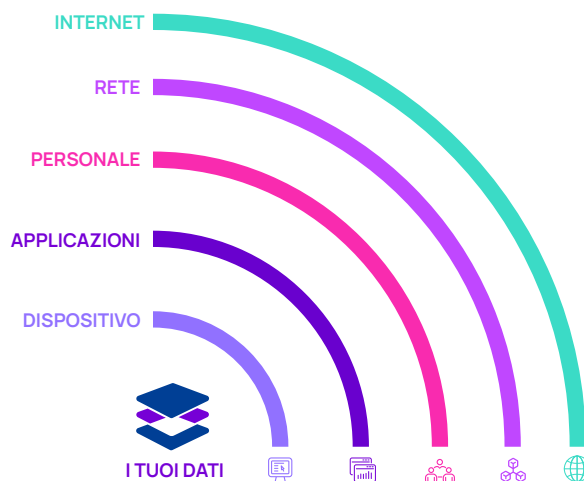


Soluzioni di sicurezza su più livelli di N-able N-central per reparti IT

Solo N-able può offrire un approccio multilivello alla sicurezza con una protezione senza paragoni e intuitività, il tutto da un'unica dashboard semplificata. Oltre alle funzionalità eccezionali, N-able offre esperienza, programmi di formazione e supporto trasformatore per aziende per una sicurezza all'avanguardia.

N-able mette a disposizione una straordinaria gamma di nove diverse funzionalità di sicurezza di base per implementare tutti i livelli di protezione della rete e sette funzionalità finalizzate al successo per dare una marcia in più ad azienda, team e competenze.



Funzionalità di sicurezza principali

- Gestione delle patch
- Rilevamento e risposta per gli endpoint
- Scansione delle vulnerabilità
- Sicurezza e-mail basata su cloud
- Gestione sicurezza e crittografia del disco
- Antivirus gestito
- Gestione delle password
- Backup
- Monitoraggio
- Sicurezza web

Funzionalità per il successo

- Esperti del settore
- Successo dei consumatori
- Assistenza 24/7 di livello mondiale
- Formazione dettagliata
- Automation Cookbook
- Community attiva
- Canali di feedback sui prodotti

I dati rappresentano la risorsa più importante nonché l'obiettivo dei criminali informatici. Implementando adeguate tecnologie di sicurezza su ciascun livello, crei diverse linee di difesa per proteggere tale obiettivo. I criminali puntano ai dati per una serie di ragioni. Potrebbero volerli distruggere, sottoporli a crittografia, usarli per chiedere un riscatto o rubarli per rivenderli sul dark web. In ogni caso, i dati sono l'obiettivo.

Un approccio alla sicurezza su più livelli blocca l'attacco nel punto più lontano possibile dai dati. Ad esempio, il blocco di un'e-mail dannosa impedisce a un potenziale attacco ransomware di penetrare nella rete. Fermare un attacco in questo modo è più sicuro che farlo quando ha già raggiunto il dispositivo e iniziato a sottoporre i file a crittografia.

Di seguito viene fornita una panoramica delle funzionalità di sicurezza su più livelli di N-able, grazie alle quali i dati vengono protetti da più punti di vista.

Soluzione di rilevamento e risposta per gli endpoint

N-able™ Endpoint Detection and Response (EDR) offre ai tecnici in prima linea la possibilità di rilevare i malware più recenti (incluso il ransomware), condurre indagini e risolvere eventuali danni causati, ad esempio, ripristinando gli endpoint allo stato precedente a un attacco e implementando misure per un incidente informatico in pochi minuti, invece che in ore.

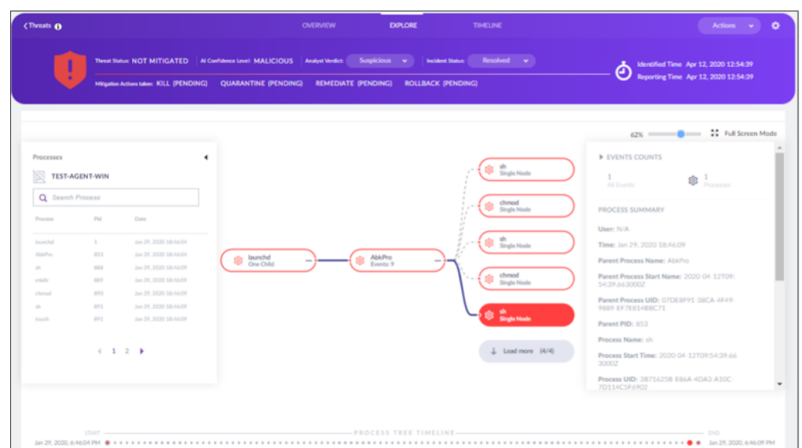
EDR è un software integrato per la gestione delle minacce con tecnologia SentinelOne. Con l'integrazione di N-central nella protezione degli endpoint di SentinelOne, EDR permette ai dispositivi Windows di difendersi e di ripristinarsi in maniera autonoma interrompendo processi, sottoponendo a quarantena l'area interessata, risolvendo qualsiasi danno ed eseguendo il rollback degli eventi per una protezione avanzata.

EDR valuta il comportamento per monitorare diversi processi e individuare gli attacchi mentre si sviluppano, implementando misure rapidamente. Questo approccio differisce dal rilevamento basato su firme impiegato dalle soluzioni antivirus tradizionali, che monitorano l'esecuzione dei processi mentre è in corso e non anticipano eventuali problemi.



