NordStellar

Welcome to NordStellar

User guide



Contents

Setup

Key setup steps

Adding assets to monitoring

Scanning the attack surface

Optional setup steps

Setting up dark web keyword monitoring

Managing users and projects

Adding a new user

Adding a new project

Alerts

Setting up alerts

Email

Slack

Microsoft Teams

Generic webhook

Responding by alert type

Data leak

External vulnerability

Suspicious domain

Features

Main section

Overview

Events

Assets

Digital threats

Leaked data: Metrics

Leaked data: Employees

Leaked data: Consumers

Dark web search

Domain squatting

Attack surface

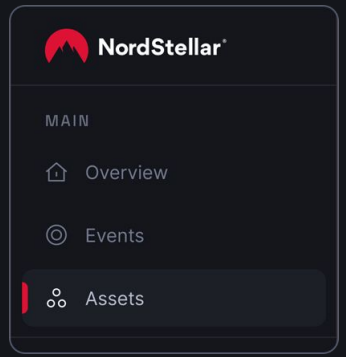
Attack surface management

Setup

Adding assets to monitoring

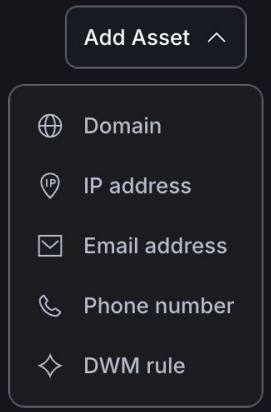
1

Go to the Assets tab and click Add asset in the upper right corner



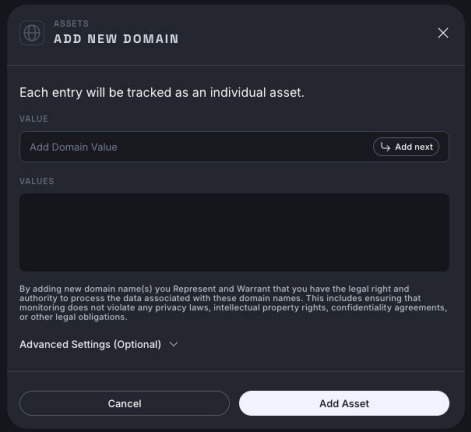
2

Choose the type of asset you want to add



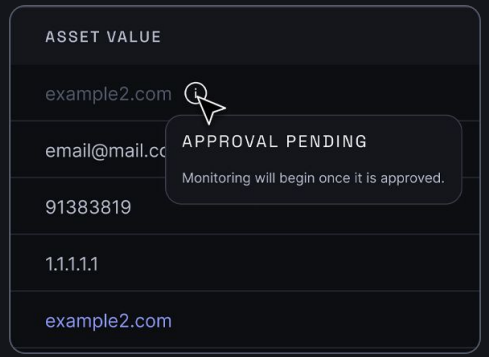
3

Enter the asset details and click Add asset



4

The asset will appear as Pending until approved by NordStellar*

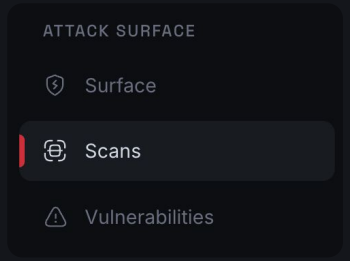


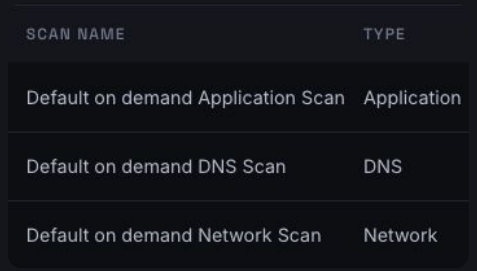
* The approval step helps prevent abuse, such as monitoring assets without authorization. You can add more assets while you wait for approval.

Note: We recommend starting by adding your main domain. Then, the subdomains, IP addresses and organizational emails will be auto-discovered by the platform.

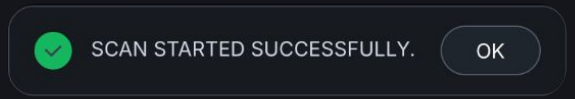
Scanning the attack surface

1. Go to the Scans tab
2. Click on one of the three default scans
3. Click the Run scan button in the upper-right corner
4. A confirmation box will appear. Repeat this process for the other two scan types





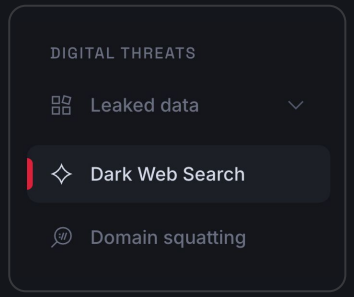




Setting up dark web keyword monitoring (1)

1

Go to the Dark Web Search tab



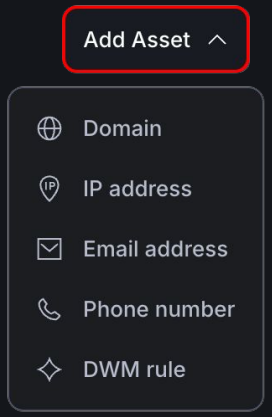
2

Enter a keyword or advanced query and click Save filter



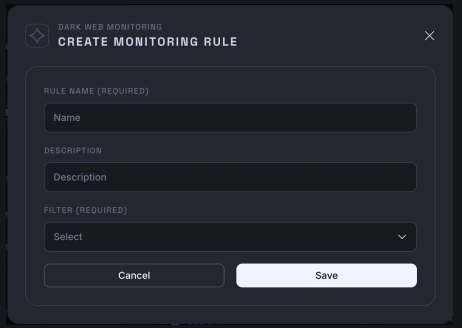
3

Go to the Assets tab, click Add asset and DWM rule



4

Fill in the required details, choose the filter you saved in step 2, and click Save



Setting up dark web keyword monitoring (2)

