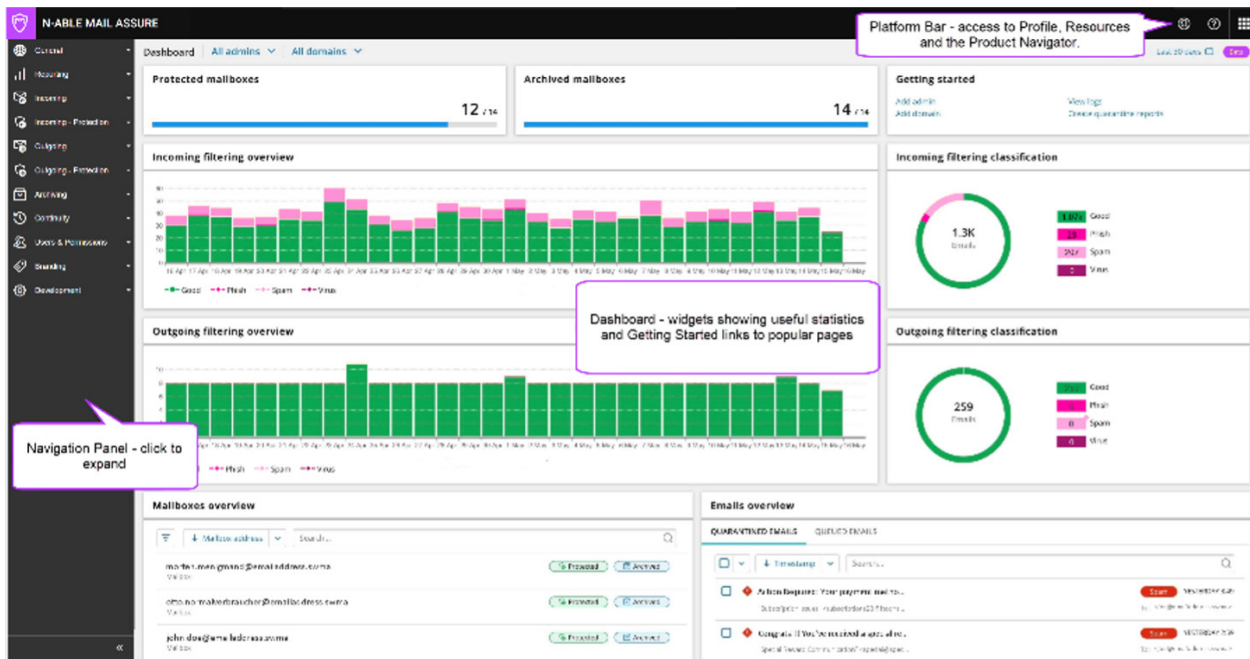
**N able™ Risk Intelligence locates sensitive and at-risk data across your managed networks and workstations, revealing how much a data breach might cost, providing:**

- Deep vulnerability scanning
- Brandable reports detailing the financial impact of risks
- Identification of inappropriate user access
- PCI, DSS, PAN, and PII scans
- At-risk data discovery
- Risk-trending reports to show improvement



The network port details report displays the listening TCP/IP ports on your system, indicating that a service is listening for external communication from a remote computer. The details report makes threats easy to see, in real time.

## Cloud-based email security



Email still matters. Even with a primary layer of security, such as the inclusions with Microsoft 365™, Mail Assure provides more control and another level of defense built to protect against spam, viruses, malware, phishing, ransomware, and other email-borne threats while protecting data with cloud-based archiving.

### N-able™ Mail Assure solution provides a host of key email security features that protect the most-targeted layer of your network:

