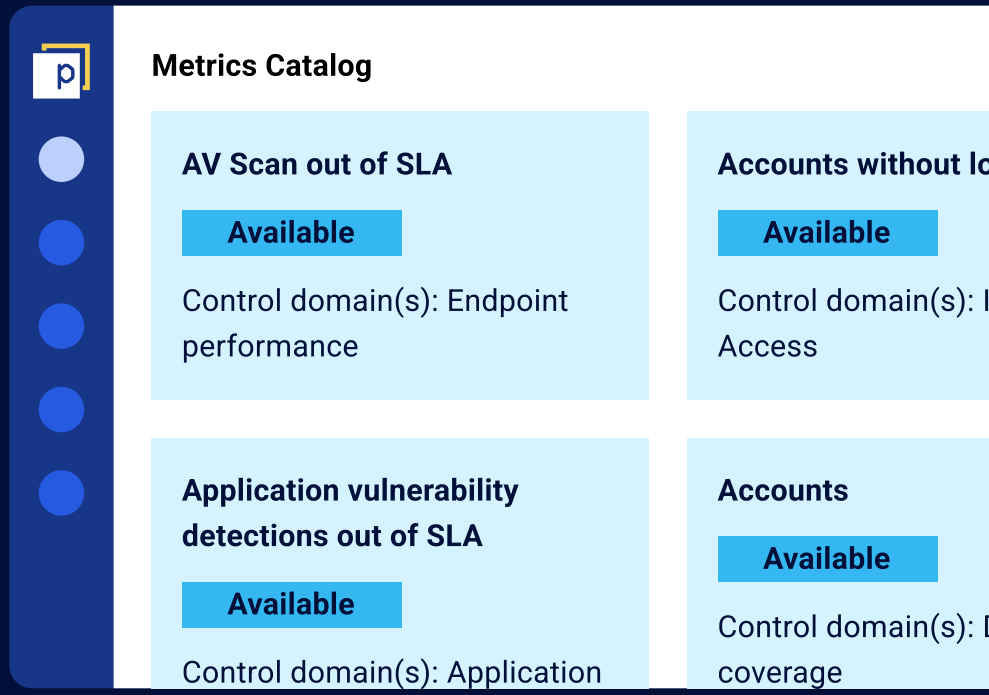
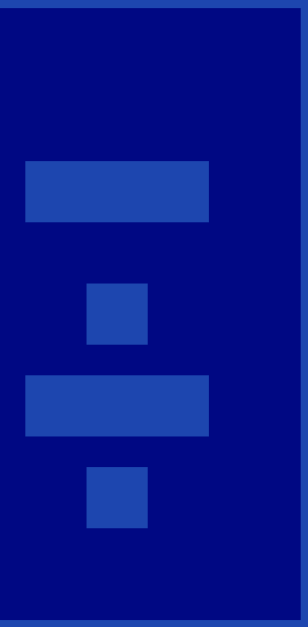
panaseer

Metrics Catalog

A guide to metrics and measurement on the Panaseer platform





What will we cover in this guide?

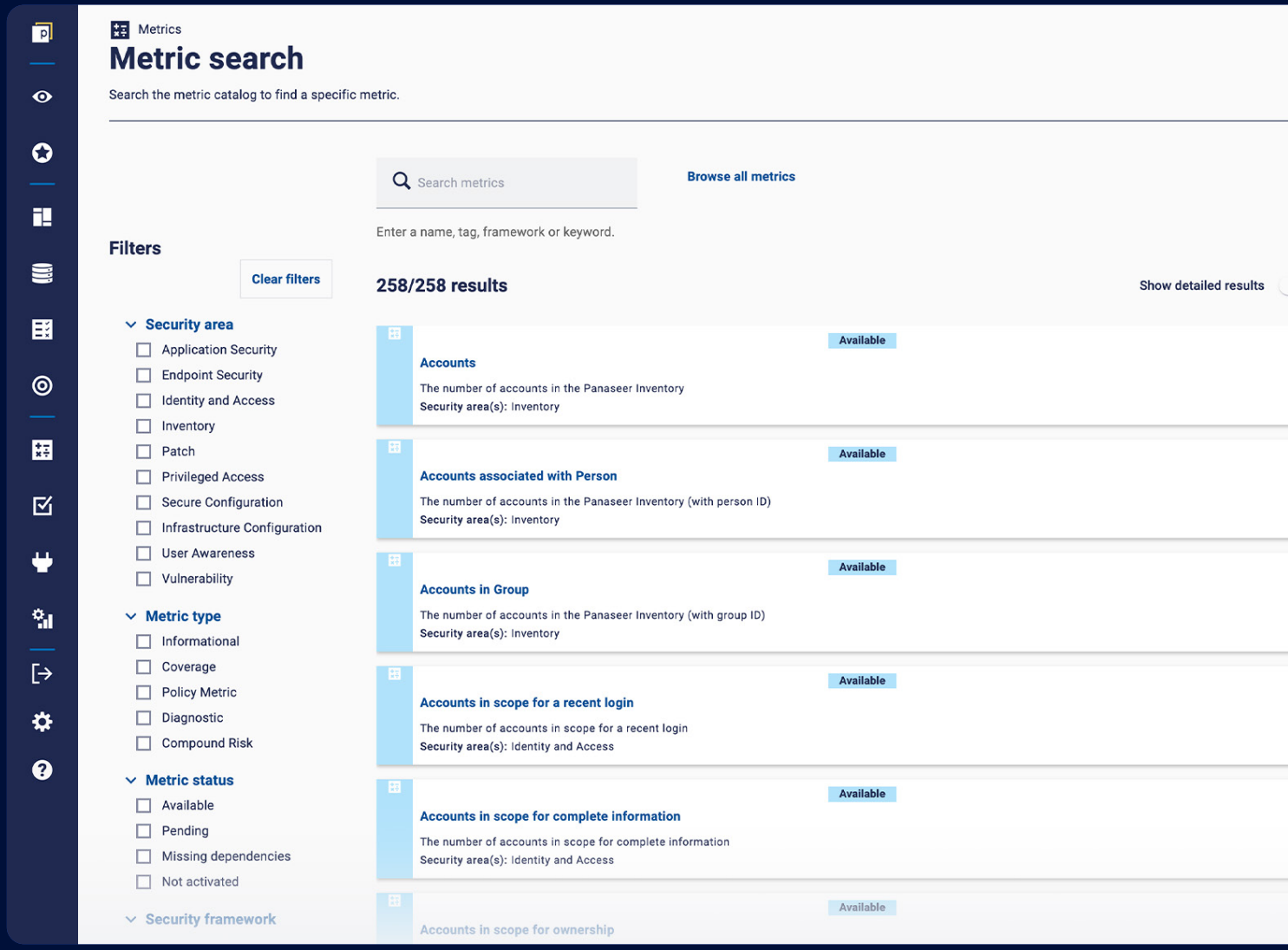
Introduction to metrics and measurement in the Panaseer platform

Panaseer provides the technology, tooling, insight, and guidance to build your organization's metrics program on your terms, allowing you to adapt it to the ever-changing security landscape.

We can support any level of metrics maturity, whether you're laying the foundations or have an advanced program.

