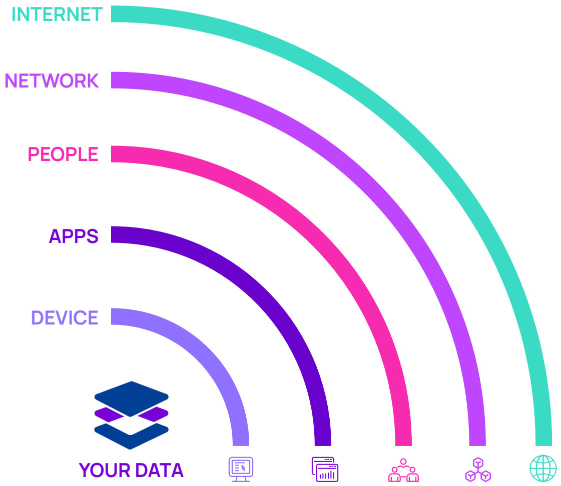
N-able RMM Layered Security for IT Departments

Only N-able can provide a multi-layered approach to security that offers unparalleled protection and exceptional ease—all in one, simple dashboard. In addition to unparalleled 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 ransomware, 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.

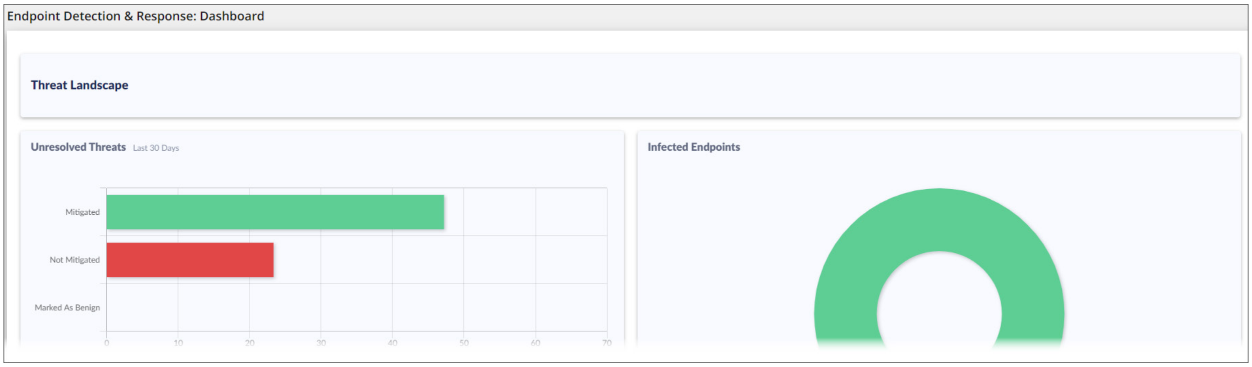
What follows is an overview of N-able layered security capabilities, which protect data at multiple levels:

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.

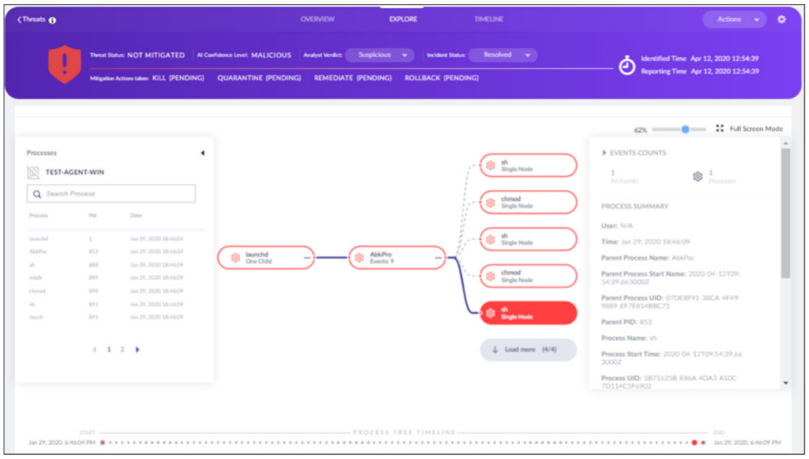
EDR is an integrated threat management software powered by SentinelOne. Combining N-able RMM with SentinelOne's endpoint protection, EDR enables Windows devices to self-defend and heal themselves by stopping processes, quarantining the affected area, fixing any damage, and rolling back events to keep 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-able RMM include the ability to deploy EDR agents, configure profiles, and monitor devices from the dashboard.