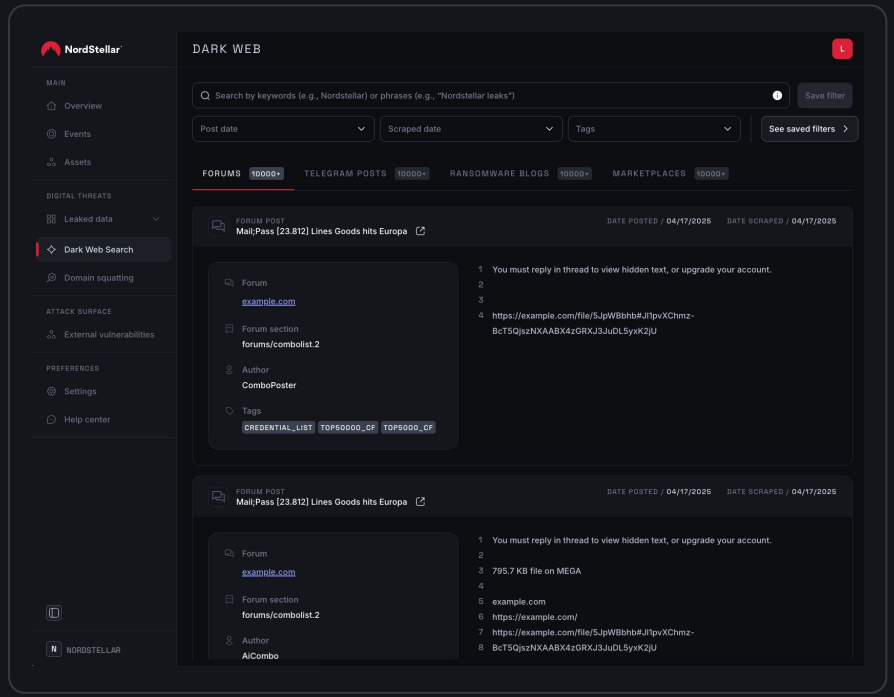
To monitor key assets on the dark web, we suggest tracking the following:

1. Organization-specific keywords

- ExampleCompany (full company name),
- ExampleCo (common abbreviation),
- “Project Athena” (internal project name),
- “John Smith” (high-profile employee PII),
- examplecompany.com (company domain),
- @examplecompany.com (company email pattern).

2. Event-specific keywords

- ExampleCompany ransomware,
- ExampleCompany leak site,
- ExampleCompany payment deadline (ransom payment deadline),
- ExampleCompany logs (company logs for sale/leaked).



Managing users and projects

Role-based access control (RBAC) provides flexible, project-based roles for secure, scalable user management—ideal for growing teams and MSPs.

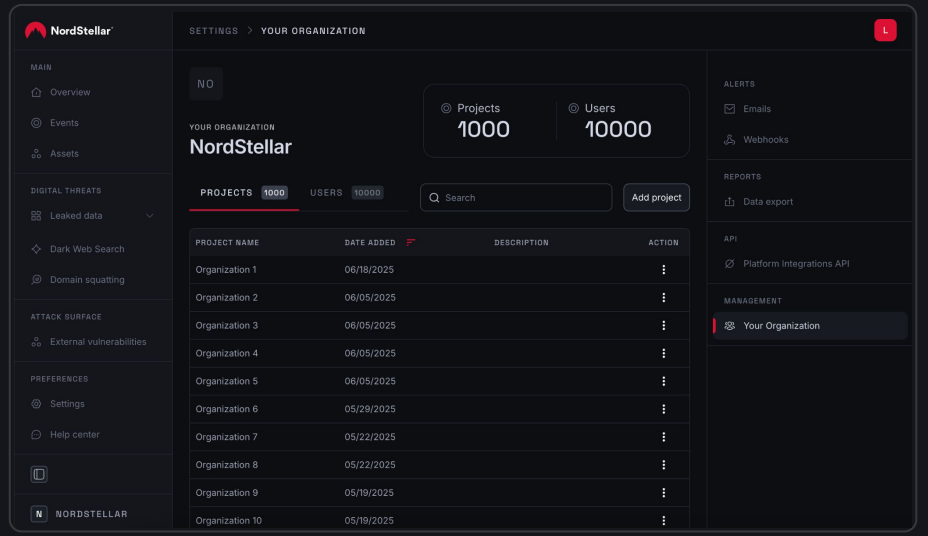
Roles overview:

1. **Org admin** (organization-wide): Full access. Manages users, roles, projects, and API keys. Always at least one Org admin required.

2. **Regular user** (per-project): Can manage assets, events, monitoring rules, filters, and view/export sensitive data.

3. **View only user** (per-project): Read-only access to all project data, including sensitive info—ideal for clients/stakeholders.

More about RBAC: NordStellar documentation.

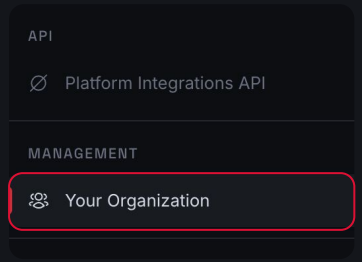


- Assign tailored permissions by project.
- Streamline onboarding and access control.
- Ensure users only access what they need.

Adding a new user

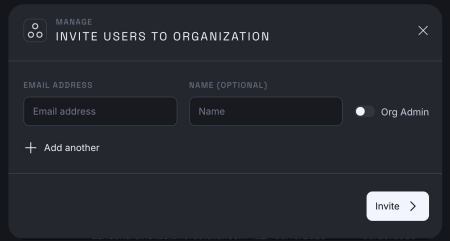
1

Go to Settings > Your Organization > Users



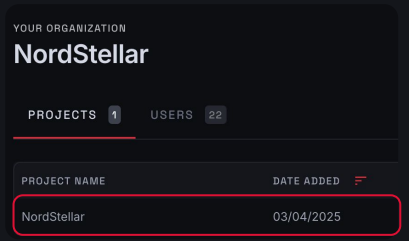
2

Click Invite new user, enter the user's information and click Invite*



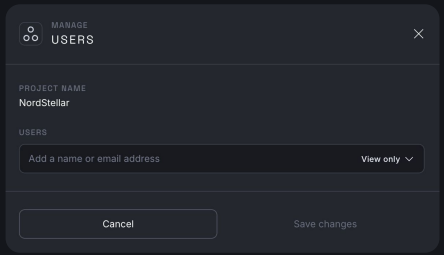
3

To grant access, go to Projects, select a project, then click Add to Project



4

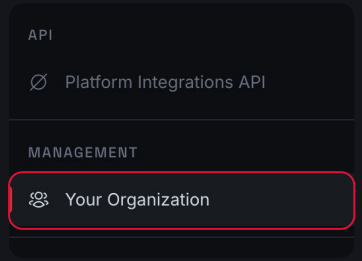
Choose the user and select a role: Regular or view-only



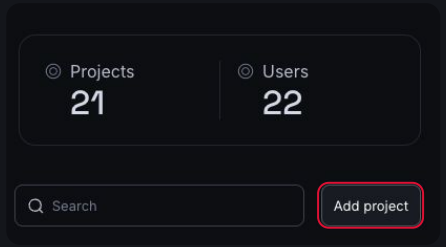
* Newly added users do not have access to any projects unless the Org Admin toggle is turned on. To give the newly created user regular or view-only access to selected projects, complete steps 3 and 4.