In this section, we will cover:

- The Panaseer platform
- Metric types
- Asset types
- Dimensions
- Visualizations



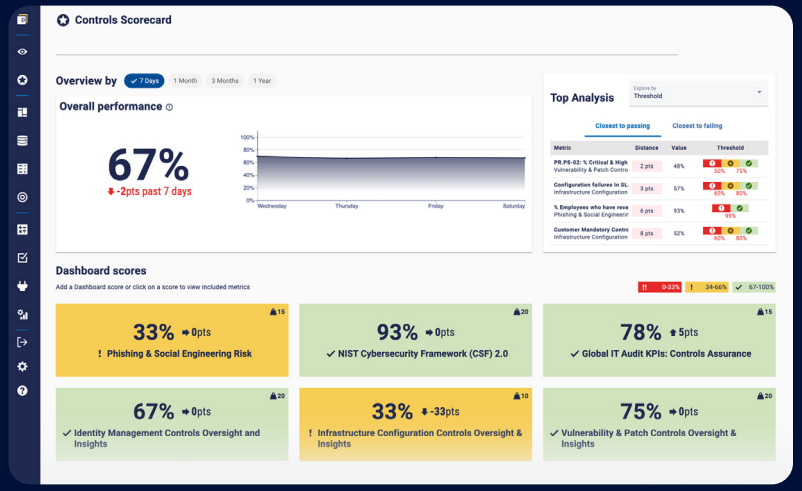
The Panaseer platform

Panaseer is an automated cybersecurity data analytics platform. It provides metrics and measures across ten cyber control domains:

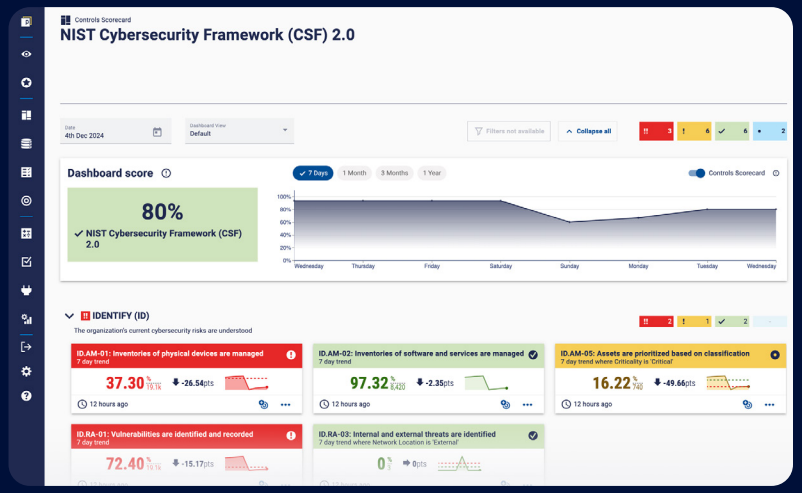
1. Device and Coverage
2. Vulnerability management
3. Endpoint Protection
4. Patch Management
5. Application Security
6. Identity and Access Management
7. Privileged Access Management
8. User Awareness
9. Cloud Configuration
10. Infrastructure Configuration

Panaseer empowers cybersecurity risk and assurance leaders in complex enterprises to manage risk and reduce control failures. Our Continuous Controls Monitoring (CCM) platform provides daily objective insights into controls coverage, effectiveness and performance. This helps to address hidden risks, strengthen governance, speed up compliance reporting, and maintain continuous audit readiness.

We ingest data from security, IT and business tools, creating connections and relationships between previously disparate data points, even where there were missing data fields previously. The output is a clear view of control owners and the assets they're accountable for. This is mapped to an objective measurement of controls effectiveness and the criticality levels determined by business factors such as services, division or region.



Cybersecurity Controls Scorecard overview



NIST cybersecurity framework (CSF) v2.0 dashboard

Metric types

A quick introduction to the types of metrics in the Panaseer platform and the value they provide.

Informational

Informational measures are straightforward counts and sums. For example, total number of vulnerabilities, or total number of Windows 7 machines. They are the building blocks for many of our more complex measurements.

Diagnostic

If you have identified areas of sub-par performance using policy metrics, diagnostic metrics provide more in-depth insight that helps you to narrow down the root cause and quickly identify actions that help reduce risk.

Policy

Policy metrics allow you to track adherence to your internal policies. This can be your organization's unique policies configured in the platform or compliance with regulatory standards and established frameworks.

Coverage

Coverage metrics provide essential context for any performance measures. It's measurement best practice track the coverage and completeness of the data sources. For example, a vulnerability scanner will only provide data on devices it scans, so you need to know what it isn't scanning.

Compound risk

Compound risk metrics combine metrics from across multiple domains to identify "toxic combinations" of risks and control failures. For example, they allow you to prioritize patching critical vulnerabilities on devices that don't have an endpoint solution in place. This is combining metrics from our patch, vulnerability and endpoint domains so you can focus on specific attack paths.

Asset types

Panaseer's metrics and measures are underpinned by comprehensive, interlinked asset inventories. This enables you to take a flexible approach, pivoting metrics to focus on different asset types.

For example, you can measure the number of servers with vulnerabilities, but then via asset linking, you can see what applications these servers host to also measure the number of applications with vulnerable servers. This allows you to focus on the asset types relevant to your objectives.

Devices, including user devices, servers, virtual machines, mobile devices, IoT, cloud infrastructure.

People, including everyone from contractors to permanent staff, with information about their title, line manager and other relevant context, such as any assets and applications they own.

Applications, including in-house, business critical applications such as payment systems, and trading systems.

Accounts, including those across Windows, Linux and Unix, both centrally managed (e.g. via Active Directory) and local, both on-prem and in the cloud.

Databases, that support your business applications, including information directly from the systems themselves or from administration tooling

Dimensions

Dimensions are the properties in the underlying data you can use to break down metrics and measures.

All metrics can be pivoted and filtered by many dimensions to focus on different asset types or areas of the business. For example, you can explore the % of outstanding out-of-policy patches (patch focused) and the % of devices with outstanding out of policy patches (device focused).

This capability can handle complex standards with different values to different subsets of your assets, allowing you to see an overall measure of policy compliance, even when the value of the standard varies. For example, you may have set an internal standard of applying patches within 30 days for servers hosting business critical, internet-facing applications and within 90 days for all other servers. Different standards can be applied based on various combinations of dimensions, such as device type, device criticality, vulnerability severity and other factors, based on your risk appetite.

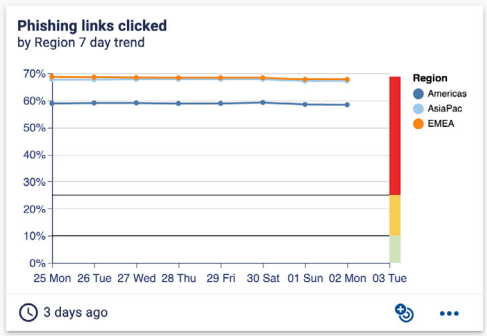
The table (right) shows some of the dimensions our customers commonly use.