EDR offre dati forensi per mitigare le minacce rapidamente, isolare la rete e proteggere i dispositivi dalle minacce emergenti.

Le nuove funzionalità integrate in N-central includono l'implementazione degli agent EDR, la configurazione dei profili e il monitoraggio dei dispositivi dalla dashboard.

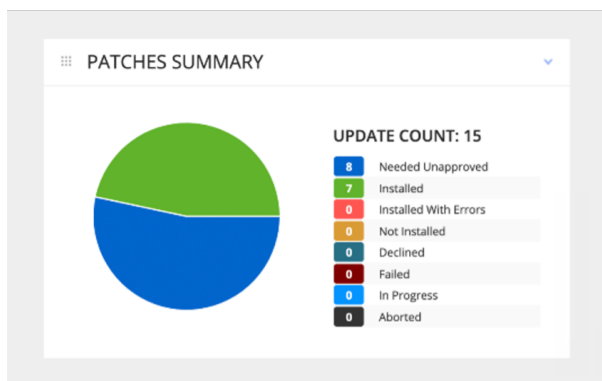
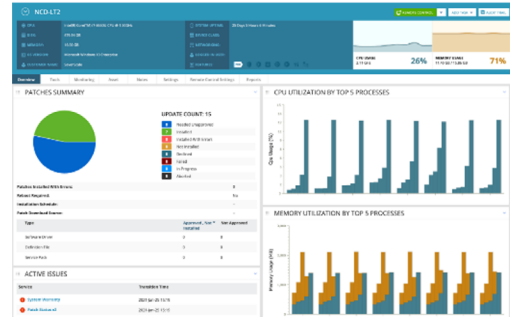


Gestione delle patch

La gestione delle patch offre ai responsabili IT la possibilità di completare il controllo granulare su quando, come e quali patch siano state implementate nella rete, sui dispositivi o nei diversi gruppi. La gestione delle patch tramite N-central® consente inoltre la protezione di diversi sistemi operativi e applicazioni di terze parti contemporaneamente.

La gestione delle patch di N-able™ N-central offre agli amministratori gli strumenti necessari, ad esempio:

- Individuazione di un site concentrator (facoltativa)
- Attivazione e applicazione dei criteri per la gestione delle patch
- Criteri personalizzati per la gestione delle patch
- Visualizzazione di informazioni dettagliate sulle patch, inclusi report
- Gestione delle patch per dispositivi singoli e multipli
- Rielaborazione delle patch non riuscite
- Azioni di approvazione delle patch
- Disinstallazione delle patch Microsoft
- Pianificazione delle patch
- Applicazioni supportate
- Nuova esecuzione manuale del controllo dello stato delle patch
- Creazione di un ciclo di vita di approvazione e di flussi di identificazione delle patch

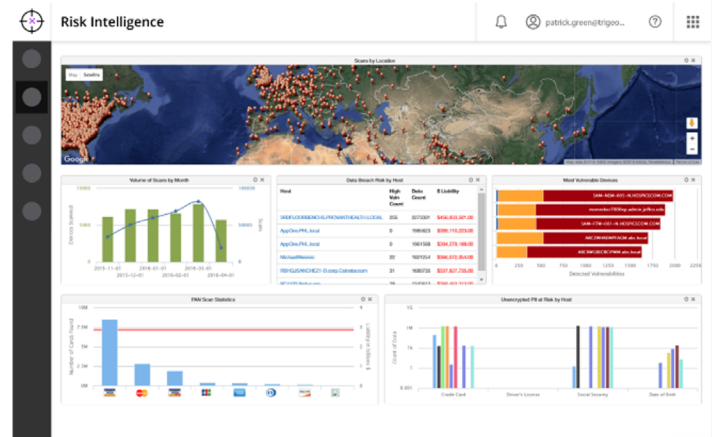


Tutto questo non solo permette di migliorare la produttività, come necessario per gestire in modo efficace la sicurezza delle applicazioni, ma offre anche strumenti intuitivi per procedure avanzate finalizzate alla sicurezza senza la necessità di formazione specializzata, consentendo alle risorse di concentrarsi sulle attività aziendali principali.

Scansione delle vulnerabilità e intelligence dei rischi

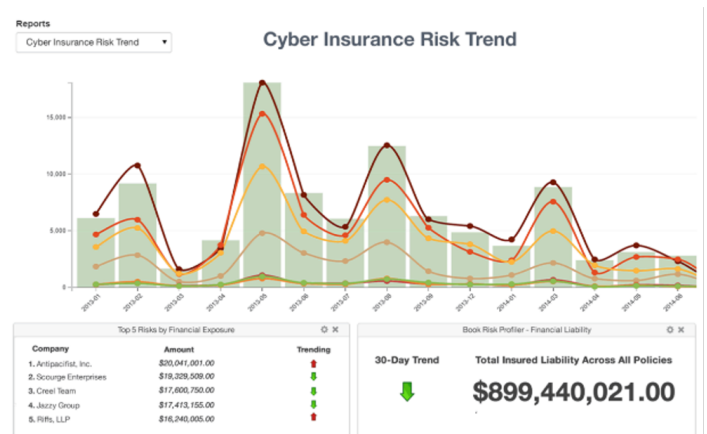
Progettate per identificare eventuali configurazioni errate o porte aperte presenti nella rete, oltre che per fornire reportistica storica, grazie a queste due funzionalità insieme i reparti IT possono mostrare i progressi circa la sicurezza nel tempo.