Adding a new project

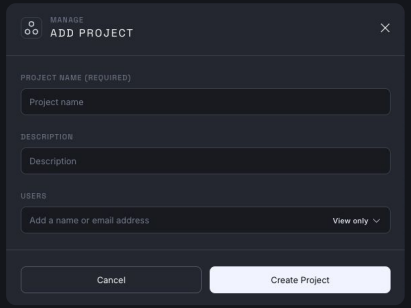
1. Go to Settings > Your Organization



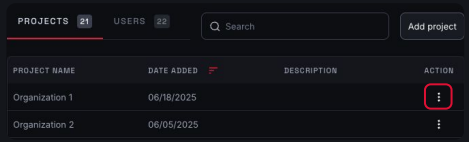
2. Click Add project



3. Enter the project name, description, and non-admin users*, then click Create Project



4. To edit a project, repeat step 1 and click the action button next to the project



* Org Admins have access to all projects by default. Only add non-admin users who need Regular or View-Only access. Users must already be invited (see Adding a new user, steps 1–2).

Alerts

NordStellar

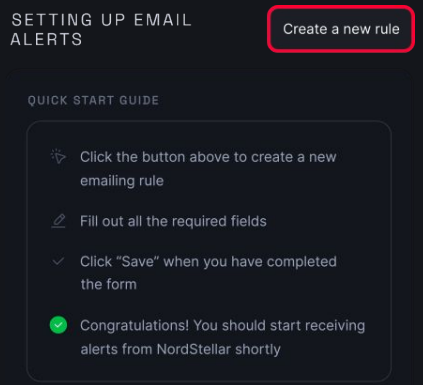
Setting up alerts

NordStellar

Setting up email alerts

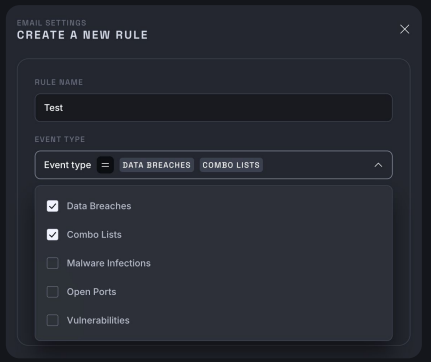
1

Go to Settings > Emails > Create a new rule



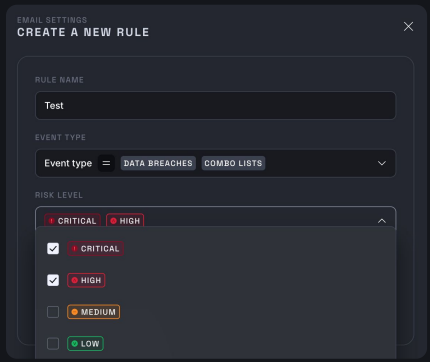
2

Name the rule and choose which events to track



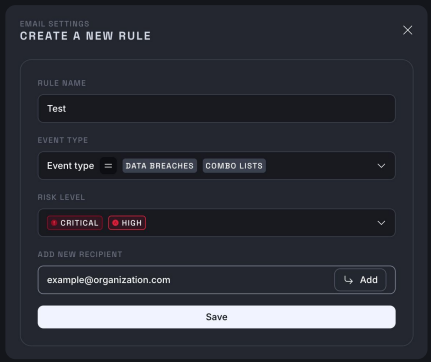
3

Select the risk levels that should trigger alerts



4

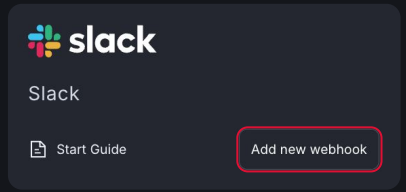
Add recipient email(s), click Add and Save