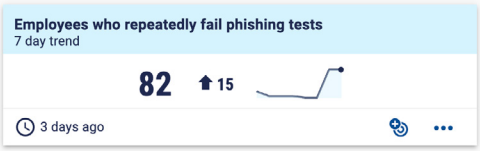
Type	Example Dimensions
Business - Organisational	Division
	Business unit
	Department
	Team
Business - Geographical	Region
	Country
	City
Devices	Device type
	Device subtype
	Operating system type
	Device criticality
	Environment type
	Network location
	Functional role
People	Job title
	Job category
	Employment type
	Line manager
Applications	Category
	Owner
	Confidentiality
	Availability
	Integrity
	Criticality
	Environment type
Accounts	Account type (service, vault etc.)
	Account subtype
	Status (active/disabled)

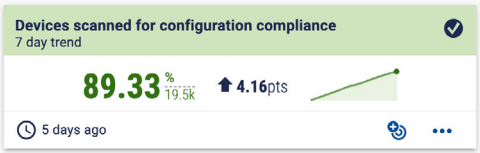
Visualizations

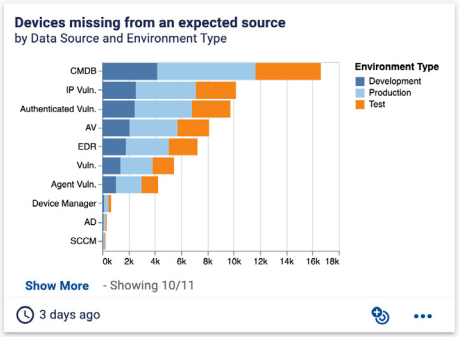
To help make the data easy to understand, you can choose the type of visualization that's best suited to each metric, using our suite of best practice options.

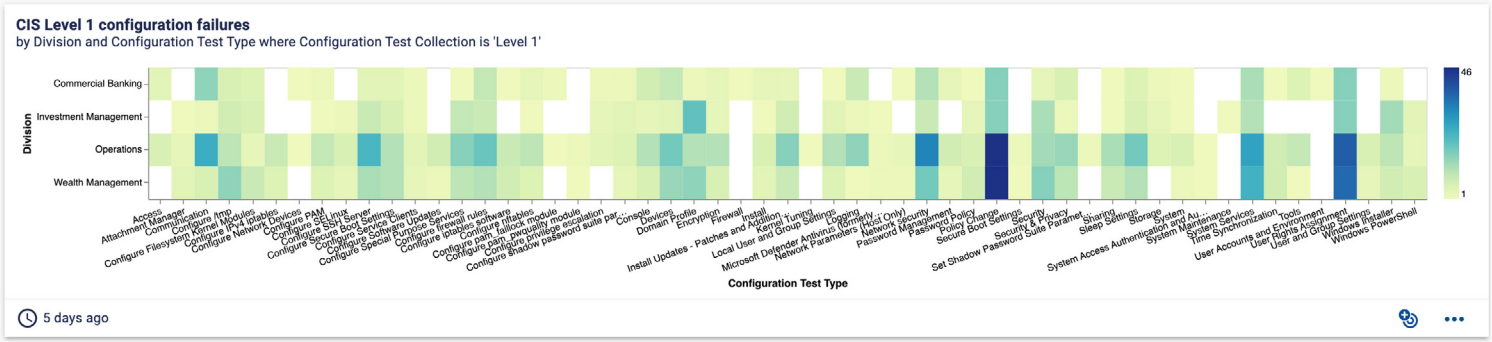
Some examples include metric cards, stacked column chart, stacked bar chart, multi-line time series chart with thresholds, spark line trellis chart with thresholds, interactive table, and heatmap.











Device and Coverage

The Device and Coverage domain provides assurance that all your devices are running the required security tools and controls.

Panaseer ingests data from sources across your security, IT and business tools, to create comprehensive asset inventories. This allows you to compare the coverage of all your data sources against the Panaseer inventory.

For example, you can ensure that all devices are in the CMDB, along with useful information brought in from other tools; have the right endpoint tools deployed; or are being picked up by your vulnerability scanners. And so much more.

Benefits

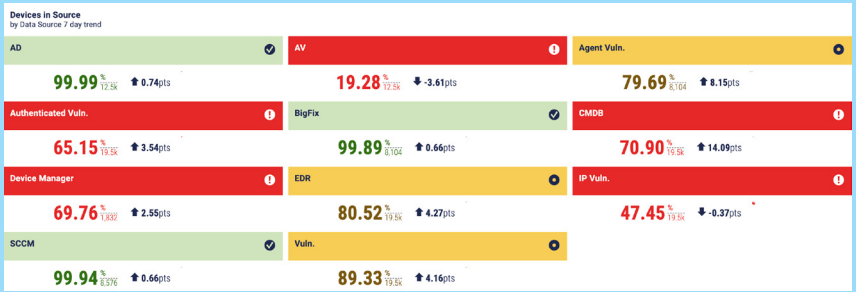
- Validate the coverage of the tools and controls running on your devices.
- Find gaps in the coverage of your tools and controls.
- Prioritize remediation of coverage gaps based on business risk.
- Consolidated, validated view of data from a range of tools
- Measure performance against your SLAs and track changes.

Example data sources

Entra ID / Azure AD | ServiceNow | SentinelOne | CrowdStrike | Tenable IO

Spotlight metric

Performance across controls



This dashboard provides coverage metrics for a range of security tools. It essentially tells you what percentage of your devices are present on that tool. Whether it's devices recorded in the CMDB, devices protected by EDR, or devices scanned by your vulnerability scanner. These coverage metrics are crucial for providing context of what you're measuring but also highlight gaps in coverage that you can fix to improve your overall security posture.

Type	Metric Name	Description
Informational	Devices With Control Check Failures	The number of devices in the Panaseer Inventory that have a status of Failed
Informational	Devices With Control Check Status	The number of devices in the Panaseer Inventory that have a status
Informational	Devices failures (percentage)	The percentage of devices failed
Informational	Accounts in Group	The number of accounts in the Panaseer Inventory (with group ID)
Informational	Accounts associated with Person	The number of accounts in the Panaseer Inventory (with person ID)
Informational	Hosted Applications	The number of hosted applications in the Panaseer Inventory (with device ID)
Informational	Applications associated with Person	The number of applications in the Panaseer Inventory (with person ID)
Informational	Devices hosting Application	The number of devices in the Panaseer Inventory (with app ID)
Informational	Devices associated with Person	The number of devices in the Panaseer Inventory (with person ID)
Informational	Groups containing Account	The number of groups in the Panaseer Inventory (with account ID)
Diagnostic	Applications never vulnerability scanned	The number of applications that have never been scanned for vulnerabilities
Coverage	Cloud accounts in CSPM	The number of cloud accounts that are in the CSPM
Coverage	Cloud accounts not in CMDB	The number of cloud accounts that are not in the CMDB
Coverage	Cloud accounts not in CSPM	The number of cloud accounts that are not in the CSPM
Informational	Accounts	The number of accounts in the Panaseer Inventory
Informational	Applications	The number of applications in the Panaseer Inventory
Informational	Cloud Accounts	The number of Cloud Accounts in the Panaseer Inventory
Informational	Databases	The number of databases in the Panaseer Inventory
Informational	Devices	The number of devices in the Panaseer Inventory (with granular filters available)
Diagnostic	Devices expected in at least 1 control	The number of devices expected in at least 1 control
Diagnostic	Devices expected in at least 2 controls	The number of devices expected in at least 2 controls
Diagnostic	Devices expected in at least 3 controls	The number of devices expected in at least 3 controls
Diagnostic	Devices missing from at least 1 control	The number of devices missing from at least 1 expected control
Diagnostic	Devices missing from at least 2 controls	The number of devices missing from at least 2 expected controls
Diagnostic	Devices missing from at least 3 controls	The number of devices missing from at least 3 expected controls