Threat Status: NOT MITIGATED | AI Confidence Level: MALICIOUS | Analyst Verdict: Suspicious | Incident Status: Resolved

Mitigation Actions taken: KILL (PENDING) QUARANTINE (PENDING) REMEDIATE (PENDING) ROLLBACK (PENDING)

Identified Time Apr 12, 2020 12:54:39
Reporting Time Apr 12, 2020 12:54:39

Process	Pid	Date
launchd	1	Jan 29, 2020 18:46:04
AbkPro	853	Jan 29, 2020 18:46:04
sh	888	Jan 29, 2020 18:46:09
mkdir	889	Jan 29, 2020 18:46:09
chmod	890	Jan 29, 2020 18:46:09
sh	891	Jan 29, 2020 18:46:09
touch	891	Jan 29, 2020 18:46:09

PROCESS SUMMARY

User: N/A

Time: Jan 29, 2020 18:46:09

Parent Process Name: AbkPro

Parent Process Start Name: 2020-04-12T09:54:39.663000Z

Parent Process UID: 07DEBF91-38CA-4F49-9889-EF7E814BBC71

Parent PID: 853

Process Name: sh

Process Start Time: 2020-04-12T09:54:39.663000Z

Process UID: 3B71625B-EB6A-4DA3-A10C-7D114C5F6902

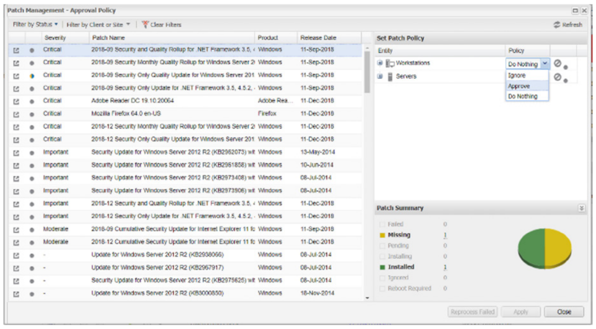
Jan 29, 2020, 6:46:04 PM

Jan 29, 2020, 6:46:09 PM

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-able RMM 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:



Patch Management - Approval Policy

Severity	Patch Name	Product	Release Date
Critical	2018-09 Security and Quality Rollup for .NET Framework 3.5, 4	Windows	11-Sep-2018
Critical	2018-09 Security Monthly Quality Rollup for Windows Server 2	Windows	11-Sep-2018
Critical	2018-09 Security Only Quality Update for Windows Server 201	Windows	11-Sep-2018
Critical	2018-09 Security Only Update for .NET Framework 3.5, 4.5.2, -	Windows	11-Sep-2018
Critical	Adobe Reader DC 19.10.20064	Adobe Rea...	11-Dec-2018
Critical	Mozilla Firefox 64.0 en-US	Firefox	11-Dec-2018
Critical	2018-12 Security Monthly Quality Rollup for Windows Server 2	Windows	11-Dec-2018
Critical	2018-12 Security Only Quality Update for Windows Server 201	Windows	11-Dec-2018
Important	Security Update for Windows Server 2012 R2 (KB2962073) wit	Windows	13-May-2014
Important	Security Update for Windows Server 2012 R2 (KB2961858) wit	Windows	10-Jun-2014
Important	Security Update for Windows Server 2012 R2 (KB2973408) wit	Windows	08-Jul-2014
Important	Security Update for Windows Server 2012 R2 (KB2973906) wit	Windows	08-Jul-2014
Important	2018-12 Security and Quality Rollup for .NET Framework 3.5, 4	Windows	11-Dec-2018
Important	2018-12 Security Only Update for .NET Framework 3.5, 4.5.2, -	Windows	11-Dec-2018
Moderate	2018-09 Cumulative Security Update for Internet Explorer 11 fo	Windows	11-Sep-2018
Moderate	2018-12 Cumulative Security Update for Internet Explorer 11 fo	Windows	11-Dec-2018
-	Update for Windows Server 2012 R2 (KB2938066)	Windows	08-Jul-2014
-	Update for Windows Server 2012 R2 (KB2967917)	Windows	08-Jul-2014
-	Security Update for Windows Server 2012 R2 (KB2975625) wit	Windows	08-Jul-2014
-	Update for Windows Server 2012 R2 (KB3000850)	Windows	18-Nov-2014