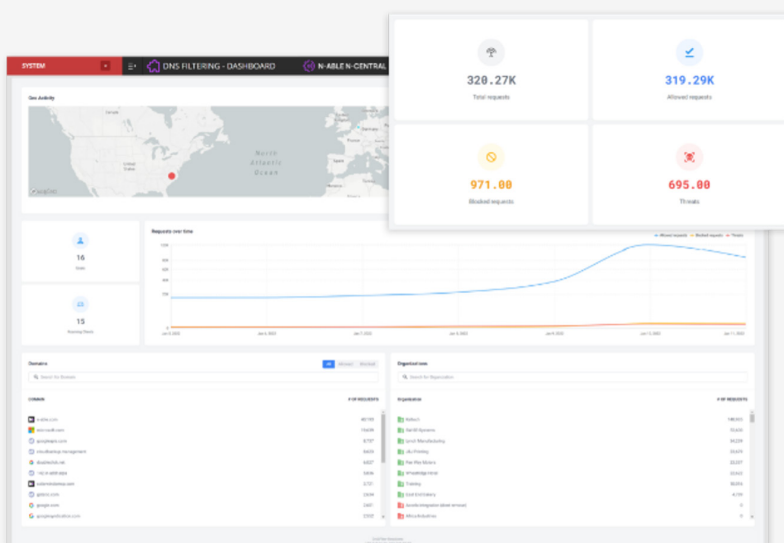
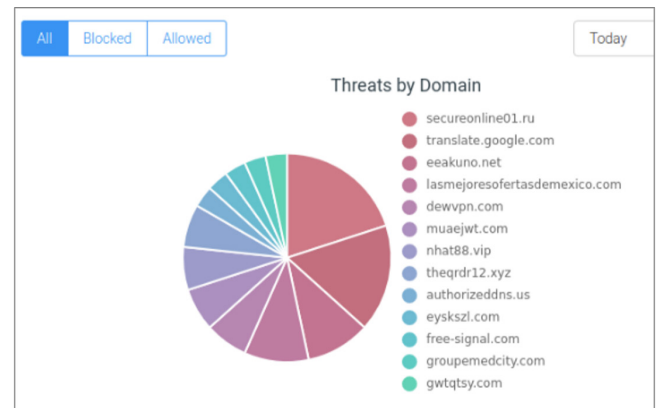
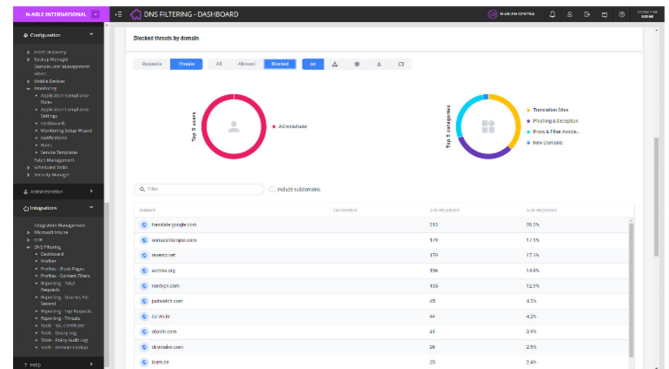
- Email security for inbound and outbound email
- Intelligent protection and filtering engine that prevents known and emerging threats
- Easy setup, add domains, and change MX records
- Web interface for both admins and end users
- Quarantine management for view, release, remove, block, or approve
- Mailbox auto-detection via SMTP or LDAP sync
- Advanced filtering statistics
- Extension and attachment blocking management
- SSL/TLS traffic encryption
- Smart host deployment for outbound email filtering
- DKIM signatures for outgoing emails to help ensure sender authenticity
- Built-in 24/7 email continuity
- Web-based access to archived and quarantined emails
- Send and receive email directly from the Mail Assure dashboard

## Web Security

Web security is critical to keep any business safe, especially with the evolution of the mobile workforce. Web database and DNS-based filtering keeps businesses, staff, and their data safe both on and off the network.