Type	Metric Name	Description
Informational	Devices	The number of devices in the Panaseer Inventory
Informational	Groups	The number of groups in the Panaseer Inventory
Informational	People	The number of people in the Panaseer Inventory
Informational	Installed Software	The number of installed software in the Panaseer Inventory
Diagnostic	Devices missing from at least 1 control	The percentage¬†of devices expected in but missing from at least 1 control
Diagnostic	Devices missing from at least 2 controls	The percentage¬†of devices expected in but missing from at least 2 controls
Diagnostic	Devices missing from at least 3 controls	The percentage¬†of devices expected in but missing from at least 3 controls
Compound risk	Device coverage and Vulnerabilities with owner phishing tests	The number of devices with vulnerabilities and who's owner has received a phishing test
Compound risk	Vulnerability detections with device coverage information	The number of vulnerability detections on devices (includes devices tool coverage information)
Compound risk	Unique Devices associated with People	The number of devices with relationships to people
Compound risk	Unique Devices hosting Application	The number of devices in the Panaseer Inventory hosting applications
Compound risk	Unique Devices not hosting Application	The number of devices in the Panaseer Inventory not hosting applications
Compound risk	Unique People without Standard Accounts	The number of People without standard accounts
Compound risk	Unique People without Standard Accounts (internal)	The number of People without standard accounts (internal)
Informational	Business Services	Number of business services in the Panaseer Inventory.
Informational	Business Services	Number of business service offerings in the Panaseer Inventory.
Informational	Devices (granular filters)	Number of devices in the Panaseer Inventory (with granular filters available).
Informational	Service Instances	Number of service instances in the Panaseer Inventory.
Informational	Devices with Software	Number of devices with software installed.
Diagnostic	Devices with software (%)	Percentage of devices with software installed.
Policy	Devices expected in AD / agent scan / authenticated scan / AV / BigFix / CMDB / device manager / EDR / IP scan / SCCM / vulnerability scan	Number of devices expected in each respective tool or scan.

Type	Metric Name	Description
Policy	Devices missing from AD / agent scan / authenticated scan / AV / BigFix / CMDB / device manager / EDR / IP scan / SCCM / vulnerability scan	Number of devices expected in but missing from each respective tool or scan.
Policy	Devices missing from AD / agent scan / authenticated scan / AV / BigFix / CMDB / device manager / EDR / IP scan / SCCM / vulnerability scan (%)	Percentage of devices expected in but missing from each respective tool or scan.
Compound Risk	Unique applications hosted on devices	Number of unique applications hosted on devices in the organization.
Compound Risk	Unique Devices without Owner	Number of devices in the Panaseer Inventory without an owner.

Vulnerability Management

The Vulnerability Management domain helps organizations to respond faster, work more effectively, and more easily comply with and report on SLAs.

Panaseer provides essential oversight to support controls governance and assurance. The platform automates analysis of vulnerability data combined with your unique business context. This allows you to manage vulnerabilities and controls performance more effectively. IT operations and asset and risk owners can use near real-time analysis to handle business risks more effectively. Compliance teams get continuous oversight of controls assurance, mapped to NIST CSF and other frameworks.

Benefits

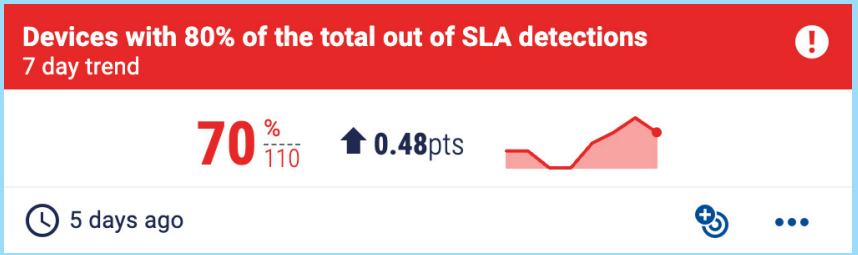
- Validate your controls coverage.
- Prioritize remediation of vulnerabilities based on business risk.
- Consolidated, validated view of data from all vulnerability tools.
- Measure performance against your SLAs, such as scan frequency and remediation frequency.
- Measure performance against established frameworks.
- Root cause analysis, from hot spots to data inspection.
- Support company-wide rapid response to known zero-day exploits.

Example data sources

Qualys | Tenable IO | Rapid7

Spotlight metric

Vulnerability outlier analysis



Find and fix the small group of devices responsible for 80% of vulnerability detections exceeding your SLA.

Our vulnerability outlier analysis helps you reduce the largest number of vulnerabilities with the least effort, ensuring you're using your remediation resources more efficiently.

Type	Metric Name	Description
Diagnostic	Vulnerability detections by vulnerabilities	The number of vulnerability detections by vulnerabilities
Informational	Vulnerability detections (High Cardinality)	The number of vulnerability detections (High Cardinality)
Diagnostic	Top Ten Devices with the Most out of SLA Vulnerability Detections	The 10 devices with the most out of SLA vulnerability detections
Diagnostic	Out of SLA detections on the worst 50 devices	The out of SLA vulnerability detections on the 50 devices with highest number of out of SLA vulnerability detections
Policy	Vulnerability detections out of SLA	The number of vulnerability detections that are out of SLA
Diagnostic	Top Ten Devices with the Most Vulnerability Detections	The 10 devices with the most vulnerability detections
Diagnostic	Top Ten Unique Vulnerabilities with the Most Detections	Top ten unique vulnerabilities with the most vulnerability detections
Policy	Vulnerability detections that satisfy SLA	The number of vulnerability detections that satisfy SLA
Coverage	Vulnerability detections with SLA	The number of vulnerability detections included in SLA analysis
Informational	Vulnerability detections	The number of vulnerability detections
Policy	Devices with 80% of the total out of SLA detections (device/region)	The smallest number of devices that account for 80% of the total out of SLA vulnerability detections (device/region)
Policy	Devices with 80% of the total out of SLA detections	The smallest number of devices that account for 80% of the total out of SLA vulnerability detections
Policy	Devices with out of SLA detections	The number of devices that have out of SLA vulnerability detections
Informational	Devices with vulnerability detections	The number of devices with vulnerability detections
Informational	Unique vulnerabilities	The number of unique vulnerability signatures
Diagnostic	Average age of vulnerability detections	The average age (days since first detection on device) of vulnerability detections
Policy	New vulnerability detections in influx	The percentage of vulnerability detections that satisfy SLA
Policy	Out of SLA detections on the worst 50 devices	The percent of out of SLA vulnerability detections found on the 50 devices with highest number of out of SLA vulnerability detections
Policy	Vulnerability detections out of SLA	The percent of vulnerability detections that are out of SLA
Policy	Devices with 80% of the total out of SLA detections (device/region)	The smallest percent of devices that account for 80% of the total out of SLA vulnerability detections (device/region)
Policy	Devices with 80% of the total out of SLA detections	The smallest percent of devices that account for 80% of the total out of SLA vulnerability detections
Policy	Devices with out of SLA detections	The percent of devices with detections that have out of SLA vulnerability detections
Compound risk	Device coverage and Vulnerabilities with owner phishing tests	The number of devices with vulnerabilities and who's owner has received a phishing test

Type	Metric Name	Description
Compound risk	Vulnerability detections with device coverage information	The number of vulnerability detections on devices (includes devices tool coverage information)

Endpoint Protection

The Endpoint Protection domain helps to ensure endpoint tools and controls are working as expected.