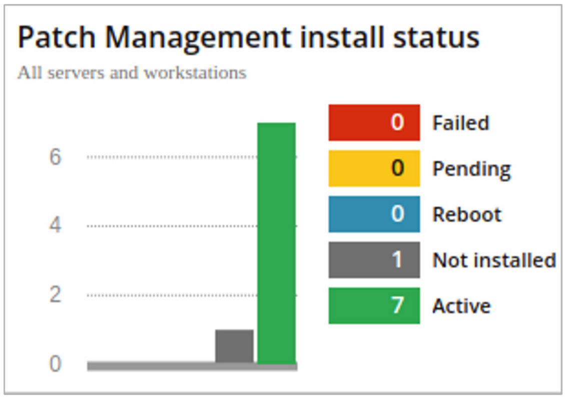
Set Patch Policy

Entity	Policy
Workstations	Do Nothing
Servers	

Patch Summary

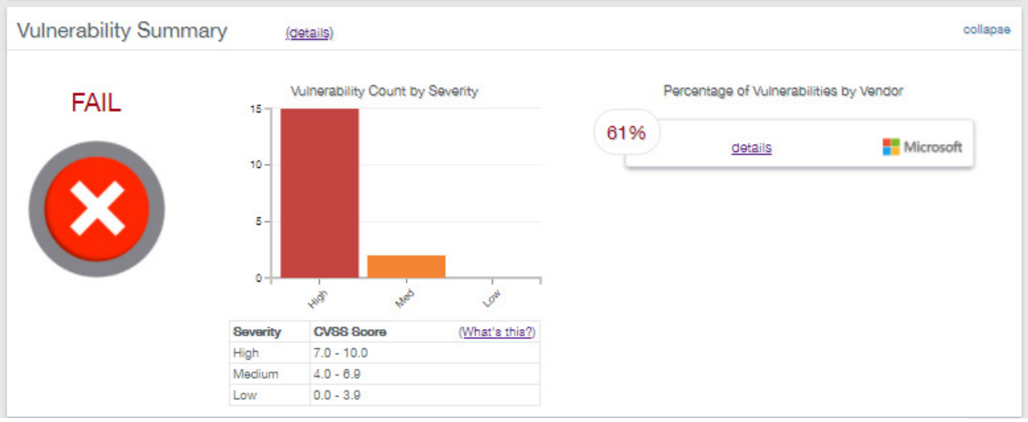
Failed	0
Missing	1
Pending	0
Installing	0
Installed	1
Ignored	0
Reboot Required	0

- 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

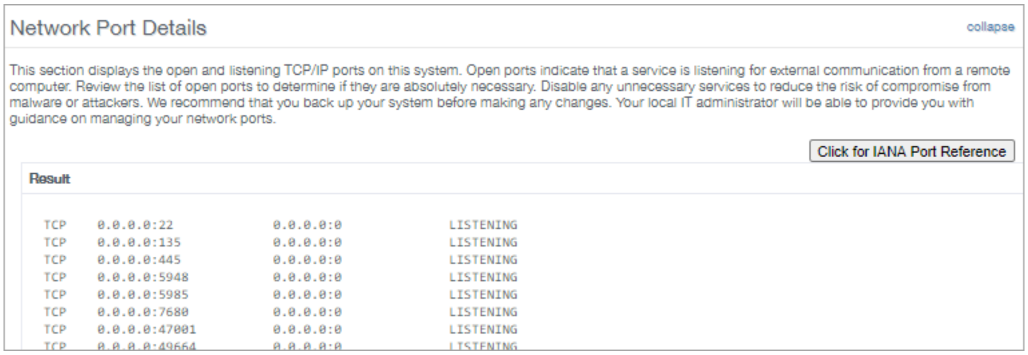


Severity	CVSS Score	(What's this?)
High	7.0 - 10.0	
Medium	4.0 - 6.9	
Low	0.0 - 3.9	

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.

The security scan report contains the vulnerability results for the selected device, revealing the security risks to the operating system and installed application. The device details contain information on when the assessment is completed, the host name, its IP address, and platform.

The vulnerability summary graph shows the vulnerability count by severity based on the common vulnerability scoring system (CVSS) with each vulnerability assigned a severity of high, medium, or low and the percentage of vulnerabilities by vendor.



This section displays the open and listening TCP/IP ports on this system. Open ports indicate that a service is listening for external communication from a remote computer. Review the list of open ports to determine if they are absolutely necessary. Disable any unnecessary services to reduce the risk of compromise from malware or attackers. We recommend that you back up your system before making any changes. Your local IT administrator will be able to provide you with guidance on managing your network ports.