La piattaforma N-central include la rete di dispositivi, la reportistica rapida e il rilevamento e l'applicazione di rimedi per le patch; le valutazioni di rischi e conformità sono componenti aggiuntivi e rappresentano protezioni essenziali per conformarsi ai requisiti normativi.



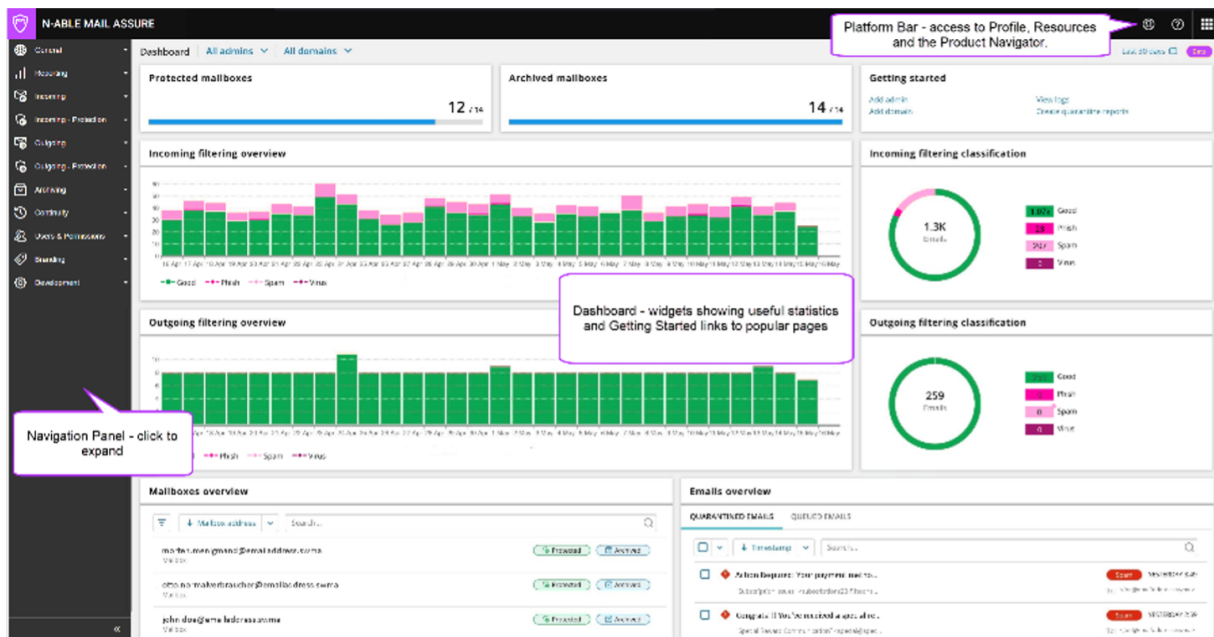
N-able™ Risk Intelligence individua i dati sensibili e a rischio in tutte le reti e le workstation gestite, rivelando i costi di una possibile violazione dei dati, grazie a:

- Scansione vulnerabilità avanzata
- Report brandizzabili che illustrano i dettagli dell'impatto economico dei rischi
- Individuazione degli accessi utente inappropriati
- Scansioni PCI, DSS, PAN e delle informazioni di identificazione personale
- Esplorazione dei dati a rischio
- Report circa le tendenze sui rischi per dimostrare i miglioramenti apportati



Il report con i dettagli sulle porte della rete mostra le porte TCP/IP di ascolto sul sistema, indicando che un servizio è in ascolto per comunicazioni esterne ricevute da un computer remoto. Con il report dettagliato le minacce sono facili da vedere, in tempo reale.

Sicurezza e-mail basata su cloud



Le e-mail contano. Anche con un primo livello di sicurezza, ad esempio le inclusioni con Microsoft 365™, Mail Assure fornisce un controllo aggiuntivo e un ulteriore livello di difesa, concepito per proteggere da spam, virus, malware, phishing, ransomware e altre minacce inviate da posta elettronica, proteggendo al contempo i dati grazie all'archiviazione basata su cloud.

N-able™ Mail Assure offre una serie di funzionalità di sicurezza e-mail che proteggono il principale obiettivo presente all'interno della rete:

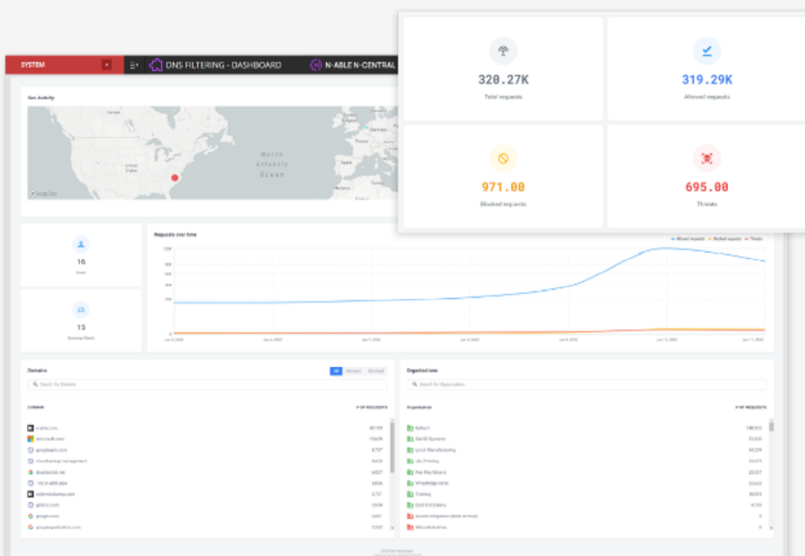
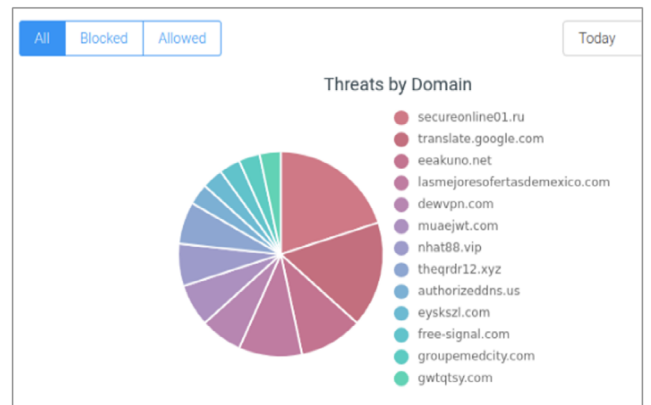
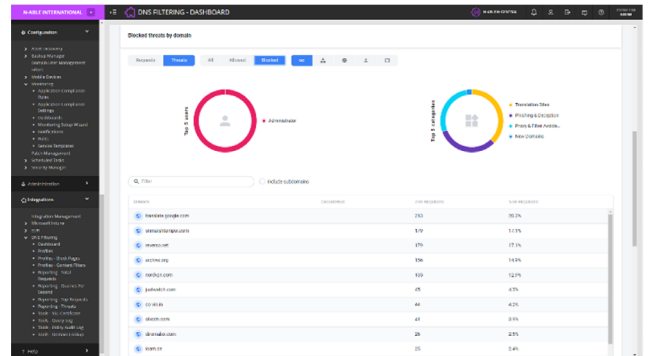
- Sicurezza e-mail per la posta in entrata e in uscita
- Motore di filtraggio e protezione intelligente che tiene alla larga le minacce note ed emergenti
- Configurazione semplificata, aggiunta di domini e modifica dei record MX
- Interfaccia web per amministratori e utenti finali
- Gestione della quarantena per la visualizzazione, il rilascio, la rimozione, il blocco o l'approvazione
- Rilevamento automatico delle caselle di posta elettronica tramite SMTP o sincronizzazione via LDAP
- Statistiche avanzate sui filtri
- Gestione del blocco di estensioni e allegati
- Crittografia del traffico SSL/TLS
- Implementazione intelligente dell'host per il filtro delle e-mail in uscita
- Firme DKIM per i messaggi in uscita per garantire l'autenticità del mittente
- E-mail continuity integrata 24 ore al giorno, tutti i giorni
- Accesso basato sul web alle e-mail archiviate e in quarantena
- Possibilità di inviare e ricevere i messaggi direttamente dalla dashboard di Mail Assure

Sicurezza web

La sicurezza web è fondamentale per proteggere qualsiasi azienda, soprattutto con l'evoluzione della forza lavoro in mobilità. I database su web e i filtri basati su DNS proteggono azienda, personale e relativi dati all'interno e all'esterno della rete.

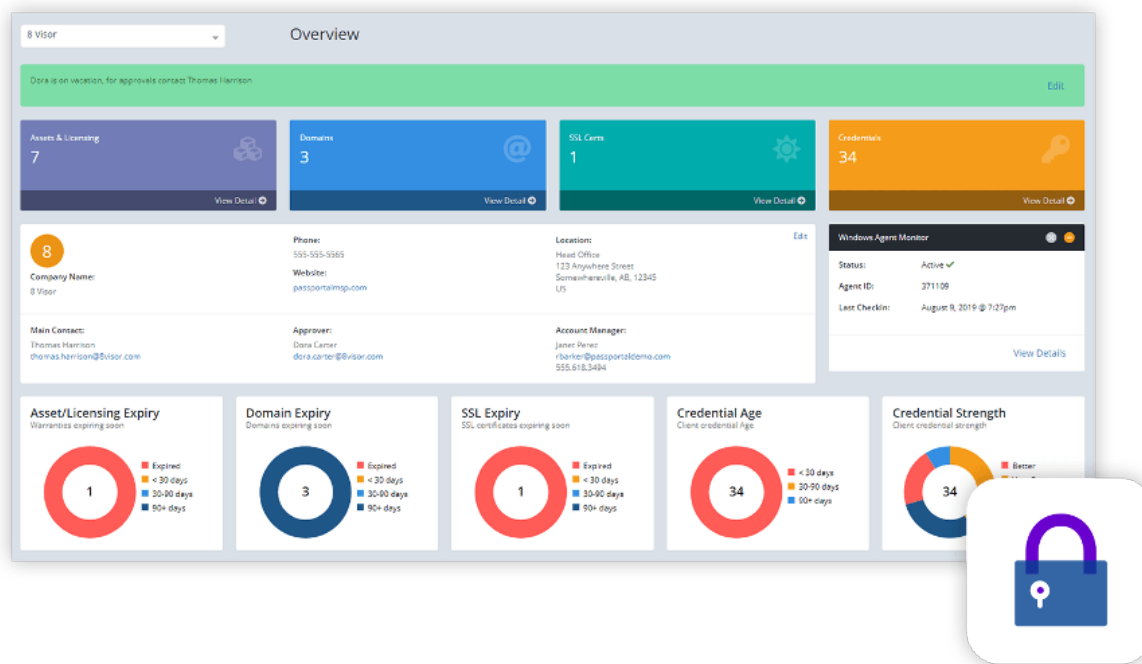
Migliaia di siti web dannosi vengono creati ogni giorno e pubblicità malevola, siti di phishing e altre minacce per la sicurezza riescono a bypassare i filtri web esistenti. N able™ DNS Filtering offre una protezione più solida, una maggiore visibilità della rete e la reportistica basata sugli utenti direttamente dalla dashboard di N-central®.

