



Mapping **NIST CSF v2.0** to Cato SASE Platform





Overview

The global threat landscape has shifted from episodic disruption to continuous, adaptive risk. Cyberattacks no longer resemble isolated storms of unrelated incidents; they represent a constant stream of threats that pose a significant risk of business disruption to organizations of all sizes. Preventing and defending against these cyber threats, while maintaining business continuity, is becoming increasingly complex for modern digital enterprises. Against this backdrop, cybersecurity frameworks such as the **NIST Cybersecurity Framework (CSF) v2.0** have become indispensable. **NIST CSF** provides organizations with structured, proven methodologies to assess, prioritize, and strengthen their defenses.

This framework serves a dual purpose. First, it delivers a strategic, risk-based assessment model. **NIST CSF** is designed to help leadership and technical stakeholders align cybersecurity investments with organizational objectives and risk tolerance. It asks the right questions: Do we know our assets? Do we protect them appropriately? Can we detect and respond effectively? By benchmarking against **NIST CSF** functions (Identify, Protect, Detect, Respond, Recover, and Govern), organizations gain a clear understanding of their current position and the necessary steps to take.

Second, it offers guidance on cybersecurity readiness. Not every organization operates at the same maturity level, nor do they need to. NIST CSF allows businesses to progress logically from foundational protections to more advanced capabilities. This is cybersecurity you can measure, and more importantly, improve.

The table below summarizes the **NIST CSF** guidance and controls that will be mapped in this document.

NIST CSF v2.0	
Functions	Categories
Govern (GV)	Organizational Context (OC) Risk Management Strategy (RM) Roles, Responsibilities, & Authorities (RR) Policy (PO) Oversight (OV) Supply Chain Risk Management (SC)
Identify (ID)	Asset Management (AM) Risk Assessment (RA) Improvement (IM)
Protect (PR)	Identity Management, Authentication & Access Ctrl. (AA) Awareness & Training (AT) Data Security (DS) Platform Security (PS) Technology Infrastructure Resilience (IR)
Detect (DE)	Continuous Monitoring (CM) Adverse Event Analysis (AE)
Respond (RS)	Incident Management (MA) Incident Analysis (AN) Incident Response and Communications (CO) Incident Mitigation (MI)
Recover (RE)	Incident Recovery Plan Execution (RC.RP) Incident Recovery Communications (RC.CO)

Please refer to the following link for more information: [NIST CSF](#)

The frameworks above provide organizations with guidance to help improve their cybersecurity posture. Utilizing this guidance to map these controls to the **Cato SASE Platform** capabilities provides the enforcement strategy to ensure enterprises become cyber-ready to protect their most sensitive resources. Whether aligning with regulators, insurers, or industry partners, adherence to frameworks demonstrates accountability. **ISO 27001:2022** certification may be the gold standard for formal audits, but **NIST CSF** provides the scaffolding on which such audit readiness is built. They translate abstract risk into tangible controls and evidence, which are essential for proving due diligence to boards, auditors, and customers.