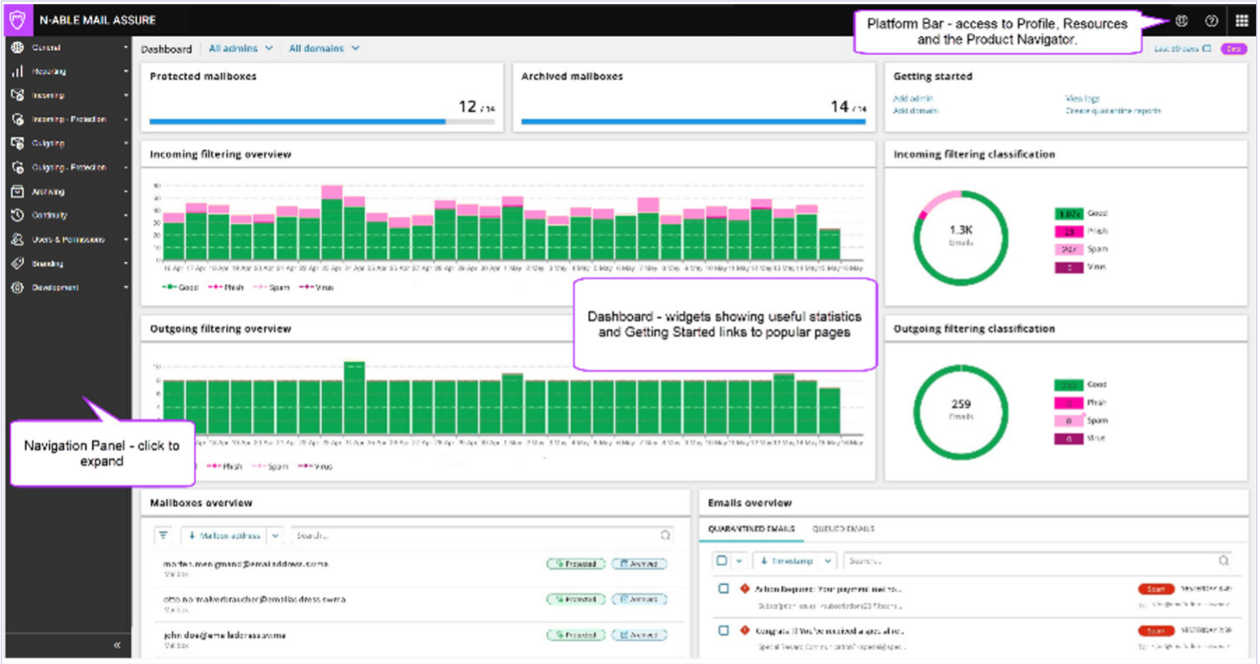
Result

```
TCP    0.0.0.0:22          0.0.0.0:0          LISTENING
TCP    0.0.0.0:135         0.0.0.0:0          LISTENING
TCP    0.0.0.0:445         0.0.0.0:0          LISTENING
TCP    0.0.0.0:5948        0.0.0.0:0          LISTENING
TCP    0.0.0.0:5985        0.0.0.0:0          LISTENING
TCP    0.0.0.0:7680        0.0.0.0:0          LISTENING
TCP    0.0.0.0:47001       0.0.0.0:0          LISTENING
TCP    0.0.0.0:49664       0.0.0.0:0          LISTENING
```

Those scores allow admins to prioritize to meet compliance goals. In addition to the details on specific software vendors and security bulletin ID's, N-able vulnerability scanning also provides details on open network ports.

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



Platform Bar - access to Profile, Resources and the Product Navigator.

Dashboard - widgets showing useful statistics and Getting Started links to popular pages

Navigation Panel - click to expand

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:

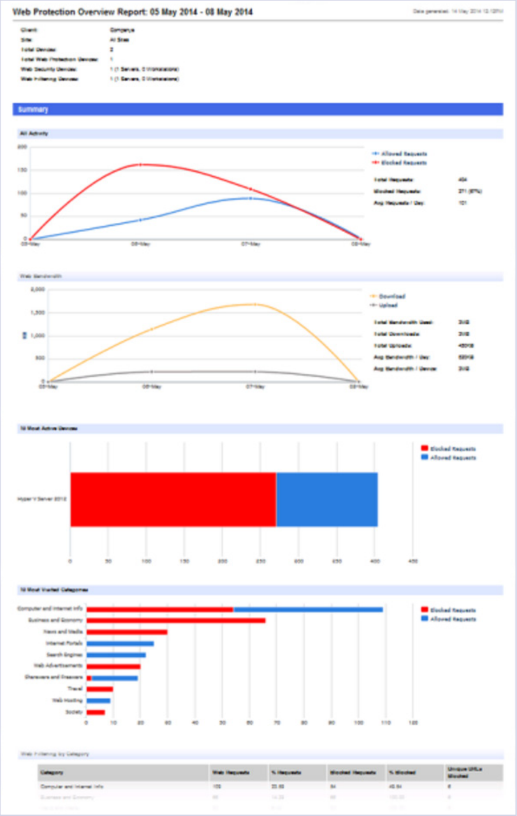
- Email security for inbound and outbound email
- Intelligent protection and filtering engine that prevents known and emerging threats
- Easy setup, add domains and change MX records
- Web interface for both admins and end users
- Quarantine management for view, release, remove, block, or approve
- Mailbox 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