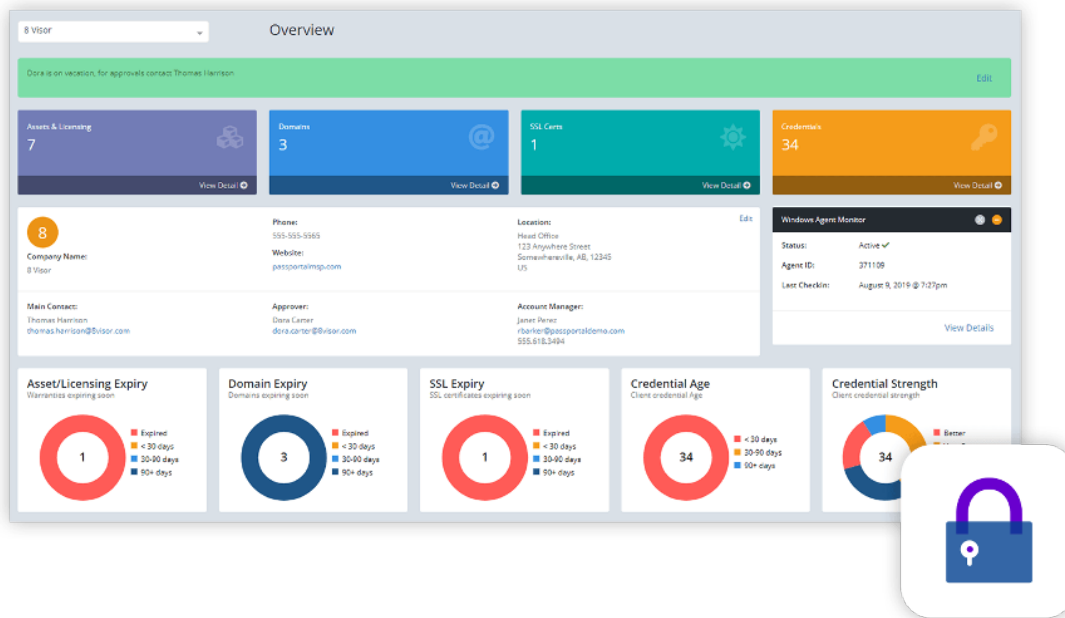
Thousands of harmful websites are created each day and malicious advertising, phishing sites, and other security threats can bypass legacy web filters. N-able™ DNS Filtering offers stronger protection, greater network visibility, and user-based reporting from within the N-central® dashboard.

Plus, the N-able product uses smart threat protection to recognize and block malicious websites in real time—before they can impact your customers and their users. Protect them both on and off network with the DNS Filtering solution. It's fully cloud-based, allowing for faster scalability and peace of mind.

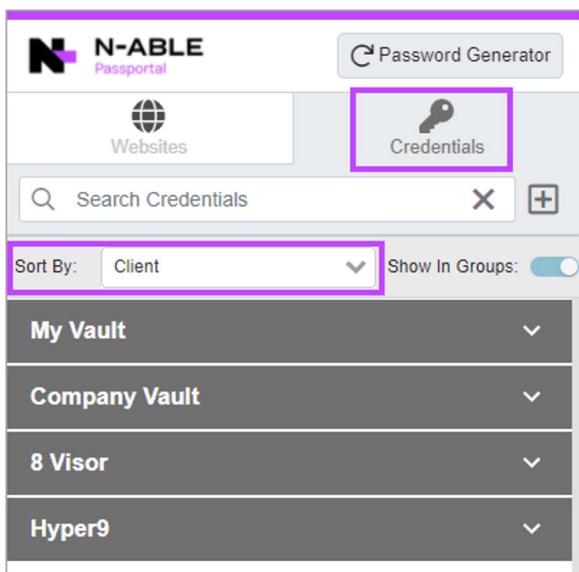


- Prevent access to unwanted and malicious content
- Block phishing, virus, zero-day, and other cyberthreats
- Smart identification of malicious domains—typically 80 hours faster than many other solutions
- Redundant and reliable anycast network: 50 data centers
- Comprehensive reports by location or user
- Visualize network activity, network traffic, and security
- Expose security weaknesses with DNS activity logs
- Create policies by group, device, or network
- Redirect users to a custom blocked page
- Block previously uncategorized phishing threats with imagery-based, anti-phishing tactics
- Mitigate botnet, malicious crypto mining, and malware threats via threat feed augmentation