In più, il prodotto di N-able impiega una protezione intelligente dalle minacce e il blocco dei siti web dannosi in tempo reale prima che danneggino i clienti e i relativi utenti. Proteggili all'interno e all'esterno della rete con la soluzione DNS Filtering. È interamente basata su cloud, il che consente una maggiore scalabilità e la massima tranquillità.

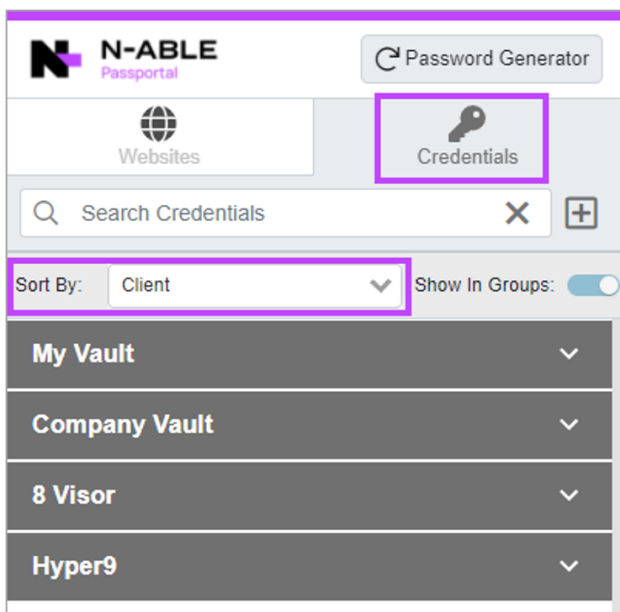


- Possibilità di prevenire l'accesso ai contenuti indesiderati e dannosi
- Blocco di phishing, virus, attacchi zero-day e delle altre minacce informatiche
- Identificazione intelligente dei domini dannosi, generalmente 80 ore più rapidamente rispetto ad altre soluzioni
- Rete anycast ridondante e affidabile con 50 data center
- Report completi per sede o utente
- Visualizzazione dell'attività di rete, del traffico e della sicurezza
- Individuazione delle falle del sistema di sicurezza grazie ai registri dell'attività DNS
- Creazione di criteri per gruppo, dispositivo o rete
- Reindirizzamento degli utenti a una pagina bloccata personalizzata
- Blocco delle minacce phishing precedentemente non inserite in alcuna categoria, grazie alle tattiche antiphishing basate su immagini
- Mitigazione di botnet, cryptomining dannoso e minacce malware tramite il feed delle minacce potenziato

Gestione delle password

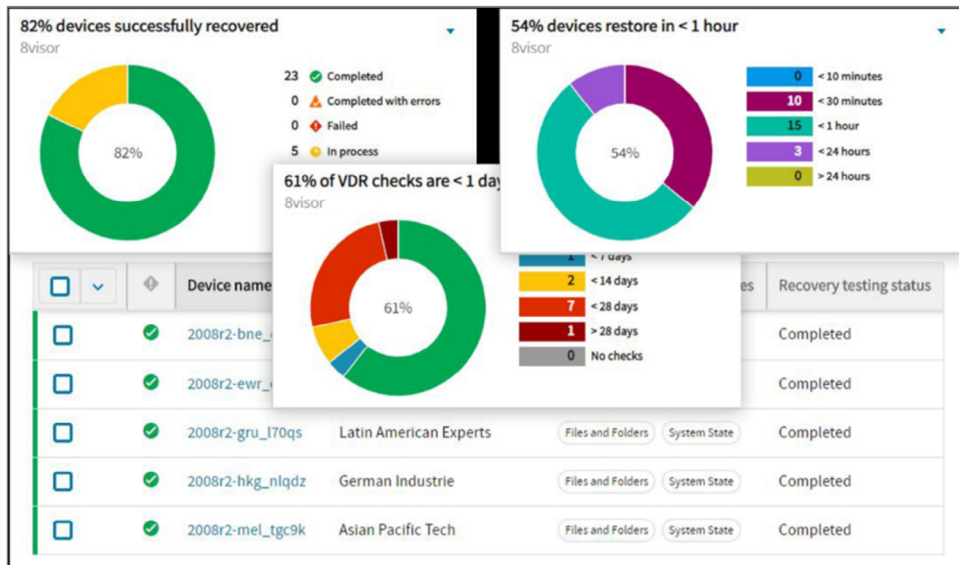


Con la gestione delle password, i responsabili IT possono implementare regole per generare password complesse, evitare il loro riutilizzo e automatizzarne la rotazione e la manutenzione di routine. Sottoponi a crittografia, archivia, gestisci e recupera le credenziali in modo rapido e sicuro, riducendo al contempo i rischi per le password.