We provide continuous assurance of your security controls, assessing the coverage and effectiveness of your endpoint tools. This helps you to achieve compliance and dramatically reduce the risk of exposure during day-to-day operations, tool migrations, and times of organizational change. Panaseer combines unique business context with data from your existing tools, providing improved oversight of your endpoint tools and controls performance. The platform provides IT operations, security teams, and asset and risk owners access to near real-time analysis to efficiently address business risk. Compliance and assurance teams can continuously map to NIST CSF (including NIST 2.0) and other frameworks.

Benefits

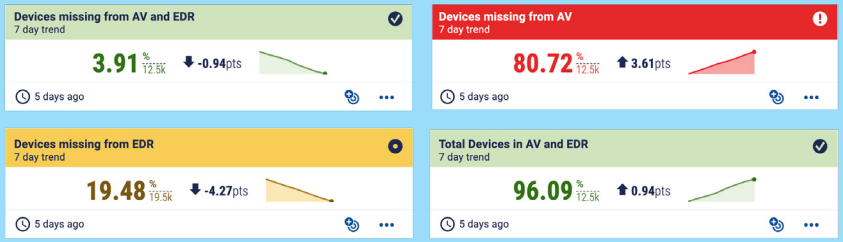
- Prioritize updates for the endpoints that pose the greatest risk to your critical infrastructure.
- Ensure EDR and AV coverage across dispersed and fragmented organizations.
- Reduce risk during tool migrations, with assurance and visibility throughout.
- Measure and improve performance against SLAs, such as scan frequency and version.

Example data sources

MS Defender | CrowdStrike | McAfee AV | Guardium | Symantec DLP

Spotlight metric

Endpoint coverage



Check which devices are most exposed, identifying those lacking AV, EDR or both.

These metrics confirm the coverage of your AV and EDR tools, so that you can check which devices should be top of your priority list for remediation as they lack any compensating controls.

Type	Metric Name	Description
Policy	AV scan out of SLA	The number of devices out of AV scan SLA
Policy	AV out of scan or update SLA	The number of devices out of AV scan SLA or out of AV update SLA
Coverage	AV devices	The number of devices included in AV SLA analysis
Policy	AV update out of SLA	The number of devices out of AV update SLA
Policy	EDR connection out of SLA	The number of devices out of EDR last connection SLA
Policy	EDR connection or version out of SLA	The number of devices out of EDR last connection SLA or EDR version SLA
Coverage	EDR devices	The number of devices included in EDR SLA analysis
Policy	EDR version out of SLA	The number of devices out of EDR version SLA
Policy	AV SLA breaches	The percentage of devices out of AV scan SLA, the percentage out of AV update SLA and the percentage out of scan or update SLA.
Policy	AV scan out of SLA	The percentage of devices out of AV scan SLA
Policy	AV scan or update out of SLA	The percentage of devices out of at least one of AV scan SLA and AV update SLA
Policy	AV update out of SLA	The percentage of devices out of update SLA
Policy	EDR connection out of SLA	The percentage of devices out of EDR last connection SLA
Policy	EDR connection or version out of SLA	The percentage of devices out of at least one of EDR last connection SLA and EDR version SLA
Policy	EDR version out of SLA	The percentage of devices out of EDR version SLA
Policy	EDR agent connection out of SLA	Number of EDR agent records that are out of last-connection SLA.
Policy	EDR agent connection or version out of SLA	Number of EDR agent records out of either last-connection SLA or version SLA.
Coverage	EDR records	Number of device records included in EDR SLA analysis (one record per device–OS combination).
Policy	EDR agent version out of SLA	Number of EDR agent records where the agent version is out of SLA.

Patch Management

The Patch Management domain provides continuous assurance that your patch program is running efficiently and as expected.

Panaseer unifies data from your patch management, CMDB and other tools to give you unrivalled insight and context on patches. Quickly identify and find coverage gaps, improve prioritization and accountability, and measure your performance against policies and SLAs. Panaseer improves prioritization and allows you to do more with limited resources and delivers deep insight into patch management performance and controls.

Benefits

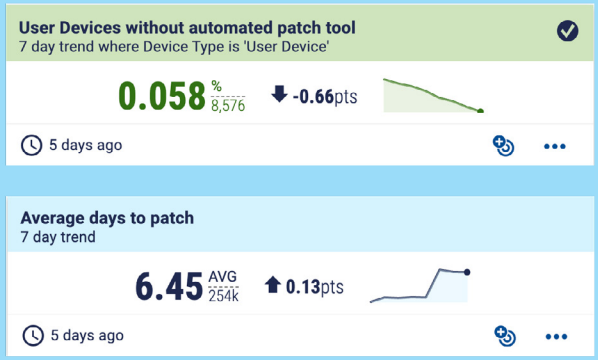
- Continuously track all your devices to understand available and outstanding patches, and evidence improvements over time in patch management performance.
- Prioritize which risks need addressing first. Identify and isolate unpatched or out-of-compliance devices and combine with business context to focus on critical assets.
- Understand if patches are applied within SLA.
- Review performance against policy for deployed patches. Uncover trends in patches that have been deployed past SLA, reducing your organization's exposure.
- Panaseer's trusted asset inventory unifies data from patch management, vulnerability scanners, CMDBs and other tools to give you unrivalled insight and context on patches.

Example data sources

SCCM

Red Hat Satellite

Spotlight metric



Review the performance of your patching programs with measurement against your key KPIs.

These metrics highlight the speed of your patching process with "Average days to patch", and which user devices aren't included with "User devices without automated patch tool".

Type	Metric Name	Description
Informational	Patches deployed recently	The number of patches deployed recently
Policy	Patches deployed out of SLA	The number of patches deployed over time after SLA
Policy	Patches deployed recently out of SLA	The number of patches deployed recently but after SLA
Informational	Patches deployed	The number of patches deployed
Policy	Devices with outstanding patches out of SLA	The number of devices with outstanding patches out of SLA
Diagnostic	Devices with outstanding patches	The number of devices with outstanding patches
Informational	Outstanding patches by patch	The number of outstanding patches by patch
Policy	Outstanding patches out of SLA	The number of outstanding patches out of SLA
Informational	Unique outstanding patches	The number of unique outstanding patches across devices
Informational	Outstanding patches	The number of outstanding patches
Informational	Patches recently outstanding	The number of patches that were outstanding recently (including outstanding and deployed patches)
Policy	Recently outstanding patches out of SLA	The number of patches out of SLA that were outstanding recently (including outstanding and deployed patches)
Policy	Historic patches out of SLA (outstanding and deployed)	The number of patches over time out of SLA (including outstanding and historic deployed patches)
Informational	Patches (outstanding and deployed)	The number of patches (including outstanding and historic deployed patches)
Diagnostic	Total days to patch	The total number of days taken from when patches become available until they are deployed
Policy	Deployed patches out of SLA	The percentage of deployed patches over time out of SLA
Policy	Patches deployed recently out of SLA	The percentage of patches deployed recently but after SLA out of all recent patches
Policy	Devices with outstanding patches out of SLA	The percentage of devices with outstanding patches out of SLA
Policy	Outstanding patches out of SLA	The percentage of outstanding patches out of SLA
Policy	Historic patches out of SLA (outstanding and deployed)	The percentage of patches over time out of SLA (including outstanding and deployed patches)
Policy	Recently outstanding patches out of SLA	The percentage of patches out of SLA that were outstanding recently (including outstanding and deployed patches)
Diagnostic	Average days to patch	The average time in days taken to deploy available patches

Application Security

The Application Security domain helps you manage the security of the applications you build in-house by providing assurance and measurement of AppSec controls.