## Password Management



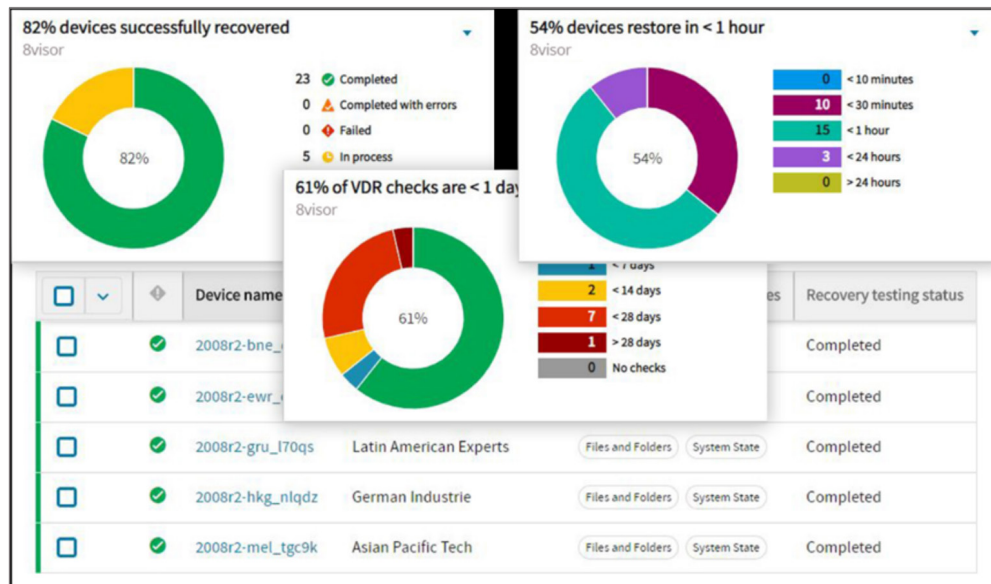
Password management allows IT managers to implement rules to generate strong passwords, eliminate re-use, and automate password rotation and routine maintenance. Encrypt, store, manage, and retrieve credentials quickly and safely, while minimizing password risks.



**N-able™ Passport** is a cloud-based platform that offers simple, secure password and documentation management tailored to your operations. Passport uses automated password protection that makes storing, managing, and retrieving passwords and department knowledge quick and easy from virtually any connected device. With credential injection that ensures fast, seamless, and secure connectivity to user devices, networks, and applications, Passport is designed to streamline the technician's day. Finally, it allows you to easily adopt and demonstrate best-practice password management workflows.



## Backup



Businesses require not only the fast, secure, hybrid architecture needed for all modern backup solutions, but also multi-storage and restoration capabilities that reduce the risk of an effective ransomware attack to nearly zero percent.

With N-able Backup you get multiple recovery options that leverage fast file and folder-level recovery as well as full-system recovery with bare-metal restore or virtual disaster recovery. Create a standby server with our continuous recovery option and recover at LAN speed via the Local Speed Vault option, if needed. Finally, test and verify backup recoverability on an automated schedule with recovery testing.

### N-able Backup includes the following from our world-class, compliant data centers worldwide:

- Support and backup of Microsoft 365
- No hardware requirements
- Automated backup deployment including profiles
- AES 256-bit encryption
- Custom private keys
- ISO-certified data centers
- Role-level access settings
- True delta technology with byte-level change tracking
- Deduplication and compression
- WAN Optimization

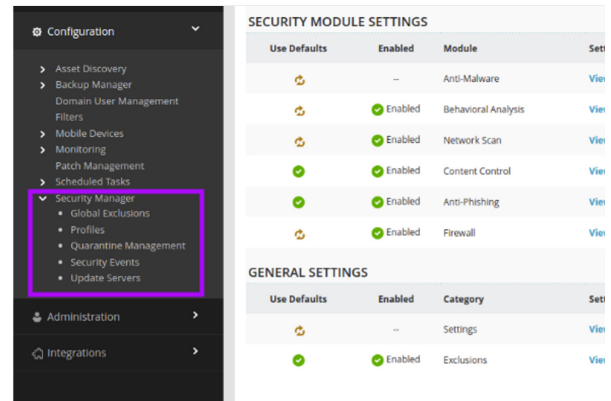
Country	HIPAA	ISO27001	ISO9001	NIST 800-53	PCI DSS	SOC 1 TYPE II	SOC 2 TYPE II
Australia		x			x	x	x
Belgium		x					
Brazil		x	x		x	x	x
Denmark		x			x	x	x
France		x	x		x	x	x
Germany		x	x		x	x	x
Italy		x	x		x	x	x
Netherlands		x	x		x	x	x
Norway		x	x				
Portugal		x	x		x	x	x
S. Africa			x				
Spain		x	x		x		
Sweden		x	x				
Switzerland		x	x		x	x	x
UK		x	x		x	x	x
Canada	x	x		x	x	x	x
USA	x	x		x	x	x	x

\*\* Other location-specific certifications exist, above table contains most requested