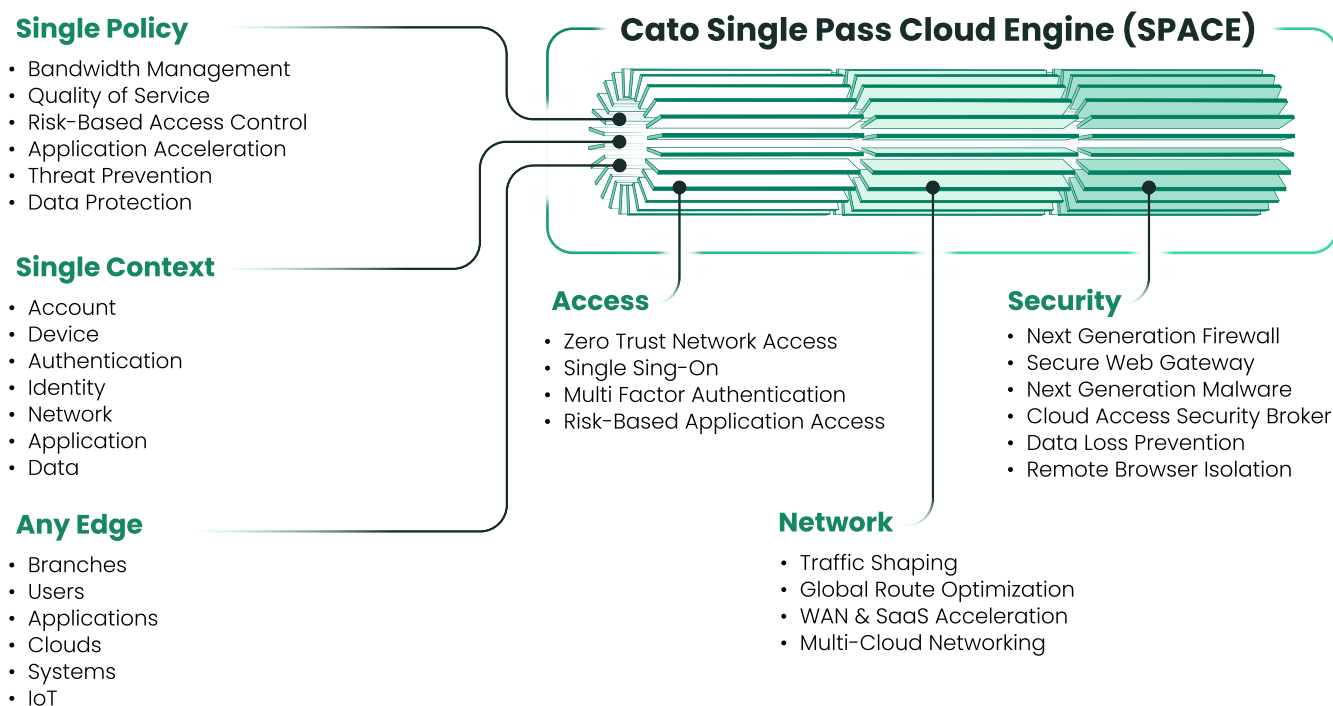
This white paper examines how this globally recognized framework aligns with Cato's converged SASE platform. By aligning **NIST CSF** with Cato's converged services, organizations can see precisely how strategic frameworks translate into operational outcomes.

The objective is simple but critical: to provide organizations with a clear mapping between framework requirements and modern **SASE** capabilities, ensuring security teams can move beyond theory into action. With this alignment, businesses can measure themselves against best-practice frameworks, operationalize controls within the Cato Platform, and demonstrate they are ready for today's risks and tomorrow's audits.

Cato SASE Platform

The **Cato SASE Platform** offers comprehensive threat protection for all edge locations (branch, data center, remote, and cloud). The platform delivers comprehensive security capabilities that protect all users. Cato's **Universal ZTNA strategy** and granular policy scheme provide comprehensive protection for end users, applications, and data based on their unique flows and contexts.

Cato has developed a unique approach to processing and inspecting traffic flows simultaneously through all security engines. Our **Single Pass Cloud Engine (SPACE)** ingests flows from all enterprise edges, including branches, users, applications, clouds, and systems. It then extracts the context from each flow, including the customer, identity, device, target application, data files and more.



The **Cato Single Pass Cloud Engine (SPACE)** is the foundation of the **Cato SASE Platform**, inspecting traffic once to create a single context that unifies user identity, device posture, application, data type, location, and threat intelligence. This single context powers a single policy framework consistently enforced across all security and networking functions, so protections follow every user, device, and data flow without gaps.