Setting up Slack alerts

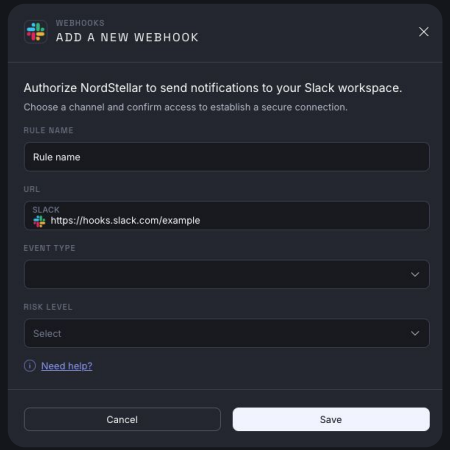
1

Go to Settings > Webhooks, then click Add new webhook in Slack card



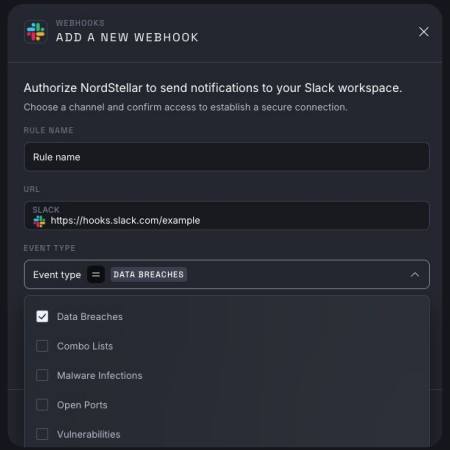
2

Name the rule and enter your Slack webhook URL



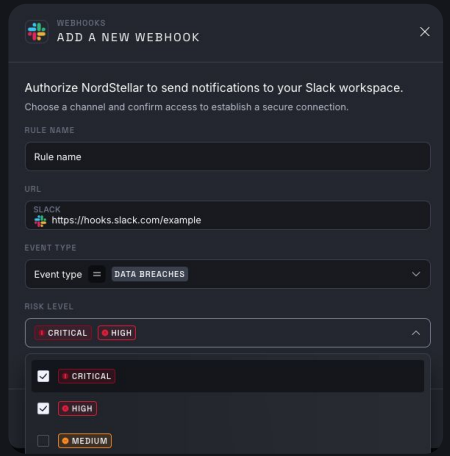
3

Choose the events that should trigger notifications



4

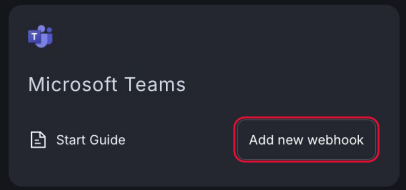
Select risk levels and click Save



Setting up Microsoft Teams alerts

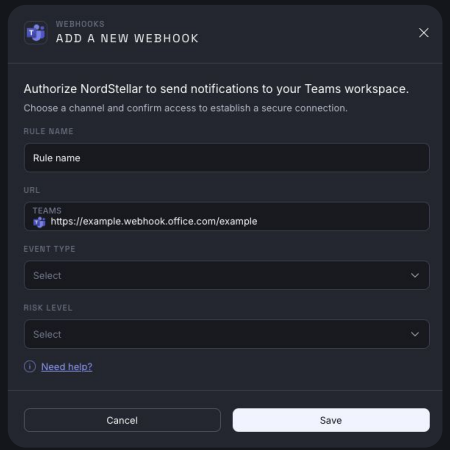
1

Go to Settings > Webhooks, then click Add new webhook in Microsoft Teams card



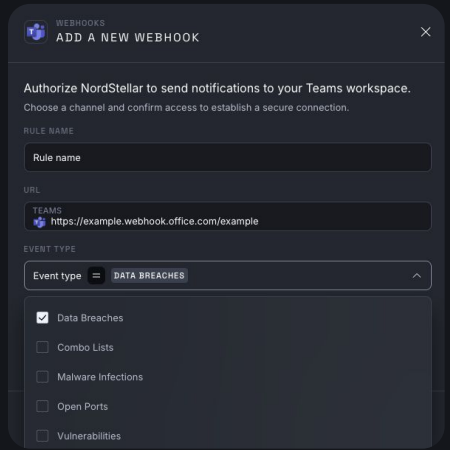
2

Name the rule and enter your Teams webhook URL



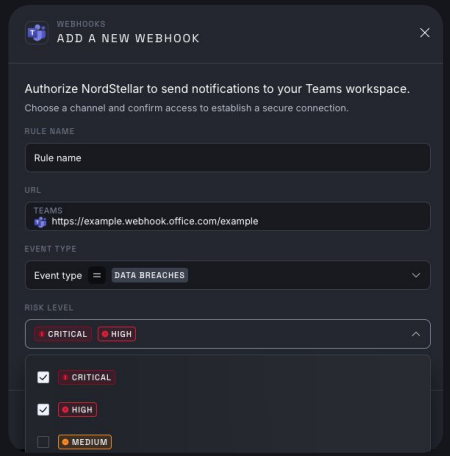
3

Choose the events that should trigger notifications



4

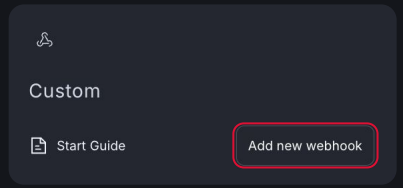
Select risk levels and click Save



Setting up generic webhook alerts

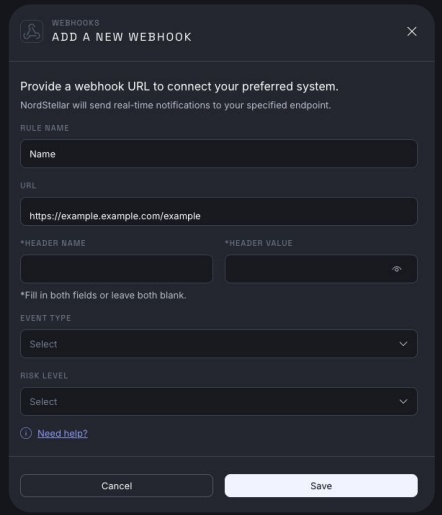
1

Go to Settings > Webhooks, then click Add new webhook in Custom card



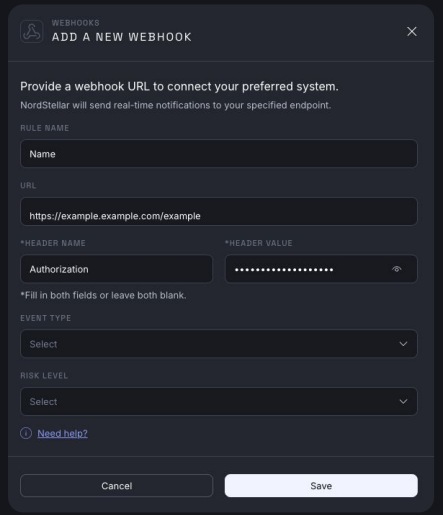
2

Name the rule, and paste your endpoint URL that accepts POST requests with JSON payloads



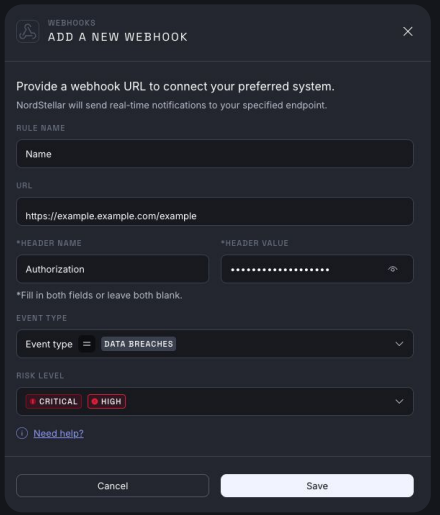
3

Optional: If your endpoint requires headers, fill in the Header name and Header value fields



4

Choose the events that should trigger notifications, select risk levels and click Save



Responding to alerts

NordStellar

Recommended responses to data leak alerts

Investigate and remediate

Conduct a thorough investigation into what caused the leak. Identify root causes, contain the damage, and put safeguards in place to stop it from happening again.

Implement MFA

Implement mandatory multi-factor authentication for all employees—and consumers, if possible—to protect accounts.

Logging and monitoring

Improve logging to detect and respond to suspicious activity more effectively. This includes monitoring access to sensitive data, system changes, and failed login attempts.

Security awareness training

Conduct comprehensive and regular security awareness training for all employees, focusing on password hygiene, phishing awareness, and social engineering tactics.

Recommended responses to external vulnerability alerts

Disable outdated protocols and ciphers

Turn off support for outdated TLS versions (1.1 and below) and weak cipher suites across all systems. Prioritize the use of TLS 1.3 and strong, modern ciphers.

Update and standardize configurations

Standardize SSL/TLS configurations across all subdomains and update regularly.