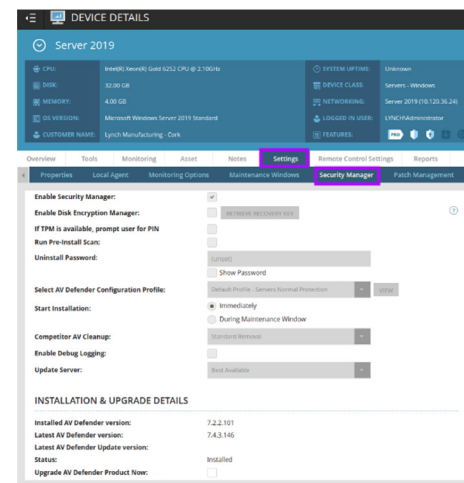
## Security Manager with Disk Encryption Management

To meet the needs of device-level protection, we developed a security manager solution that deploys, and can be managed, directly from the N-central dashboard. For businesses that don't yet require EDR, this solution can be tailored to meet your specific needs, with the option to permit end-user interactions like running scans and updating threat definitions. In addition, you can enable volume-level disk encryption to further protect your data.



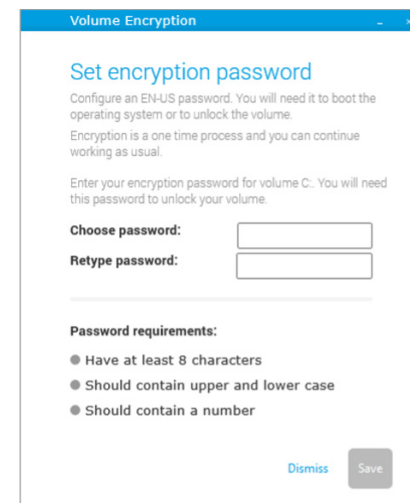
Disk encryption protects data against threats like theft or accidental loss by making information on hard drives unreadable to unauthorized users. Disk encryption is ideally suited to environments where data is a critical asset or governed by compliance regulations such as GDPR, PII, PCI DSS, and there's a risk of data loss.

N-able protection policies control every aspect of Security Manager. This includes scan schedules, remediation actions upon threat discovery, and end-user interactions. We've included default policies to get you started, as well as the option to create custom policies to meet your precise requirements.



Our engine and policies are provided by Bitdefender, a security industry leader whose policies are on both Windows and Mac installations. Plus, security manager settings supported by your computer's operating system are applied automatically.

N-able disk encryption leverages native BitLocker so you can take advantage of any existing encryption you may already have and start benefiting from our easy-to-manage recovery key system. Our encryption manager allows for multiple security options—trusted platform module, passwords, among others—for simple customization.



## Device Monitoring

Monitoring provides frontline techs, IT managers, and security specialists the real-time and historical trending to predict and seek out threats and attacks before they have a chance to escalate. Monitoring makes potential attacks visible and sends instant alerts about abnormal trends, which are critical early indicators.

Monitoring agents are specialized software that help keep workstations, servers, and networks up to date through continuous, 24/7 scanning. They alert IT support staff to potential problems and help keep malicious software off the monitored systems. These agents help ensure safety and reliability while keeping track of networks.

N-able device monitoring gives you the deep visibility to manage security correctly. It allows you to keep your networks healthy, do proactive maintenance and stay ahead of potential threats.

- Receive alerts about potential issues
- Patch and update software across your devices
- Schedule tasks, like updating and running antivirus, or performing daily backups
- Automate routine maintenance
- Windows, Mac, and Linux compatibility
- Advanced network monitoring and management for servers and workstations across multiple customer sites
- Alerts on issues like disk health, out-of-date antivirus, and service status
- Configuration profiles allow you to push out agents together, or in groups
- Secure connections and encrypted data transfers via HTTPS
- Network performance monitoring
- Discover, import, and monitor critical network devices using SNMP, such as firewalls, routers, printers, and switches
- Mobile device monitoring
- Virtual machine monitoring