Compliance Alignment: Platform vs Products

When it comes to **NIST CSF** compliance, a platform holds a decisive advantage over fragmented products. Products may check all the boxes, including discrete controls in isolation. However, they inevitably introduce silos, inconsistent policies, and operational overhead. A platform, by contrast, unifies security and networking into a single policy framework, delivering end-to-end visibility, enforcement, and audit-ready reporting across all **NIST** functions. With a platform like **Cato SASE Platform**, compliance is not about stitching together logs and controls from disparate tools; it's in the DNA. **Cato SPACE**, for example, inspects once and enforces consistently, ensuring that all security controls are seamlessly aligned. This eliminates policy drift, reduces the risk of misconfiguration, and provides governance teams with real-time evidence of control effectiveness. The result is a measurable, sustainable path to compliance, enabling organizations to move beyond the checklists. A platform ensures business resilience.

Mapping NIST CSF v2.0 to the Cato SASE Platform

Cato SASE Platform delivers operational simplicity while ensuring governance and compliance are built in. **Cato SPACE**'s single-context single-policy approach helps organizations align controls more easily to **NIST CSF v2.0** functions (Identify, Protect, Detect, Respond, and Recover). This makes it foundational for compliance readiness, reduced complexity, and a stronger security posture.

Additionally, Cato detection and response services help organizations simplify their path to **NIST CSF v2.0** compliance by unifying detection, response, and reporting. Event correlation across the full SASE stack uncovers real threats, while 24/7 **SOC** expertise validates, escalates, and guides remediation. Together, they reduce noise, accelerate response, and deliver audit-ready reporting that supports governance and compliance. The result is stronger protection, faster decision-making, and measurable progress toward cybersecurity readiness.

The following section outlines the mapping of the **Cato SASE Platform** to **NIST CSF v2.0**.



Govern (GV): The organization's cybersecurity risk management strategy, expectations, and policies are established, communicated, and monitored

Supply Chain Risk Management (GV.SC)

Supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders

Subcategory	Cato SASE Platform Approach
GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	Cato continuously monitors supplier risks throughout the relationship. Cloud Access Control Broker (CASB) and Secure Web Gateway (SWG) monitoring track SaaS risks over time. Unsanctioned GenAI use is discovered via a shadow-AI dashboard and CASB enforces granular access and data-upload policies through a policy engine. IPS/NGAM/DNS Security blocks malicious traffic originating from compromised 3rd party services and applications. CMA logs the supplier-related risk activity.



Identify (ID): The organization's current cybersecurity risks are understood

Asset Management (ID.AM)

Assets that enable organizations to achieve their business purposes are identified and managed consistently in relation to their relative importance to organizational objectives and the organization's risk strategy.

Subcategory	Cato SASE Platform Approach
ID.AM-01: Inventories of hardware managed by the organization are maintained.	Cato SASE Platform automatically discovers and classifies connected devices (laptops, servers, IoT/OT devices) by analyzing network traffic across all sites and edges. Device fingerprints (OS, protocols, applications) are visible in the Cato Management Application (CMA) , providing a live inventory without requiring endpoint agents.

Subcategory

Cato SASE Platform Approach

ID.AM-02: Inventories of software platforms and applications are maintained

Cato CASB identifies sanctioned and unsanctioned SaaS usage. **SWG + FWaaS** logs catalog applications accessed across the environment. Applications are automatically categorized by type, risk level, and usage frequency. By combining inline inspection with **CASB** and **SWG**, Cato provides visibility into both enterprise applications and shadow IT. This inventory forms the basis for governance-driven **SaaS** adoption and data protection controls.

ID.AM-03: Inventories of data assets are maintained

Data Loss Prevention (DLP) inspects data flows for sensitive content (PII, PCI, HIPAA, IP). **Cato's DLP** engine enriches asset inventory by associating data flows with applications, users, and destinations. This enables governance teams to track sensitive data assets in transit and enforce controls against unauthorized movement. Data access attempts (uploads, downloads, sharing) are logged and classified in **CMA**.

ID.AM-04: Inventories of organizational communications and data flows are maintained

The **Single Pass Cloud Engine** inspects all **WAN**, internet, and cloud traffic, logging source, destination, application, and protocol metadata. Centralized logging in **CMA** provides a complete map of communications and dependencies. With Cato, organizations maintain real-time inventories of communication paths and data flows. This allows teams to identify dependencies between applications, services, and partners, which is essential for business continuity planning and risk analysis.

ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained

Cato contributes by providing inventories of sensitive data in transit and associated metadata, which complements broader data governance inventories. **DLP** inspects data flows, detecting sensitive data types (**PII, PCI, HIPAA, IP**). Metadata (user, application, destination, data category) is logged for each inspected transaction.

ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles

Cato supports operational lifecycle management by maintaining enforcement and visibility throughout the use and retirement of systems, services, and data. **Cato SASE** ensures continuous policy enforcement across asset lifecycles:

- **FWaaS, SWG, and IPS** protect systems and services during operational phases.
- **ZTNA** ensures only authorized users/devices connect as lifecycle roles change.
- **CASB** monitors **SaaS** adoption and deprecation.

Policies and logging in **CMA** track usage across an asset's operational life.

Risk Assessment (ID.RA)

The organization understands the cybersecurity risk to the organization, assets, and individuals.

Subcategory	Cato SASE Platform Approach
ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	Cato Intrusion Prevention System (IPS) and Next-Gen Anti-Malware (NGAM) detect and block exploit attempts against vulnerable assets. Logs show which systems were targeted, effectively recording observed vulnerabilities being exploited. However, Cato does not replace traditional vulnerability scanners. Cato helps identify exploited vulnerabilities in transit but does not perform complete vulnerability discovery across all assets.
ID.RA-02: Cyber threat intelligence is received from information-sharing forums and sources	Cato operationalizes threat intelligence ingestion and applies it across the entire SASE platform. Cato ingests global threat intelligence feeds (malware signatures, IP/domain blocklists, zero-day exploit updates) into the Single Pass Cloud Engine . Customers benefit from Cato Threat Research Unit intelligence without having to manage multiple feeds themselves.
ID.RA-03: Internal and external threats to the organization are identified and recorded	Cato continuously records observed internal and external threats through centralized detection and event logging. XDR/MDR correlates threats across network flows, SaaS, and remote access. SWG/CASB/DNS filtering log external threats (phishing sites, C2 domains). IPS/DLP highlight internal risks (lateral movement, sensitive data exfiltration).
ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	Cato provides technical prioritization of detected threats, but does not perform a complete business impact analysis, which remains a governance function. XDR analytics utilize AI/ML to prioritize alerts based on likelihood and potential impact (e.g., differentiating between commodity malware and targeted exploitation). The Cato Sandbox provides a fully isolated cloud-native environment to execute and analyze suspicious files using static and dynamic techniques, yielding forensic-grade insights for advanced threat hunting and response. MDR analysts validate events and provide context on severity and business impact.

Subcategory	Cato SASE Platform Approach
ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	Cato contributes security-driven prioritization of risk response but doesn't replace enterprise risk management processes. XDR/MDR dashboards show correlated risks and recommended responses. CMA enables policy adjustments (e.g., block new risky apps, restrict traffic categories).
ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated	Cato supports tracking and technical enforcement of chosen risk responses. MDR SOC analysts guide customers on incident handling and remediation. CMA allows tracking and enforcement of updated policies across the global network. Events and changes are logged for communication and review.
ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	Cato offers technical enforcement and visibility into exceptions/changes, though business-level risk evaluation is external. CMA provides role-based policy control and audit logs of all changes. Exceptions (e.g., whitelisting an app/site) are centrally logged, ensuring visibility of governance deviations.
ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established	Cato provides operational vulnerability response by updating defenses quickly, but disclosure handling processes (bug bounties, vendor management) remain external to Cato. Our Threat Research Unit continuously receives and analyzes vulnerability disclosures (CVE data, zero-days). Updates to IPS/NGAM signatures are distributed globally across the Cato Cloud within hours.

Improvement (ID.IM)

Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions.