N-able™ Passport è una piattaforma basata su cloud che offre la gestione semplificata e sicura di password e documentazione, personalizzata in base alle tue esigenze. Passportal impiega la protezione automatizzata delle password che accelera e semplifica l'archiviazione, la gestione e il recupero delle password e delle conoscenze del reparto, virtualmente da qualsiasi dispositivo connesso. Grazie all'inserimento delle credenziali che assicura la connettività rapida, fluida e sicura a dispositivi utente, reti e applicazioni, Passportal è stato concepito per semplificare le operazioni quotidiane dei tecnici. Infine, consente di adottare e di dimostrare senza problemi i flussi di lavoro di gestione delle password basati su best practice.

Backup



Le aziende non solo richiedono l'architettura veloce, sicura e ibrida necessaria per ogni soluzione di backup moderna, ma anche funzionalità multistorage e di ripristino per ridurre il rischio di un attacco ransomware andato a buon fine a quasi lo zero percento.

Con N-able Backup hai a disposizione diverse opzioni di recupero che impiegano il ripristino veloce di file e cartelle, oltre al ripristino bare metal dell'intero sistema o al disaster recovery virtuale. Crea un server di standby con l'opzione di ripristino continuo e recupera i file alla velocità della LAN tramite l'opzione Local Speed Vault, se necessario. Infine, testa e verifica la recuperabilità del backup con programmazione automatizzata con il test del ripristino.

N-able Backup include le seguenti funzionalità, grazie ai data center conformi e di alto livello presenti ovunque:

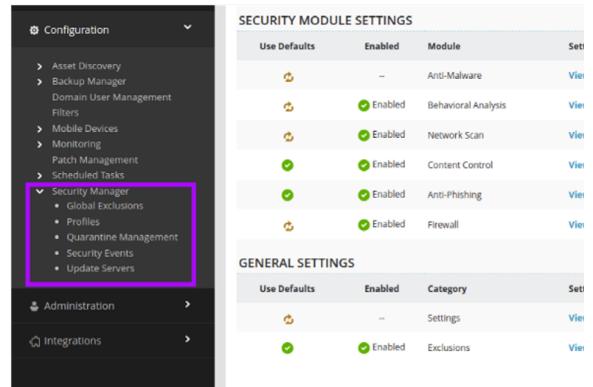
- Supporto e backup di Microsoft 365
- Nessun requisito hardware
- Implementazione automatica dei backup inclusi i profili
- Crittografia AES a 256 bit
- Chiavi private personalizzate
- Data center con pppcertificazione ISO
- Impostazioni di accesso a livello di ruolo
- Tecnologia True Delta con monitoraggio delle modifiche a livello di byte
- Deduplica e compressione
- Ottimizzazione WAN

Paese	HIPAA	ISO27001	ISO9001	NIST 800-53	PCI DSS	SOC TYPE II	SOC 2 TYPE II
Australia		X			X	X	X
Belgio		X					
Brasile		X	X		X	X	X
Canada	X	X		X	X	X	X
Danimarca		X			X	X	X
Francia		X	X		X	X	X
Germania		X	X		X	X	X
Italia		X	X		X	X	X
Norvegia		X	X				
Paesi Bassi		X	X		X	X	X
Portogallo		X	X		X	X	X
Regno Unito		X	X		X	X	X
Spagna		X	X		X		
Stati Uniti	X	X		X	X	X	X
Sudafrica			X				
Svezia		X	X				
Svizzera		X	X		X	X	X

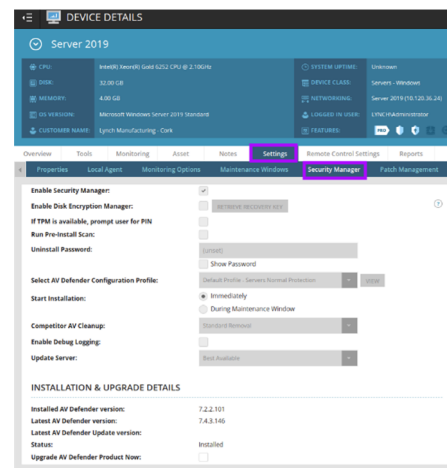
**Sono disponibili altre certificazioni specifiche per i diversi paesi. La tabella in alto include solo quelle più richieste

Gestione sicurezza con gestione della crittografia del disco

Per rispondere alle esigenze della protezione a livello di dispositivo, abbiamo sviluppato una soluzione di gestione della sicurezza implementabile e gestibile direttamente dalla dashboard di N-central. Per le aziende che non richiedono un servizio di rilevamento e risposta per gli endpoint, questa soluzione è personalizzabile in base alle specifiche esigenze, con la possibilità di consentire l'intervento degli utenti finali, ad esempio l'esecuzione di scansioni e l'aggiornamento delle definizioni delle minacce. Inoltre, è possibile abilitare la crittografia del disco a livello di volume per proteggere ulteriormente i dati.