Disable weak SSH algorithms

Disable weak Diffie-Hellman key exchange algorithms, weak MAC algorithms, and CBC mode ciphers. Prioritize the use of strong, modern algorithms and key exchange methods.

Review SSH authentication methods

Ensure secure access by disabling password authentication where possible and using key-based authentication instead. If passwords are required, enforce strong password policies and MFA.

Recommended responses to suspicious domain alerts

Investigate the domain

Review registrar, WHOIS data, DNS records, and website content to identify abuse or impersonation.

Assess risk and gather evidence

Determine potential harm (phishing, brand abuse, etc.). Save screenshots, WHOIS info, and DNS data.

Report and escalate

Submit abuse reports to the registrar and hosting provider. File UDRP or DMCA complaints if applicable.

Report malicious activity & continue monitoring

Report to Google, Microsoft, and national CERTs. Continue monitoring via NordStellar.

Find a more detailed checklist in the NordStellar documentation.

Features

NordStellar

Main section

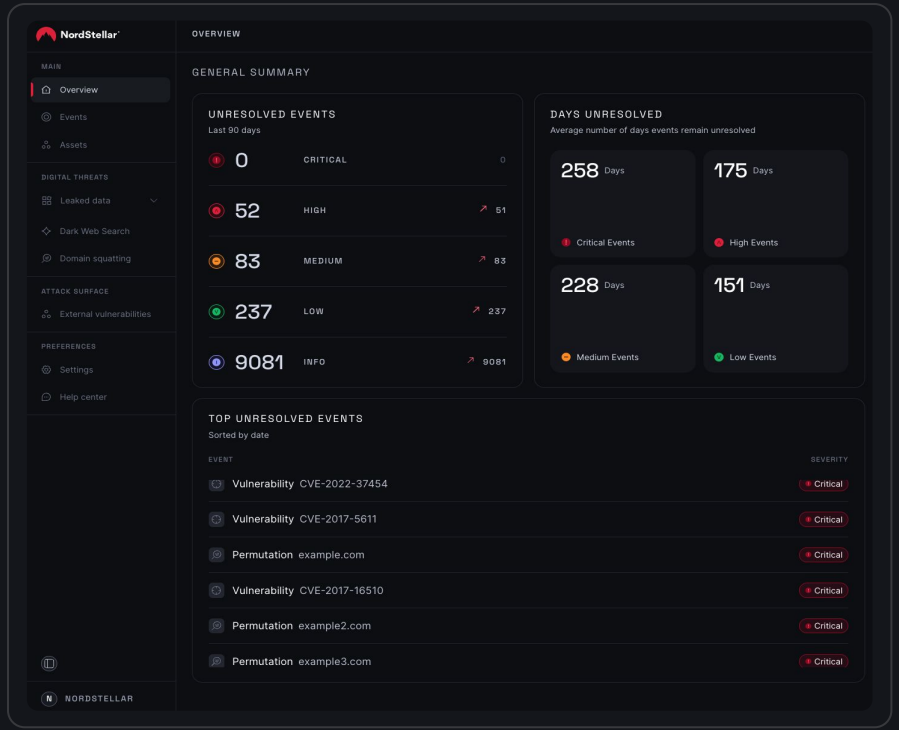
NordStellar

Overview

The *Overview* dashboard shows the key metrics of your organization's cyber threat exposure.

Risk levels are categorized based on incident severity:
Critical: Severe risk with significant potential impact
High: Serious risk with significant potential impact
Medium: Moderate risk
Low: Mild risk
Info: Low-priority issue with minimal potential impact

Risk level is determined by:
- Type and sensitivity of exposed data
- How recent the breach is
- Context-specific detection rules
- A predefined risk scoring framework
- CVE data evaluation, including CVSS and EPSS scores*



*CVE - common vulnerabilities and exposures, CVSS - common vulnerability scoring system, EPSS - exploit prediction scoring system

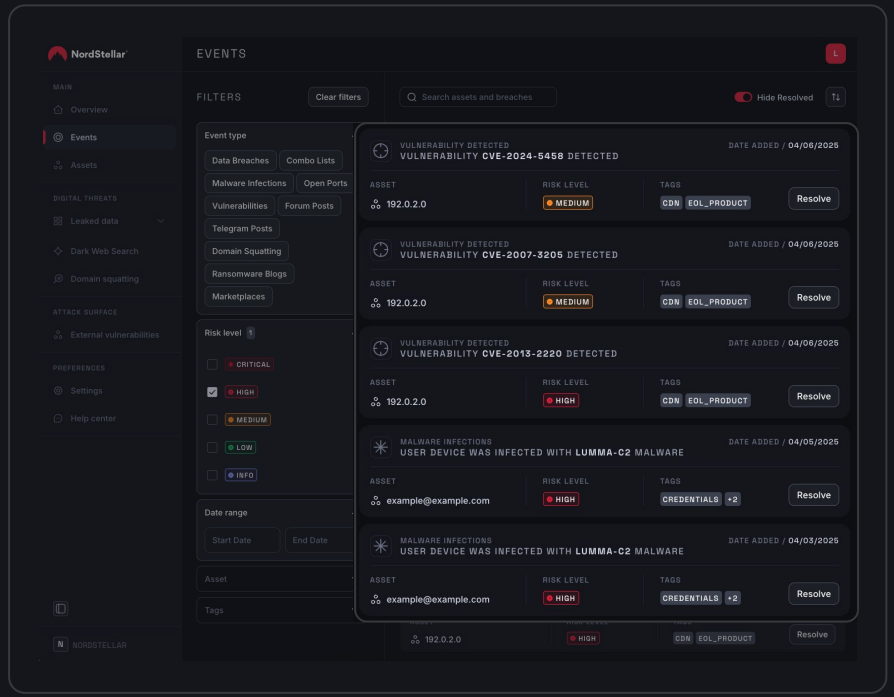
Events

The *Events* page gives you a real-time view across your monitored assets and rules.

We recommend to visit the *events* section right after asset approval. You can then:

- Review incidents from the last 6-12 months
- Prioritize and address high-risk events
- Mark reviewed items as Resolved

- Stay ahead with real-time updates on security events.
- Prioritize remediation of high-risk vulnerabilities.
- Improve overall security posture.



Assets

The *Assets* page is where you manage your organization's assets—add or edit anything you monitor.