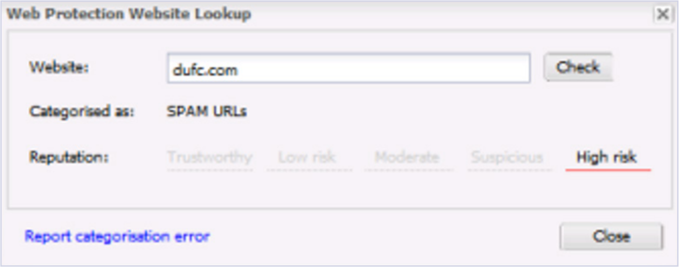
As the number of web-based security threats multiply— from phishing sites, proxies, and websites pushing malware to spyware, adware, and botnets—it's vital that you take control of your users' web security to avoid accidental strays onto malicious websites.

With the Windows-only web protection solution, you can deliver web security, web filtering, and web-bandwidth monitoring for your users any place, anytime—and all configured and managed directly from your RMM dashboard.

Web protection is installed on each monitored device and provides full visibility into the user's online activity regardless of their location, including the websites they have visited, website categories (including pornography, hate, and racism), and website reputation (such as trustworthy, suspicious, high-risk) along with the web bandwidth consumed.



Leveraging an extensive site categorization database to provide URL coverage for more than 280,000,000 domains, web protection is designed to provide optimal browsing speed through multiple categorization servers strategically positioned around the globe. This affords the highest level of flexibility without a loss in performance, making it ideal for both stationary and highly mobile organizations.



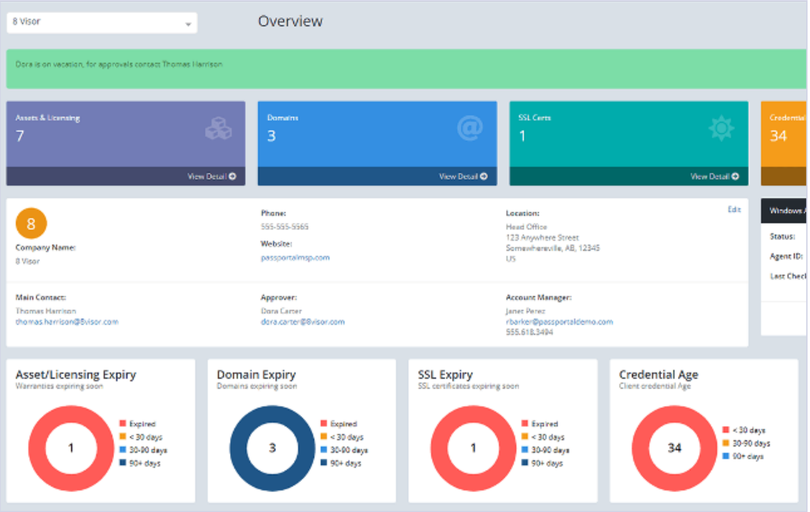
Web Protection Website Lookup

Website: dufc.com

Categorised as: SPAM URLs

Reputation: High risk

Password Management


8 Visor

Overview

Dora is on vacation, for approvals contact Thomas Harrison

Assets & Licensing 7

Domains 3

SSL Certs 1

Credentia 34

Company Name: 8 Visor

Phone: 555-555-5565

Website: passportalmsp.com

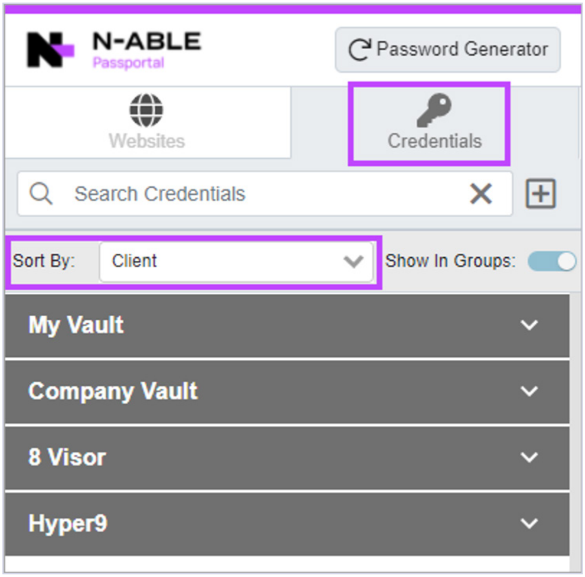
Location: Head Office
123 Anywhere Street
Somewhereville, AB, 12345
US