Panaseer improves AppSec decision-making with near-real-time security metrics and insight into application ownership. This improves accountability for security across the wider business and helps make security a priority during app development. Panaseer helps you understand the effectiveness of your AppSec program and enables you to create reports and configurable dashboards aligned to security frameworks and standards.

Benefits

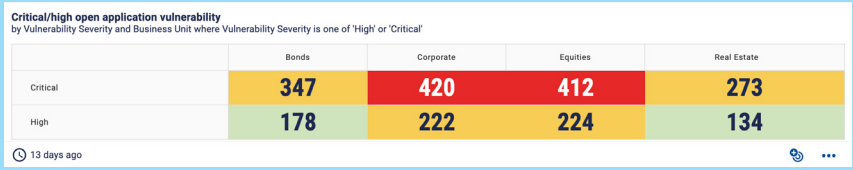
- Improve visibility and accountability by associating an application's security posture to its business owner.
- Prioritize remediation of application security flaws based on business risk.
- Identify the types of flaws occurring most commonly across the organization, allowing you to prioritize in-house developer training and address root causes.
- Combine different types of application scanning data and approaches, such as penetration testing, DAST and SAST), helping to address common flaws across your processes.

Example data sources

Checkmarx | Snyk | Fortify

Spotlight metric

Vulnerabilities on in-house applications



Identify which business areas need more support to resolve critical/high application security issues with a color coded view of issue hot spots.

This metric assesses the number of vulnerabilities on applications built in-house. It provides vulnerability counts color coded based on thresholds you've set (less than 200 is exceeding, less than 400 is passing, and over 400 is failing).

Data is split by business unit to help drive accountability for security in app development.

Type	Metric Name	Description
Informational	Applications with detections and number of detections	The number of open applications with vulnerability detections and the number of detections
Informational	Applications with open critical/high vulnerability detections	The number of applications with open critical/high vulnerability detections
Informational	Applications with open vulnerability detections	The number of applications with open vulnerability detections
Policy	Applications out of scan SLA	The number of applications that have not been vulnerability scanned recently in line with SLA
Coverage	Applications in scope for scan SLA	The number of applications included in vulnerability scan frequency SLA analysis
Policy	Applications scanned in line with SLA	The number of applications that have been vulnerability scanned recently in line with SLA
Informational	Closed application vulnerability detections	The number of remediated application vulnerability detections
Policy	Critical/high application vulnerability detections out of SLA	The number of open critical/high application vulnerability detections out of remediation SLA
Informational	Critical/High Application Vulnerability Detections	The number of open critical/high application vulnerability detections
Policy	Application vulnerability detections out of SLA	The number of open application vulnerability detections out of remediation SLA
Informational	Open application vulnerability detections	The number of open application vulnerability detections
Diagnostic	Total remediation time for application vulnerability detections	The total time in days taken to remediate application vulnerability detections
Diagnostic	Average age of application vulnerability detections	The average age (days since first detection on application) of vulnerability detections
Diagnostic	Average open vulnerability detections per affected application	The average number of open vulnerability detections per application with detections
Policy	Applications out of scan SLA	The percentage of applications that have not been vulnerability scanned recently in line with SLA
Policy	Application vulnerability detections out of SLA	The percentage of open application vulnerability detections out of remediation SLA
Diagnostic	Average remediation time for application vulnerability detections	The average time in days taken to remediate application vulnerability detections
Compound risk	Unique Devices hosting Application	The number of devices in the Panaseer Inventory hosting applications
Compound risk	Unique Devices not hosting Application	The number of devices in the Panaseer Inventory not hosting applications
Diagnostic	Applications never vulnerability scanned	Number of applications that have never been scanned for vulnerabilities.
Policy	Applications out of scan SLA (%)	Percentage of applications that have not been vulnerability scanned recently in line with SLA.
Compound Risk	Accounts with access to applications	Number of accounts with access to an application.

Identity and Access Management

The Identity and Access domain provides continuous assurance that your IDAM program is performing as expected.

Panaseer combines data from security, IT and business tools, specifically security and people data, to enhance visibility into your IDAM program. This includes near-real-time analysis for IT operations, asset owners and risk owners to address business risks more effectively. Compliance teams benefit from continuous oversight aligned with NIST CSF and other frameworks.

Benefits

- Continuously monitor your identity and access management program with near real-time reporting and dashboards.
- Correlate security, IT and business data into a single, reliable source.
- Use automation and data science for a comprehensive account inventory enriched with business context.
- Track, measure and report against your policies, industry standards and best practices. These include impactful “active leavers” metrics, account ownership, and more.
- Simplify IDAM reporting and prioritize actions to reduce business risks.
- Get a clear, prioritized view of identities and access privileges, enriched with your unique business context, allowing you to focus on high-risk areas.

Example data sources

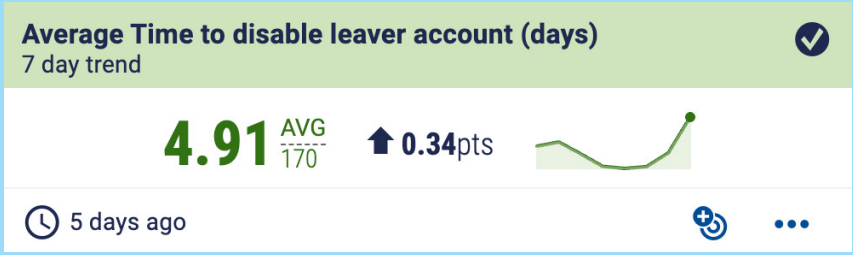
Entra ID / Azure AD

SailPoint

Workday

Spotlight metric

Active leavers



Quickly close down active leaver accounts to avoid delays or human error creating a risk to critical assets.

This metric identifies active accounts that are owned by former employees, a common KPI for IAM programs. The color-coded metric shows that performance is within the target threshold you’ve set, but is becoming more problematic, as the time is trending up.

Type	Metric Name	Description
Diagnostic	Active leaver accounts	The number of active accounts with owner no longer employed
Informational	Admin accounts	The number of active administrator accounts
Informational	Accounts in scope for complete information	The number of accounts in scope for complete information
Diagnostic	Disabled leaver accounts	The number of disabled accounts with owner whose employment terminated in the last month
Informational	Number of accounts reporting in IDAM (with owner information)	The number of accounts reported in the IDAM module plus information about the account owner
Informational	Accounts in scope for password reset	The number of accounts in scope for a recent password reset
Policy	Accounts with incomplete info	The number of accounts with incomplete information
Diagnostic	Accounts of last month's leavers	The number of accounts with an owner that left in the last month
Policy	Accounts in scope for a recent login	The number of accounts in scope for a recent login
Policy	Accounts without login	The number of accounts without a recent login
Policy	Accounts without owner	The number of accounts without an owner
Policy	Accounts without password reset	The number of accounts without a recent password reset
Informational	Accounts in scope for ownership	The number of accounts in scope for ownership
Informational	Service accounts	The number of active service accounts
Diagnostic	Leavers with active accounts	The number of people that are no longer employed, but still have at least one active account
Diagnostic	Total active days before disabling leaver accounts	The total time in days taken to disable leaver accounts
Policy	Accounts with incomplete information	The percentage of accounts with incomplete information
Policy	Accounts without login	The percentage of accounts without a recent login
Policy	Accounts without owner	The percentage of accounts without an owner
Policy	Accounts without password reset	The percentage of accounts without a recent password reset
Diagnostic	Disabled leaver accounts	Percentage of disabled accounts belonging to people whose employment terminated within the last month
Diagnostic	Average active days before disabling leaver accounts	The average time in days taken to disable leaver accounts
Compound risk	Unique People without Standard Accounts	The number of People without standard accounts
Compound risk	Unique People without Standard Accounts (internal)	The number of People without standard accounts (internal)

Privileged Access Management

The Privileged Access Management (PAM) domain offers continuous assurance that your PAM program is working as expected.