Customer	Site	Remote Control	Tools	Device/Probe	Device Class
Keltech	--			SLS-0001	Workstation
Keltech	--			SLS-0002	Servers - VM
Keltech	--			HP-001	Servers - ES
Keltech	--			HP-002	Servers - ES
Lynch Manufacturing	--			CheckPoint S0300	Switch/Router
Lynch Manufacturing	--			CheckPoint S0300	Switch/Router
Lynch Manufacturing	--			CheckPoint S0300	Switch/Router
Lynch Manufacturing	--			CheckPoint S0300	Switch/Router
Lynch Manufacturing	--			HP-001	Servers - VM
Lynch Manufacturing	--			Infoblox - Trunk 821	Switch/Router
Lynch Manufacturing	--			Infoblox - Trunk 822	Switch/Router

Service	Status	Transition	Last Scan Time
Agent Status		2021-Dec-17 23:10	2022-Feb-09 19:57
CPU		2021-Dec-17 23:10	2022-Feb-09 19:29
Disk - C:		2021-Dec-17 23:10	2022-Feb-09 19:28
Disk - F:		2022-Feb-07 06:40	2022-Feb-09 19:50
EDR Status		2022-Feb-07 06:40	2022-Feb-09 19:59
Memory		2021-Dec-17 23:10	2022-Feb-09 19:29
N-able Backup Product Status		2022-Feb-08 06:41	2022-Feb-09 19:45
N-able Backup Status - Files and folders		2022-Jan-14 05:33	2022-Feb-09 19:46
N-able Backup Status - System State		2022-Feb-08 05:44	2022-Feb-09 19:46
N-able Backup Status - Total Backup		2022-Jan-14 05:33	2022-Feb-09 19:46

Customer	Site	Remote Control	Tools	Device Name	Agent Status	Application Compile	Backup Manager Status	Backup Manager Status	CPU
Keltech	--			SLS-0002		--	--	--	--
Keltech	--			SLS-0002		--	--	--	--
Lynch Manufa...	--			Mat - Catalina VM		--	--	--	--
Lynch Manufa...	--			SLS-0048		--	--	--	--
Lynch Manufa...	--			SLS-0049		--	--	--	--
Lynch Manufa...	Cork			SLS-0006		--	--	--	--
Maryborough ...	--			SLS-0083		--	--	--	--
Maryborough ...	--			Windows 11		--	--	--	--

## Layered Security Elements

### ENDPOINT DETECTION AND RESPONSE (EDR)

Provides frontline technicians with the ability to detect the latest malware—including ransomware—and to investigate and remediate any damage caused. That includes restoring endpoints to their healthy states, and completing a threat incident response in just minutes, not hours.

### PATCH MANAGEMENT

Patch management gives IT managers complete granular control over when, how, and which patches are deployed across the network, devices, or groups. Patch management through N-central also allows protection of multiple operating systems and third-party applications simultaneously.

### VULNERABILITY SCANNING

Designed to identify potential misconfiguration or open ports on the network as well as provide historical reporting. Together, these elements allow IT departments to show security progress over time.

### CLOUD-BASED EMAIL SECURITY

Email still matters. Even with a primary layer of security, such as the inclusions with Microsoft 365™, Mail Assure provides more control and another level of defense built to protect against spam, viruses, malware, phishing, ransomware, and other email-borne threats, while protecting data with cloud-based archiving.

### WEB SECURITY

Web security is critical to keep any business safe, especially with the evolution of the mobile workforce. Web database and DNS-based filtering keeps businesses, staff, and their data secure, both on and off the network.

### PASSWORD MANAGEMENT

Password management allows IT managers to implement rules to generate strong passwords, eliminate re-use, and automate password rotation and routine maintenance. Encrypt, store, manage, and retrieve credentials quickly and safely, while minimizing password risks.

### BACKUP

Businesses require not only the fast, secure, hybrid architecture needed for all modern backup solutions, but also multi-storage and restoration capabilities that reduce the risk of an effective ransomware attack to nearly zero percent.

### SECURITY MANAGER WITH DISK ENCRYPTION MANAGEMENT

To meet the needs of device-level protection, we developed a managed antivirus solution that deploys, and can be managed, directly from the dashboard. Plus, you can enable volume-level disk encryption to further protect your data.

### DEVICE MONITORING

Monitoring provides frontline techs, IT managers, and security specialists the real-time and historical trending to predict and seek out threats and attacks before they have a chance to escalate. Monitoring makes potential attacks visible and sends instant alerts about abnormal trends, which are critical early indicators.