Main Contact: Thomas Harrison thomas.harrison@8visor.com

Approver: Dora Carter dora.carter@8visor.com

Account Manager: Janet Perez rbarker@passportaldemo.com 555.618.3494

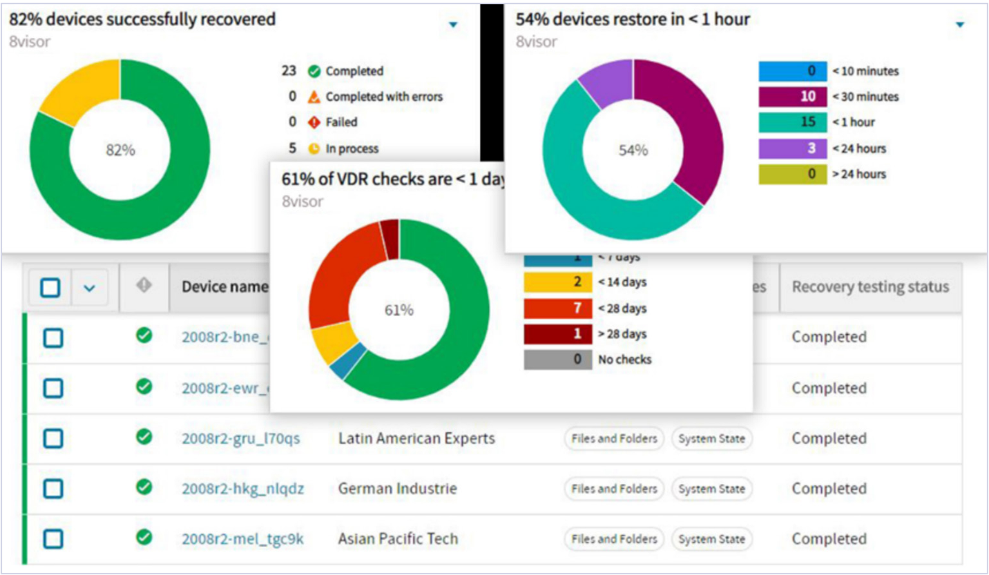
Password management allows IT managers to implement rules to generate strong passwords, eliminate re-use, and automate password rotation and routine maintenance. Encrypt, store, manage, and retrieve credentials quickly and safely, while minimizing password risks.


Sort By: Client

Show In Groups:

N-able Passportal™ is a cloud-based platform that offers simple, secure password and documentation management tailored to your operations. Passportal 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, Passportal is designed to streamline the technician's day. Finally, it allows you to easily adopt and demonstrate best-practice password management workflows.

Backup



82% devices successfully recovered
8visor

82%

23	✓ Completed
0	⚠ Completed with errors
0	◆ Failed
5	● In process

54% devices restore in < 1 hour
8visor

54%

0	< 10 minutes
10	< 30 minutes
15	< 1 hour
3	< 24 hours
0	> 24 hours

61% of VDR checks are < 1 day
8visor

61%

1	< 7 days
2	< 14 days
7	< 28 days
1	> 28 days
0	No checks

□		Device name			Recovery testing status
□	✓	2008r2-bne_			Completed
□	✓	2008r2-ewr_			Completed
□	✓	2008r2-gru_l70qs	Latin American Experts	Files and Folders System State	Completed
□	✓	2008r2-hkg_nlqdz	German Industrie	Files and Folders System State	Completed
□	✓	2008r2-mel_tgc9k	Asian Pacific Tech	Files and Folders System State	Completed

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.

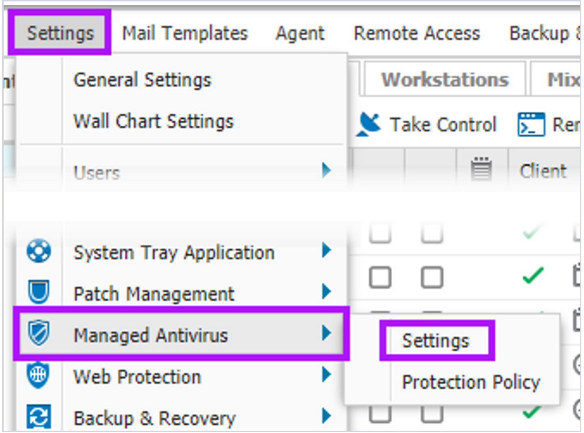
N-able Backup includes the following from our world-class, compliant data centers worldwide:

- Support and backup of Microsoft 365
- No hardware requirements
- Automated backup deployment including profiles
- AES 265-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

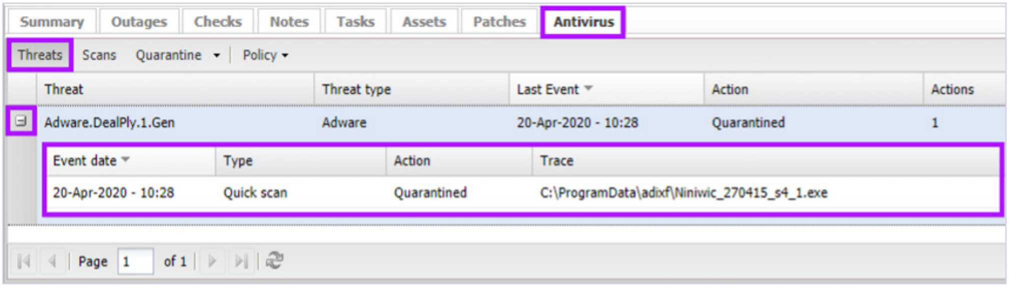
** Other location-specific certifications exist, above table contains most requested

Managed antivirus with disk encryption management



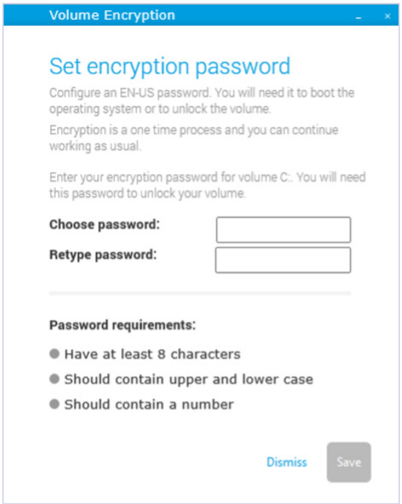
To meet the needs of device-level protection, we developed a security manager solution that deploys and can be managed directly from the dashboard. For businesses that don't yet require EDR, this solution can be tailored to meet your specific needs, with the option to permit end-user interactions like 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 Protection policies control every aspect of managed antivirus. This includes scan schedules, remediation actions taken 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.



Threat	Threat type	Last Event	Action	Actions
Adware.DealPly.1.Gen	Adware	20-Apr-2020 - 10:28	Quarantined	1

Event date	Type	Action	Trace
20-Apr-2020 - 10:28	Quick scan	Quarantined	C:\ProgramData\adixf\Niniwic_270415_s4_1.exe


Volume Encryption

Set encryption password

Configure an EN-US password. You will need it to boot the operating system or to unlock the volume.

Encryption is a one time process and you can continue working as usual.

Enter your encryption password for volume C:. You will need this password to unlock your volume.

Choose password:

Retype password:

Password requirements:

- Have at least 8 characters
- Should contain upper and lower case
- Should contain a number

Our engine and polices 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.

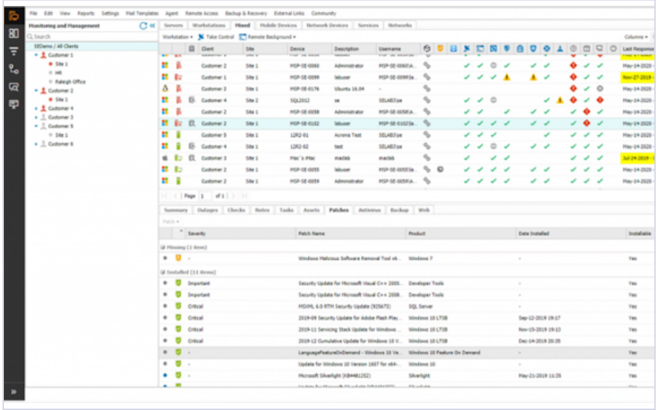
N-able disk encryption leverages native BitLocker so you can take advantage of any existing encryption you may already have and start benefiting from our easy-to-manage recovery key system. Our encryption manager allows for multiple security options—trusted platform module, trusted platform module, passwords,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