Panaseer combines data from security, IT and business tools to enhance visibility into your PAM program. One of the biggest challenges with PAM is gathering all the necessary data. The process is often manual and outdated by the time it's complete. Panaseer gives you a clear, prioritized view of all identities, hierarchies, and access privileges, simplifying the management and reporting of user identities and privileges.

Benefits

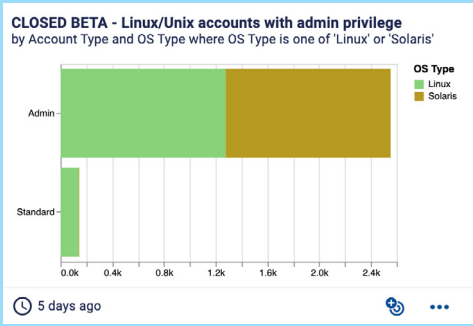
- Continuously monitor privileged access with near real-time reporting and dashboards.
- Correlate security, IT and business data into a single source.
- Automation and data science for comprehensive inventories of people and accounts, enriched with business context.
- Track, measure and report against your policies, industry standards and best practices. These include inheritance paths, admin accounts, devices with admin rights, and more.
- Simplify reporting and prioritize actions to reduce business risk.
- Get a clear, prioritized view of all access privileges, enriched with your unique business context, allowing you to focus on high-risk areas.

Example data sources

Qualys | CyberArk | Splunk

Spotlight metric

Linux/Unix accounts with admin privilege



Check which accounts have privileged access within your organization.

This information can be presented by multiple dimensions, such as OS type, region, business unit or job role - helping provide valuable added context for clear decision making.

Type	Metric Name	Description
Diagnostic	Linux/Unix accounts with admin privilege	The number of Linux/Unix accounts with administrative privileges
Diagnostic	Windows accounts with admin Privilege	The number of Windows accounts with administrative privileges
Diagnostic	Linux/Unix devices with direct admin privilege	The number of Linux/Unix devices with directly assigned administrative privileges
Coverage	Linux/Unix devices with login events	The number of Linux/Unix devices with login events in security logs
Coverage	Linux/Unix devices with permissions data	The number of Linux/Unix devices with permissions data available for analysis
Diagnostic	Windows devices with direct admin privilege	The number of Windows devices with directly assigned administrative privileges
Coverage	Windows devices with login events	The number of Windows devices with login events in security logs
Coverage	Windows devices with permissions data	The number of Windows devices with permissions data available for analysis
Diagnostic	Paths to Linux/Unix admin privilege	The number of assignment paths to Linux/Unix administrative privileges
Diagnostic	Paths to Windows admin privilege	The number of assignment paths to Windows administrative privileges
Policy	Linux/Unix login policy infringements	The number of Linux/Unix login events per day that infringed login policies for accounts with administrative privileges
Policy	Windows login policy infringements	The number of Windows login events per day that infringed login policies for accounts with administrative privileges
Compound Risk	Employees with privileged access accounts who have not completed phishing training	Number of employees with privileged access accounts who have not completed phishing training within SLA (last 30 days).

User Awareness

The User Awareness domain provides automated metrics and measurement for your user awareness program.

Panaseer combines data from security, IT and business tools, specifically user awareness and people data, to enhance visibility into your user awareness program. It's enriched with business context to allow you to more efficiently address business risk.

Benefits

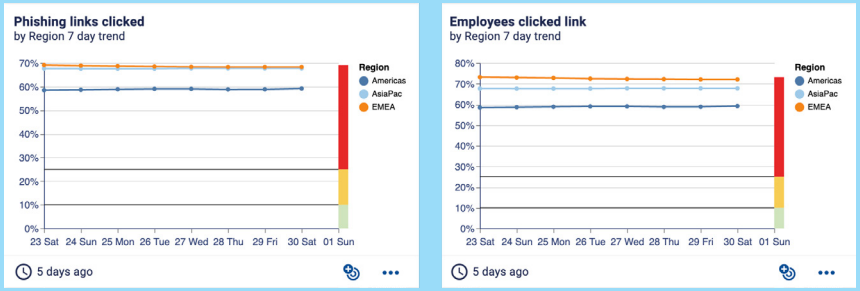
- View your awareness program through the context of people, not just email addresses. Get context on how users perform over time, who manages them, what devices they use, and what applications they have access to.
- Prioritize your user awareness training program. Identify risks such as senior stakeholders in roles with access to sensitive data, phishing test performance, or business units that are under-performing compared to others.
- See historical trends and repeating patterns to see if people learn from their mistakes. "Repeat offenders" metrics show consecutive phishing test failures by the same people.
- Celebrate positive behaviors to increase user awareness and build a stronger security culture. By measuring who is reporting phishing test emails, you can identify and reward your champions.
- Get context on the mission-critical business processes or operations a particular cloud environment supports.

Example data sources

KnowBe4 | Proofpoint | Cofense

Spotlight metric

User awareness KPIs over time



Analyze how user awareness KPI performance is trending over time.

These metrics show how different parts of the business are performing against user awareness KPIs you've set for the users clicking phishing links. This data can be segmented by business dimensions such as geography, business unit or job role.

Type	Metric Name	Description
Informational	Active phishing campaigns	The number of active phishing awareness campaigns
Informational	Phishing links clicked	The number of links clicked in phishing awareness emails
Informational	Phishing emails sent	The number of phishing emails sent for all awareness campaigns
Informational	Phishing emails sent for active campaigns	The number of phishing emails sent for currently active awareness campaigns
Informational	Employees clicked multiple links	The number of employees who clicked a URL on more than one phishing awareness email
Informational	Employees clicked links	The number of employees who clicked a URL on one or more phishing awareness emails
Coverage	Employees not included in phishing awareness campaigns	The number of eligible employees that have not been sent any phishing emails
Policy	Employees failed phishing test	The number of employees who failed a phishing test
Policy	Employees repeatedly failed phishing test	The number of employees who failed a phishing test more than once
Informational	Employees sent phishing test	The number of employees that have been sent one or more phishing awareness emails
Informational	Employees received phishing test	The number of employees that have received one or more phishing awareness emails
Informational	Employees for phishing awareness campaigns	The number of employees with email addresses eligible for phishing awareness tests
Informational	Total number of reports of suspected phishing emails	Total number of reports of suspected phishing emails
Informational	The count of distinct users who have reported a suspected phishing email	The number of unique users who have made at least one report of a suspected phishing email
Informational	Phishing links clicked	The percentage of phishing links clicked per phishing emails sent
Informational	Employees clicked multiple links	The percentage of tested employees who clicked a URL on more than one phishing email
Informational	Employees clicked link	The percentage of tested employees who clicked a URL on one or more phishing awareness emails
Coverage	Employees not included in phishing awareness campaigns	The percentage of eligible employees that have not been sent any phishing emails
Policy	Employees failed phishing test	The percentage of employees who failed a phishing test
Policy	Employees repeatedly failed phishing test	The percentage of employees who failed a phishing test more than once
Informational	Employees received phishing test	The percentage of eligible employees that have received one or more phishing emails
Informational	Users Reporting Suspected Phishing Emails	The percentage of users reporting suspected phishing emails
Compound risk	Device coverage and Vulnerabilities with owner phishing tests	The number of devices with vulnerabilities and who's owner has received a phishing test
Informational	Employees who completed training past SLA deadline	Number of employees who completed user training after the SLA deadline (trainings active in last 30 days).