NordStellar asset status:

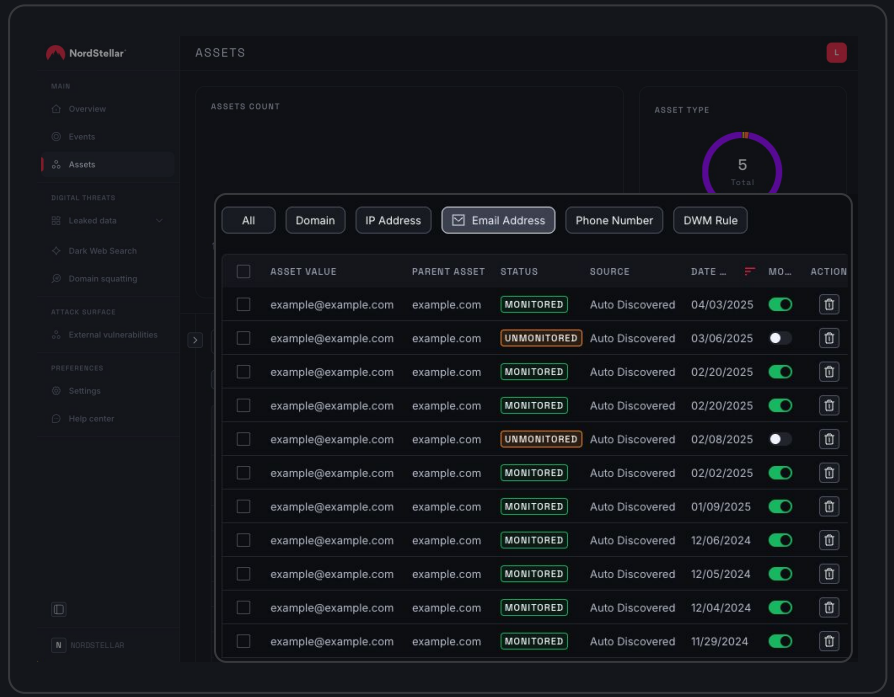
Monitored: the asset is being actively monitored within the NordStellar platform

Unmonitored: the asset is added but not currently being monitored (toggled OFF)

Orphaned: assets that were pulled in automatically (e.g. IP addresses linked to a domain via AWS or Cloudflare)

Pending: these assets are awaiting ownership verification by the NordStellar team. These appear greyed out until approved.

Maintain clear visibility of your critical assets.



Digital threats

NordStellar

Leaked data: Metrics

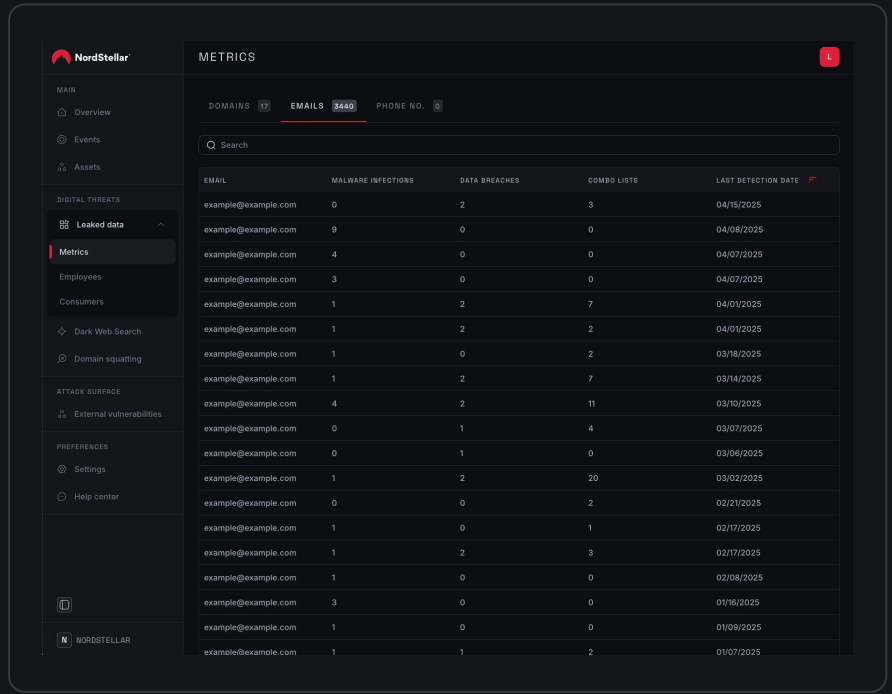
The *Leaked data* module scans for exposed data tied to your organization, including:

- Domain names: Linked to leaks from malware or combo lists
- Emails/phone numbers: Corporate and personal contacts flagged if exposed

It detects leaks from:

- Data breaches
- Malware infections (infostealers)
- Combo lists (credential dumps)

- Minimize damage from leaked data.
- Recover compromised user accounts.
- Prevent cybercriminals from using or selling them.



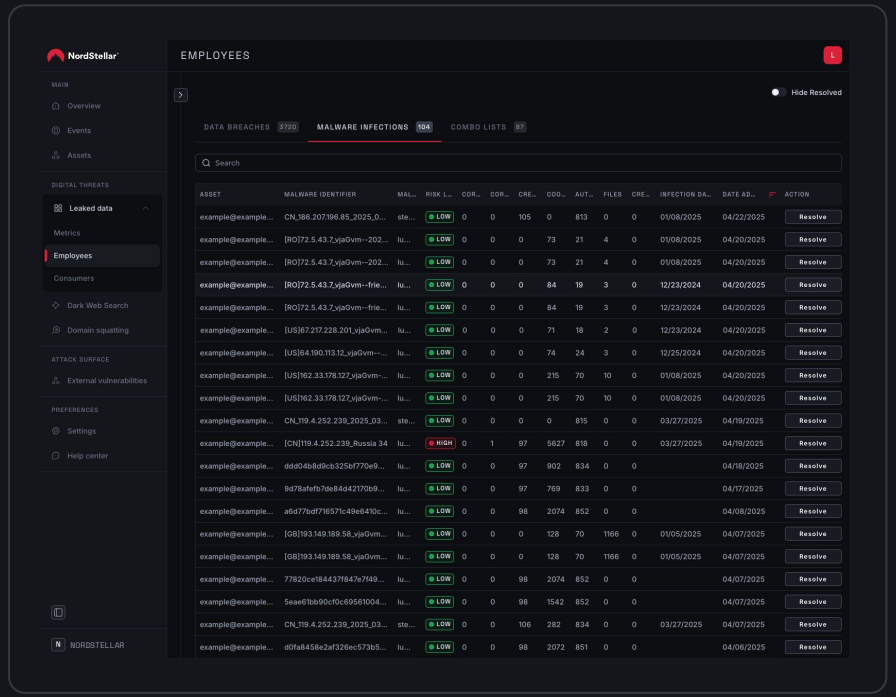
Leaked data: Employees

In the *Employees* page, you can:

- Filter events by type, risk level, date range, or asset
- Sort results by date added or risk level
- View event details by clicking any entry (see *Event details* section)
- Mark events as Resolved after reviewing them

In case of data leak: recommended actions.