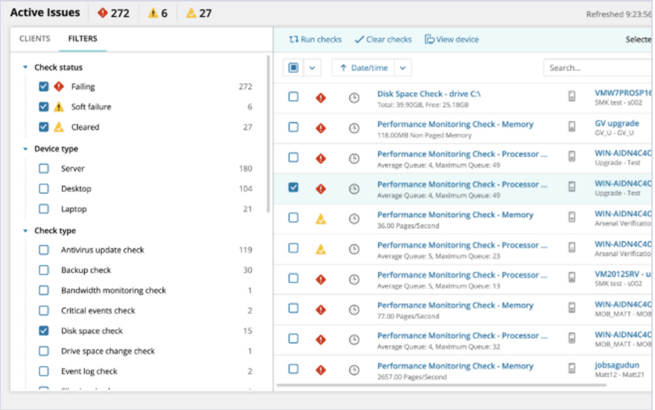
Device Monitoring

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 of potential attacks.

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.





Active Issues ◆ 272 ⚠ 6 ⚠ 27 Refreshed 9:23:56

CLIENTS FILTERS

▾ Check status
- ☑ ◆ Failing 272
- ☑ ⚠ Soft failure 6
- ☑ ⚠ Cleared 27

▾ Device type
- ☐ Server 180
- ☐ Desktop 104
- ☐ Laptop 21

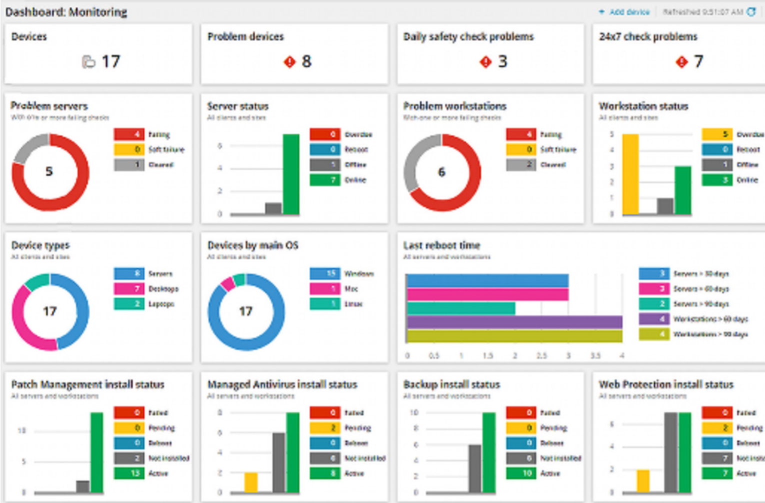
▾ Check type
- ☐ Antivirus update check 119
- ☐ Backup check 30
- ☐ Bandwidth monitoring check 1
- ☐ Critical events check 2
- ☑ Disk space check 15
- ☐ Drive space change check 1
- ☐ Event log check 2

Run checks | Clear checks | View device | Selecte

Date/time | Search...

- ☐ ◆ Disk Space Check - drive C:\ — Total: 39.90GB, Free: 25.18GB — VMW7PROSP16 SMK test - s002
- ☐ ◆ Performance Monitoring Check - Memory — 118.00MB Non Paged Memory — GV upgrade GV_U - GV_U
- ☐ ◆ Performance Monitoring Check - Processor ... — Average Queue: 4, Maximum Queue: 49 — WIN-AIDN4C4C Upgrade - Test
- ☑ ◆ Performance Monitoring Check - Processor ... — Average Queue: 4, Maximum Queue: 49 — WIN-AIDN4C4C Upgrade - Test
- ☐ ⚠ Performance Monitoring Check - Memory — 36.00 Pages/Second — WIN-AIDN4C4C Arsenal Verificatio
- ☐ ⚠ Performance Monitoring Check - Processor ... — Average Queue: 5, Maximum Queue: 23 — WIN-AIDN4C4C Arsenal Verificatio
- ☐ ◆ Performance Monitoring Check - Processor ... — Average Queue: 5, Maximum Queue: 13 — VM2012SRV - u SMK test - s002
- ☐ ◆ Performance Monitoring Check - Memory — 77.00 Pages/Second — WIN-AIDN4C4C MOB_MATT - MOB
- ☐ ◆ Performance Monitoring Check - Processor ... — Average Queue: 4, Maximum Queue: 32 — WIN-AIDN4C4C MOB_MATT - MOB
- ☐ ◆ Performance Monitoring Check - Memory — 2657.00 Pages/Second — jobsagudun Matt12 - Matt21

- Receive alerts on 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



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 if 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.

MANAGED ANTIVIRUS WITH DISK ENCRYPTION MANAGEMENT

To meet the needs of device level protection, we developed a Managed Antivirus solution that's deployed and managed directly from the dashboard. In addition, 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 of potential attacks.