Subcategory	Cato SASE Platform Approach
ID.IM-01: Improvements are identified from evaluations	Cato provides the evidence and performance data used in evaluations that drive continuous improvement. The CMA provides detailed logs, dashboards, and reports that organizations can utilize during audits, compliance reviews, and third-party evaluations. XDR/MDR reports provide SOC-driven insights into gaps and trends, highlighting areas where improvements are needed.

Subcategory	Cato SASE Platform Approach
ID.RA-02: Cyber threat intelligence is received from information-sharing forums and sources	Cato operationalizes threat intelligence ingestion and applies it across the entire SASE platform . Cato ingests global threat intelligence feeds (malware signatures, IP/domain blocklists, zero-day exploit updates) into the Single Pass Cloud Engine . Customers benefit from Cato Threat Research Unit intelligence without having to manage multiple feeds themselves.
ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	Cato does not write IR plans , but provides the data, response capabilities, and feedback loops that help organizations maintain and improve them. MDR SOC post-incident reports provide direct input into refining IR plans by documenting attack paths, effectiveness of response, and lessons learned. CMA central policy engine allows rapid updates to firewall, SWG , ZTNA , IPS , and DLP policies based on IR plan revisions.



PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used

Identity Management, Authentication, and Access Control (PR.AA)

Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed in accordance with the assessed risk of unauthorized access.

Subcategory	Cato SASE Platform Approach
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	Cato does not create or manage identities, but it enforces governance of authorized identities across the network fabric. Cato integrates with IdPs (Okta, Azure AD, Ping) to enforce that only validated user identities can access resources. ZTNA ties access sessions to specific user identities and device contexts. Service accounts and API access can be governed by policies enforced in the Cato Management Application (CMA) .
PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	Cato ensures identity assertions are bound to session context, complementing the IdP 's proofing process. Cato leverages the identity proofing done by the IdP and enforces additional context-based checks: • Device posture validation, • Geolocation, • Time-of-day restrictions. Access sessions are dynamically authorized based on these contextual signals.
PR.AA-03: Users, services, and hardware are authenticated	Cato ensures that only authenticated users/devices/services are allowed onto the network fabric or to access protected apps. ZTNA enforces authentication before granting access to apps, SaaS , or private resources. Cato supports MFA enforcement through IdP integration. Hardware endpoints (IoT/OT devices) are authenticated based on network behavior and policy enforcement.
PR.AA-04: Identity assertions are protected, conveyed, and verified	Cato protects identity assertions in transit and validates them before permitting access. All sessions between users and the Cato Cloud use TLS encryption. Identity tokens and assertions from IdPs are validated before authorizing traffic. ZTNA ensures assertions remain intact throughout the session.

Subcategory	Cato SASE Platform Approach
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Cato enforces identity-driven access policies, ensuring least privilege and RBAC are practical realities. CMA policies define which users/groups can access which apps/resources. ZTNA enforces least privilege by granting access only to explicitly authorized applications. Admin RBAC in CMA enforces separation of duties for management tasks.

Data Security (PR.DS)

Data are managed consistently with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Subcategory	Cato SASE Platform Approach
PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	The Cato SASE Platform addresses data-at-rest on the platform via several techniques to provide full protection. To provide our service, we are required to store account-specific data on our servers, so we can enforce policies, authenticate users, prioritize traffic and store statistical information to provide our customer with network analytics. All customer data is kept in encrypted storage. To deliver a key management solution that fulfills the CIA principle on its own, we have implemented a proprietary distributed KMS (Key Management System) that is based on industry standard secret sharing algorithm.
PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	Cato directly protects data-in-transit confidentiality, integrity, and availability across the entire SASE platform. Cato SASE Platform's backbone is built on end-to-end TLS encryption for all WAN, cloud, and internet traffic. IPS/NGAM protects integrity by inspecting for malicious tampering, injection, or exploit attempts. DLP policies prevent sensitive data leakage in transit. ZTNA ensures only authenticated/authorized users establish encrypted sessions to apps.

Platform Security (PR.PS)

The hardware, software and services of physical and virtual platforms are managed consistently with the organization's risk strategy to protect their confidentiality, integrity and availability.