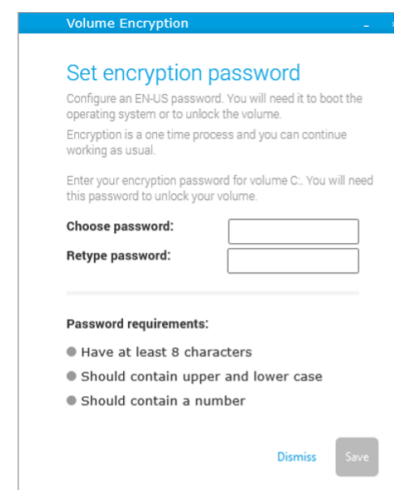


La crittografia del disco protegge i dati da minacce quali furto o perdita accidentale, rendendo le informazioni presenti sulle unità illeggibili per gli utenti non autorizzati. La crittografia del disco è perfetta per ambienti in cui i dati rappresentano una risorsa fondamentale o in cui vigono regolamenti per la conformità, come GDPR, PII e PCI DSS ed è presente il rischio di perdita dei dati.



I criteri di protezione di N-able controllano ogni aspetto della gestione sicurezza, ad esempio le pianificazioni delle scansioni, gli interventi di risoluzione non appena viene individuata una minaccia e gli interventi degli utenti finali. Abbiamo incluso alcuni criteri predefiniti per aiutarti a iniziare, oltre che la possibilità di creare criteri personalizzati in base alle tue specifiche esigenze.

Il nostro motore e i criteri sono forniti da Bitdefender, un leader per la sicurezza nel settore i cui criteri sono presenti nelle installazioni Windows e Mac. In più, è prevista l'applicazione automatica delle impostazioni della gestione sicurezza supportate dal sistema operativo del computer in uso.



La crittografia del disco di N-able sfrutta il meccanismo nativo BitLocker per utilizzare eventuali crittografie esistenti e iniziare a beneficiare del nostro intuitivo sistema di recupero. La gestione crittografia dispone di diverse opzioni di sicurezza (tra cui modulo piattaforma affidabile, password, ecc.) per la personalizzazione semplificata.

Monitoraggio dispositivi

Il monitoraggio offre a tecnici in prima linea, responsabili IT ed esperti di sicurezza le tendenze in tempo reale e storiche per prevedere e individuare minacce e attacchi prima che si diffondano. Il monitoraggio consente di vedere i potenziali attacchi e di inviare avvisi istantanei sulle tendenze anomale, che rappresentano indicatori chiave precoci.

Gli agent di monitoraggio rappresentano software specializzati grazie a cui è possibile tenere aggiornati workstation, server e reti tramite una scansione continua, 24 ore al giorno, tutti i giorni. Avvisano il personale IT di potenziali problemi e tengono alla larga i software dannosi dai sistemi monitorati. Tali agent assicurano la sicurezza e l'affidabilità monitorando al contempo le reti.

Grazie al monitoraggio dispositivi di N-able, hai la visibilità completa per gestire la sicurezza in modo corretto, puoi preservare l'integrità della rete, effettuare la manutenzione proattiva e restare al passo con le potenziali minacce.

- Ricezione di avvisi sui potenziali problemi
- Applicazione di patch e aggiornamento dei software su tutti i dispositivi
- Pianificazione delle attività come l'aggiornamento e l'esecuzione dell'antivirus o l'avvio dei backup quotidiani
- Automatizzazione della manutenzione di routine
- Compatibilità con Windows, Mac e Linux
- Monitoraggio e gestione avanzati della rete per server e workstation presso le sedi di diversi clienti
- Avvisi per problemi quali integrità del disco, antivirus datato e stato del servizio
- Profili di configurazione per eseguire il push di tutti gli agent insieme o in gruppi
- Connessioni sicure e trasferimento dati sottoposto a crittografia tramite HTTPS
- Monitoraggio delle prestazioni di rete
- Individuazione, importazione e monitoraggio di dispositivi di rete critici tramite SNMP, ad esempio firewall, router, stampanti e switch
- Monitoraggio dispositivi mobili
- Monitoraggio macchine virtuali

Customer	Site	Remote Control	Tools	Device/Probe	Device Class
Keltech	--	[Green]	[Icon]	SLS-0007	Workstation
Keltech	--	[Green]	[Icon]	SLS-0002	Servers - VM
Keltech	--	[Green]	[Icon]	stp-001-01	Servers - ES
Keltech	--	[Green]	[Icon]	stpm-01	Servers - ES
Lynch Manufacturing	--	[Green]	[Icon]	CheckPoint SC3800	Switch/Rout
Lynch Manufacturing	--	[Green]	[Icon]	CheckPoint SC3800	Switch/Rout
Lynch Manufacturing	--	[Green]	[Icon]	CheckPoint SC3800	Switch/Rout
Lynch Manufacturing	--	[Green]	[Icon]	CheckPoint SC3800	Switch/Rout
Lynch Manufacturing	--	[Green]	[Icon]	HW11	Servers - VM
Lynch Manufacturing	--	[Green]	[Icon]	Infoblox - iZone K2	Switch/Rout
Lynch Manufacturing	--	[Green]	[Icon]	Infoblox - Tronic S22	Switch/Rout
Lynch Manufacturing	--	[Green]	[Icon]	Infoblox - Tronic S22	Switch/Rout