Type	Metric Name	Description
Informational	Employees who completed user training	Number of employees who completed user trainings active in the last 30 days.
Informational	Employees enrolled in user training	Number of employees enrolled in user trainings active in the last 30 days.
Informational	Employees who passed user training	Number of employees who passed user trainings active in the last 30 days.
Diagnostic	Employees who completed training past SLA deadline	Percentage of employees who completed user training after the SLA deadline (trainings active in last 30 days).
Diagnostic	Employees who completed user training	Percentage of employees who completed user training out of those enrolled (trainings active in last 30 days).
Diagnostic	Employees who passed user training	Percentage of employees who passed user training out of those who completed trainings active in last 30 days.
Compound Risk	People who have received phishing tests (includes accounts information)	Number of people who have received phishing tests, including account information.

Cloud Configuration

The Cloud Configuration domain provides visibility across cloud accounts and misconfigurations.

Panaseer combines data from multiple cloud sources (such as CSPMs) with additional data sources (such as your CMDB) and enriches it with business context. Gain unprecedented insight and oversight of your cloud configuration program, while prioritizing fixes for the misconfigurations that are affecting the most important parts of the business. This allows you to drive accountability and ownership of these accounts.

Benefits

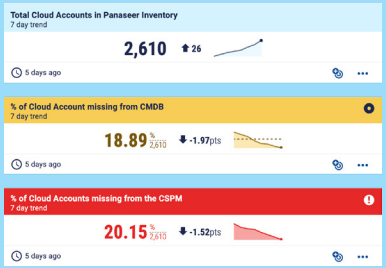
- Gain full visibility of all your cloud accounts and identify those not covered by configuration scanning.
- Prioritize fixing misconfigurations based on business risk.
- Drive accountability for the ownership of cloud accounts and their configuration.
- Use out-of-the-box metrics and dashboards to explore trends in misconfigurations and compare remediation progress against security policy SLAs.
- Filter on the exclusions that have been recorded in your CSPM/CSP so that reporting on SLAs is accurate while exclusions are clear.
- Get context on the mission-critical business processes or operations a particular cloud environment supports.

Example data sources

Azure | AWS | Google Cloud | Wiz

Spotlight metric

Cloud account inventory coverage



Identify cloud accounts missing from other inventories and important security and IT tools.

These metrics show the total cloud accounts in your environment using data from multiple sources and tools. They highlight the percentage of cloud accounts missing from your CMDB and CSPM. Not only does this represent a breakdown in process, but also increases your risk where misconfigurations and remediation are not being managed.

Type	Metric Name	Description
Informational	Cloud Accounts with configuration failures	The number of Cloud Accounts in the Panaseer Inventory with configuration failures detected
Policy	Cloud configuration failures out of SLA	The number of out of SLA configuration failures detected on Cloud Accounts
Informational	Cloud configuration failures	The number of configuration failures detected on Cloud Accounts
Informational	Cloud configuration tests	The total number of configuration tests on Cloud Accounts
Informational	Cloud Accounts with configuration failures	The percentage of Cloud Accounts seen in the CSPM with configuration failures detected
Policy	Cloud configuration failures out of SLA	The percentage of configuration failures detected on Cloud Accounts that are out of SLA
Coverage	Cloud Accounts not in CMDB	The percentage of Cloud Accounts in the Panaseer Inventory that are not in the CMDB
Coverage	Cloud Accounts not in CSPM	The percentage of Cloud Accounts in the Panaseer Inventory that are not in the CSPM
Informational	Cloud configuration tests failed	The percentage of all configuration tests on Cloud Accounts that failed

Infrastructure Configuration

The Infrastructure Configuration domain provides continuous assurance that devices are compliant with configurations.

Panaseer provides an essential tool in your Configuration Management process. We monitor and visualize your device configuration compliance in metrics and dashboards that report against your baselines or established benchmarks. The platform removes the burden from busy IT, security and compliance teams by highlighting misconfigurations, unauthorized changes or configuration drifts. The Panaseer inventory provides business context around devices with misconfigurations, which allows you to identify and prioritize actions.

Benefits

- Enables IT, security and compliance teams to quickly identify and target misconfigured or non-compliant devices.
- Provides auditors with detail, context and insight into your organization's configuration management practices.
- Measures compliance with industry standard or custom configuration benchmarks.
- Track remediation activities and improve accountability with additional information on device ownership.
- Automation reduces manual processes around tracking and proving compliance. This supports faster, more accurate audit and allows your team to focus on more important tasks.

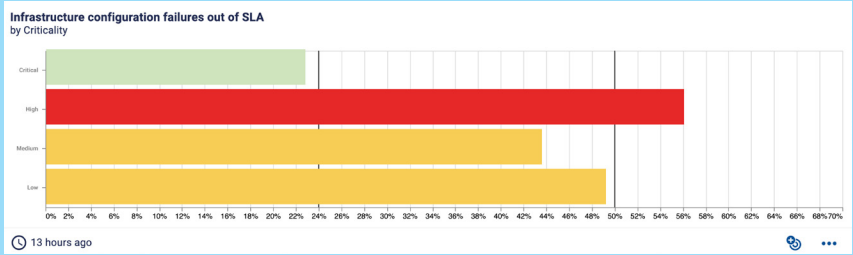
Example data sources

Qualys Compliance

Progress Chef

Spotlight metric

Infrastructure configuration failures out of SLA



Prioritize configuration issues based on a combination of criticality and SLA compliance.

This metric shows all misconfigurations, categorized by criticality with a clear color code to highlight those which are exceeding the acceptable threshold you've set.

Type	Metric Name	Description
Policy	Infrastructure configuration failures out of SLA	The number of out of SLA configuration failures detected on infrastructure
Informational	Infrastructure configuration failures	The number of configuration failures detected on Infrastructure
Informational	Devices with configuration test failures	The number of devices with configuration test failures
Informational	Devices with configuration test results	The number of devices with configuration tests results
Informational	Infrastructure configuration tests	The total number of configuration tests on Infrastructure
Policy	Infrastructure configuration failures out of SLA	The percentage of configuration failures detected on infrastructure assets that are out of SLA
Informational	Devices with configuration test failures	The percentage of all devices with configuration test failures
Informational	Infrastructure configuration tests failed	The percentage of all configuration tests on infrastructure assets that failed

Interested?

If you would like to learn more about the Panaseer platform, reach out to the team at:

success@panaseer.com

Or request a demo at:

panaseer.com/request-a-demo