Proactively identify and respond to employee data leaks.



Leaked data: Consumers

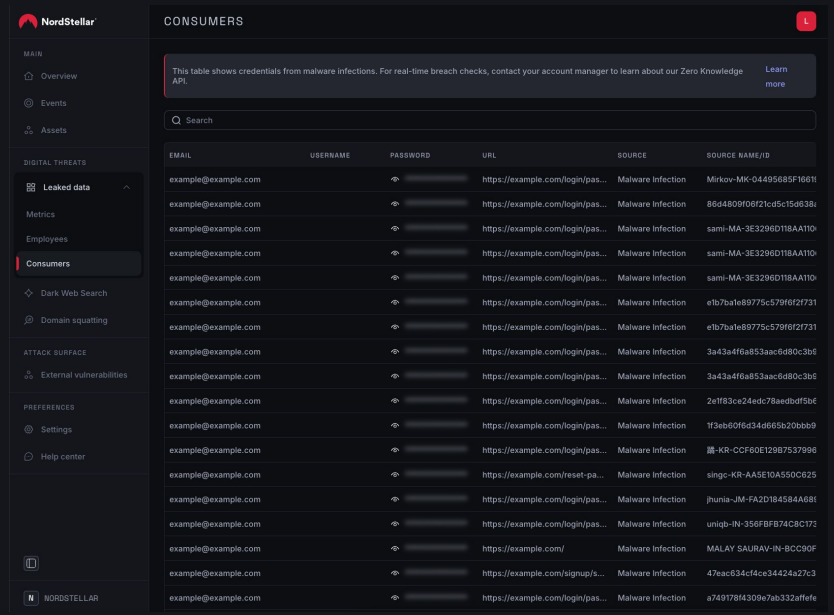
The functionality available in *Consumers* view:

- Customer credentials table: shows leaked customer credentials including email, username, password, and the URL of the login page

- Source information: each entry displays the source (either malware infection or combo list), source name, infection date, and date the leak was added to the system

In case of data leak: Check our recommended actions.

Quickly detect and respond to leaked consumer credentials.



Dark web search (1)

Dark web search lets you explore key data sources for potential threats: Forum posts, Telegram posts, ransomware blogs, and marketplaces. Use keywords, phrases, or advanced queries to search across them all.

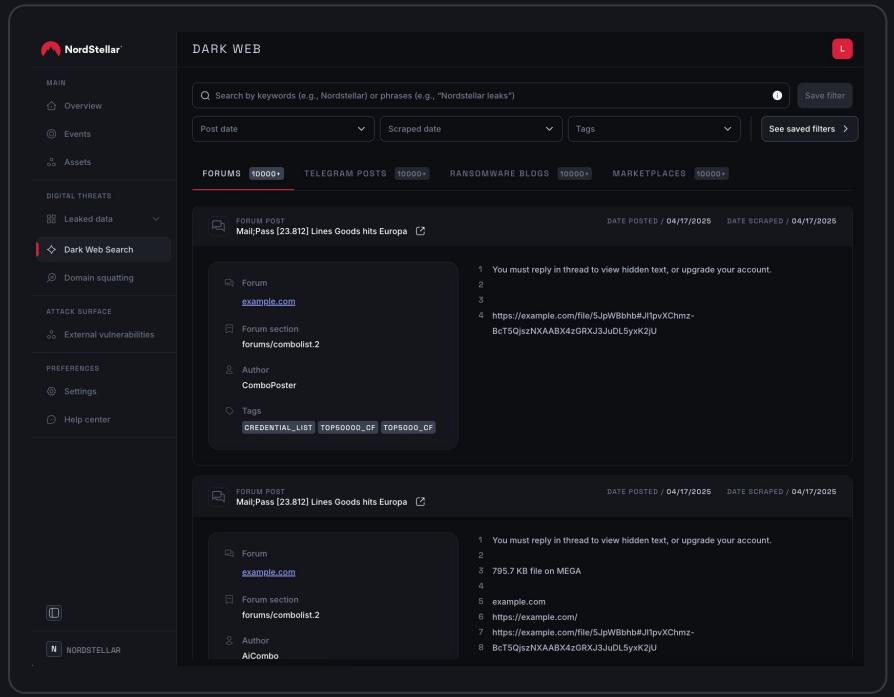
1. Enter your search terms in the search bar:
   - Use single keywords
   - Use quotes for exact phrase matches
   - Use boolean operators (AND, OR, NOT) or Lucene syntax for complex queries

2. Set search parameters (optional):
   - Tags: Filter results by monitored categories
   - Date range: Focus on a specific timeframe

3. Click Search to run your query

4. Click See more to view the full content of a post (if available).

- Actively search for emerging threats and indicators of compromise.
- Explore topics and trends within specific online communities.



Dark web search (2)

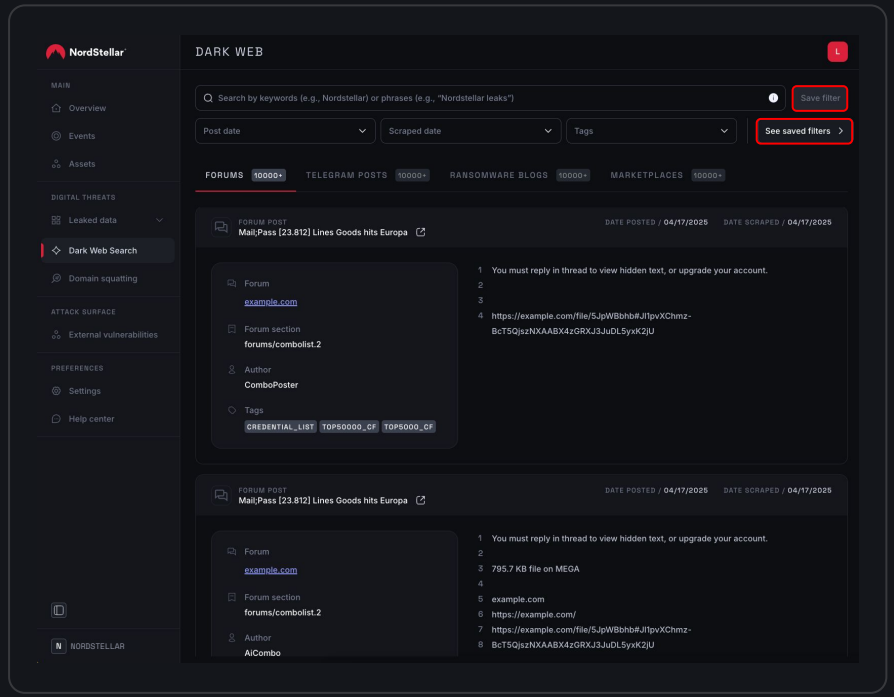
Running the same query regularly? You can save the search filter for convenient future use:

1. Follow the steps in the previous slide, and click Save filter
2. In the modal, fill in the required fields and click Save

Applying a saved filter to your query:

1. Click See saved filters button.
2. Hover over a filter and click Apply filter to use it for your search

- Easily perform repetitive search with the same filters.
- Manage threat exposure for multiple organizations from a single account.



Domain squatting

Domain squatting monitoring starts automatically when you add a domain to your Assets list*. It detects malicious registrations that mimic your brand—helping you stay ahead of phishing, malware, and impersonation attempts.

It uses multiple techniques to identify and assess threats:

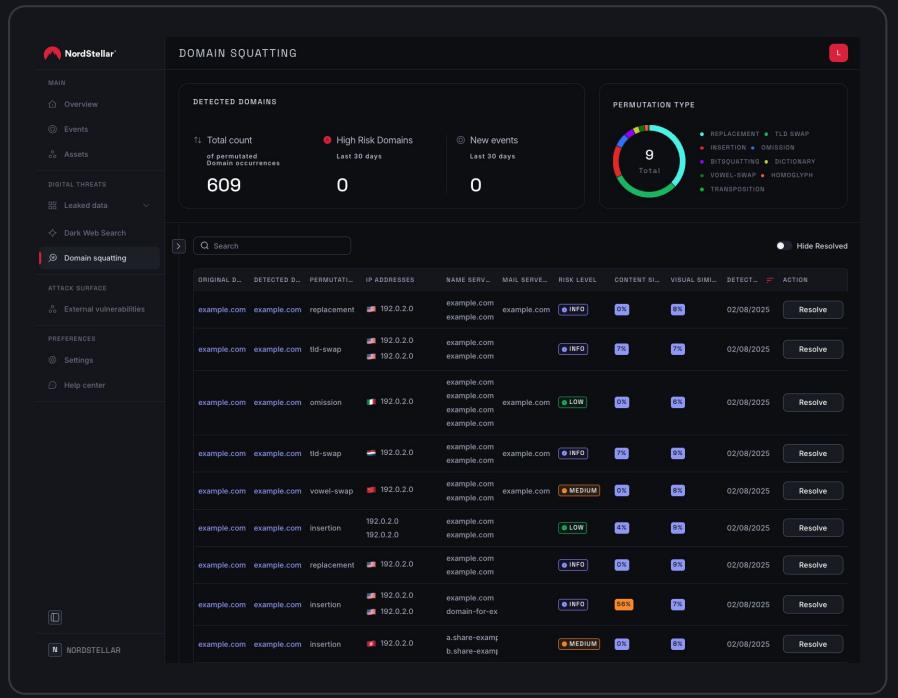
- Continuous monitoring: NordStellar uses dnstwist to generate domain variations and monitor for new or suspicious registrations in real time

- Risk analysis: Each detected domain is evaluated using similarity algorithms, threat intelligence feeds, and WHOIS data. You'll get details on threat type, confidence, severity, and recommended actions

- Deep investigation: For each flagged domain, NordStellar shows screenshots, redirect chains, WHOIS records, and similarity scores

*Monitoring is active only after asset approval.

- Immediately identify fraudulent or malicious domain registrations.
- Prevent reputational damage and phishing attacks.



Attack surface management

NordStellar

Attack surface management

Attack surface management (ASM) gives you continuous visibility into your organization's external exposure.

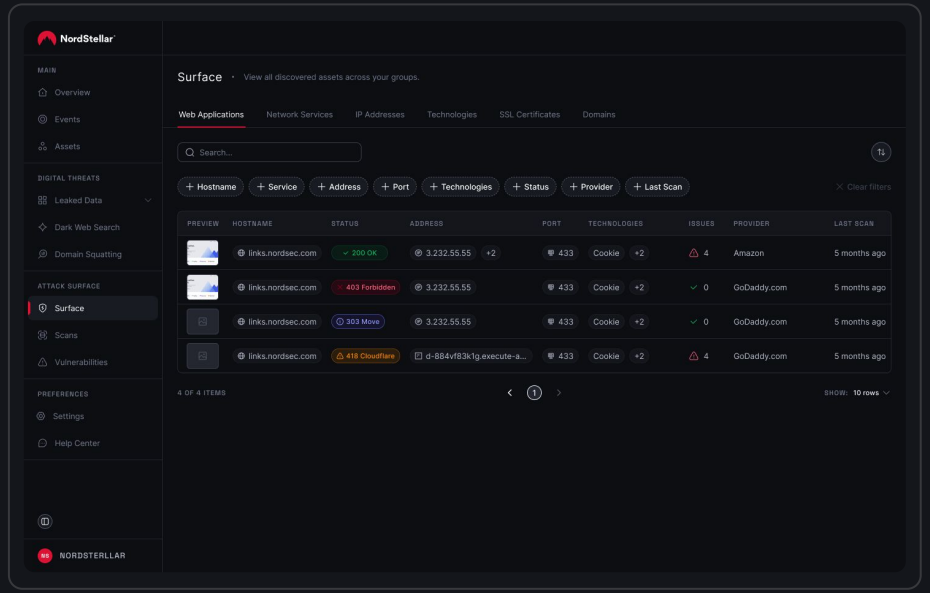
Surface: View all discovered assets across web applications, network services, and other groups.

Scans: Schedule, manage and monitor your security scans across all assets.

Vulnerabilities: View and manage all security vulnerabilities across your assets and infrastructure. You may sort and prioritize them by risk level.

ASM not only detects, but also verifies vulnerabilities by testing them.

- Gain full visibility into your entire attack surface.
- Identify and close exploitable gaps before attackers do.



Need help getting started?

Reach out to your account manager
Check out NordStellar documentation