Service	Status	Transition	Last Scan Time
Agent Status	[Green]	2021-Dec-17 23:10	2022-Feb-09 16:57
CPU	[Green]	2021-Dec-17 23:10	2022-Feb-09 19:29
Disk - C:	[Green]	2021-Dec-17 23:10	2022-Feb-09 19:28
DNS Flapping Status	[Green]	2022-Feb-07 06:40	2022-Feb-09 16:50
EDR Status	[Red]	2022-Feb-07 06:40	2022-Feb-09 19:59
Memory	[Green]	2021-Dec-17 23:10	2022-Feb-09 19:29
N-able Backup Product Status	[Green]	2022-Feb-08 06:41	2022-Feb-09 16:45
N-able Backup Status - Files and folders	[Green]	2022-Jan-14 05:33	2022-Feb-09 19:46
N-able Backup Status - System State	[Green]	2022-Feb-06 05:44	2022-Feb-09 19:46
N-able Backup Status - Total Backup	[Green]	2022-Jan-14 05:33	2022-Feb-09 16:46
Patch Status v2	[Green]	2022-Feb-05 09:49	2022-Feb-09 09:49

Container	Site	Remote Control	Tools	Device Name	Agent Status	Application Compliance	Backup Manager Events	Backup Manager Status	CPU
Keltech	--	[Green]	[Icon]	SLS-0002	[Green]	--	--	--	
Keltech	--	[Green]	[Icon]	SLS-0050	[Green]	--	--	--	
Lynch Manufa...	--	[Green]	[Icon]	Mac - Catalina VM	[Blue]	--	--	--	
Lynch Manufa...	--	[Green]	[Icon]	SLS-0048	[Green]	--	--	--	
Lynch Manufa...	--	[Green]	[Icon]	SLS-0049	[Green]	--	--	--	
Lynch Manufa...	Cork	[Green]	[Icon]	SLS-0006	[Green]	--	--	--	
Maryborough ...	--	[Green]	[Icon]	SLS-0083	[Green]	--	--	--	
Maryborough ...	--	[Green]	[Icon]	Windows 11	[Green]	--	--	--	

Elementi della sicurezza su più livelli

RILEVAMENTO E RISPOSTA PER GLI ENDPOINT

Offre ai tecnici in prima linea la possibilità di rilevare i malware più recenti (incluso il ransomware), condurre indagini e risolvere eventuali danni causati. È inclusa la possibilità di ripristinare gli endpoint allo stato precedente a un attacco e di implementare misure per un incidente informatico in pochi minuti, invece che in ore.

GESTIONE DELLE PATCH

La gestione delle patch offre ai responsabili IT la possibilità di completare il controllo granulare su quando, come e quali patch siano state implementate nella rete, sui dispositivi o nei diversi gruppi. La gestione delle patch tramite N-central consente inoltre la protezione di diversi sistemi operativi e applicazioni di terze parti contemporaneamente.

SCANSIONE DELLE VULNERABILITÀ

Progettata per identificare eventuali configurazioni errate o porte aperte presenti nella rete, oltre che per fornire reportistica storica. Con la combinazione di questi due elementi, i reparti IT possono mostrare i progressi circa la sicurezza nel tempo.

SICUREZZA E-MAIL BASATA SU CLOUD

Le e-mail contano. Anche con un primo livello di sicurezza, ad esempio le inclusioni con Microsoft 365™, Mail Assure fornisce un controllo aggiuntivo e un ulteriore livello di difesa, concepito per proteggere da spam, virus, malware, phishing, ransomware e altre minacce inviate da posta elettronica, proteggendo al contempo i dati grazie all'archiviazione basata su cloud.

SICUREZZA WEB

La sicurezza web è fondamentale per proteggere qualsiasi azienda, soprattutto con l'evoluzione della forza lavoro in mobilità. I database su web e i filtri basati su DNS proteggono azienda, personale e relativi dati all'interno e all'esterno della rete.

GESTIONE DELLE PASSWORD

Con la gestione delle password, i responsabili IT possono implementare regole per generare password complesse, evitare il loro riutilizzo e automatizzarne la rotazione e la manutenzione di routine. Sottoponi a crittografia, archivia, gestisci e recupera le credenziali in modo rapido e sicuro, riducendo al contempo i rischi per le password.

BACKUP

Le aziende non solo richiedono l'architettura veloce, sicura e ibrida necessaria per ogni soluzione di backup moderna, ma anche funzionalità multistorage e di ripristino per ridurre il rischio di un attacco ransomware andato a buon fine a quasi lo zero percento.

GESTIONE SICUREZZA CON GESTIONE DELLA CRITTOGRAFIA DEL DISCO

Per rispondere alle esigenze della protezione a livello di dispositivo, abbiamo sviluppato una soluzione antivirus gestita implementabile e gestibile direttamente dalla dashboard. Inoltre, è possibile abilitare la crittografia del disco a livello di volume per proteggere ulteriormente i dati.

MONITORAGGIO DISPOSITIVI

Il monitoraggio offre a tecnici in prima linea, responsabili IT ed esperti di sicurezza le tendenze in tempo reale e storiche per prevedere e individuare minacce e attacchi prima che si diffondano. Il monitoraggio consente di vedere i potenziali attacchi e di inviare avvisi istantanei sulle tendenze anomale, che rappresentano indicatori chiave precoci.