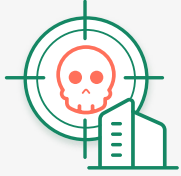
Subcategory	Cato SASE Platform Approach
PR.PS-01: Configuration management practices are established and applied	Cato enforces consistent, centralized configuration management with governance controls. The Cato Management Application (CMA) provides centralized configuration management across FWaaS, SWG, ZTNA, CASB, DLP, IPS , and other services. Role-based access control (RBAC) and audit logs ensure governance over policy changes. Policies are applied globally in near real-time across all PoPs.
PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	Cato manages the maintenance and patching of the SASE software stack directly, reducing customer risk. As a managed cloud service, Cato continuously patches and updates IPS, NGAM, DNS , and other inspection engines with the latest threat intelligence. Updates are transparent to customers and require no manual patching.
PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk	Cato maintains its own platform hardware, but it does not manage third-party or customer-owned infrastructure. Cato operates a global private backbone and PoPs , and Cato is responsible for maintaining and refreshing its own hardware infrastructure. Customers using Cato Socket edge devices receive managed updates; however, lifecycle replacement is handled by Cato, not the end-users.
PR.PS-04: Log records are generated and made available for continuous monitoring	Logging and monitoring are core capabilities of Cato SASE Cloud . All security events are logged in real time. Logs are accessible via CMA dashboards.
PR.PS-05: Installation and execution of unauthorized software are prevented	Cato prevents unauthorized or malicious software installation via inline enforcement and access controls. SWG and CASB policies block access to unsanctioned SaaS. IPS/NGAM prevent the download and execution of malicious software through inline inspection. ZTNA ensures only authorized apps can be accessed by defined users.

Subcategory	Cato SASE Platform Approach
PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	This mapping applies to Cato as the service provider, not customers, as it is relevant to Cato's internal practices, which are crucial to platform assurance. Cato follows secure SDLC practices for its cloud services (secure coding, testing, vulnerability scanning, patching). Customers benefit indirectly by consuming a service built and maintained under secure development governance.

Technology Infrastructure Resilience (PR.IR)

Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity and availability, and organizational resilience.

Subcategory	Cato SASE Platform Approach
PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	Cato directly protects networks against unauthorized logical access through inline enforcement and zero-trust principles. Zero Trust Network Access (ZTNA) : Ensures only authenticated and authorized users can access specific applications (least-privilege enforcement). FWaaS + SWG : Provide granular access controls at the network and application layers. IPS, NGAM, DNS Security : Block malicious or unauthorized traffic attempting to exploit network resources.
PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	Cato provides platform-level resilience by design through redundancy, failover, and secure backbone operations. Global Private Backbone : Built on a distributed mesh of Points of Presence (PoPs) for redundancy. Automatic Failover : User and site traffic reroutes to the next available PoP during outages or disruptions. Built-in WAN Optimization & QoS : Ensure performance under normal and adverse network conditions. Multi-layered Security : IPS, NGAM, DNS , and DLP continue to inspect traffic under all conditions, ensuring ongoing protection.
PR.IR-04: Adequate resource capacity to ensure availability is maintained	Cato ensures adequate resource capacity through its elastic architecture and global scale. Elastic, cloud-native architecture : Cato scales compute resources across PoPs to meet demand. Load balancing and auto-scaling : Ensure performance during peak usage. Global SLA-backed backbone : Provides predictable latency and availability.



DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed

Continuous Monitoring (DE.CM)

Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.

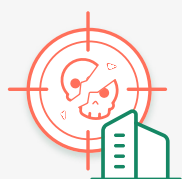
Subcategory	Cato SASE Platform Approach
DE.CM-01: Networks and network services are monitored to find potentially adverse events	Cato directly monitors networks and services for adverse security events. The Single Pass Cloud Engine inspects all WAN, internet, and cloud traffic in real time. FWaaS , IPS , NGAM , DNS Security , and SWG continuously detect anomalous or malicious events. CMA dashboards and XDR/MDR consolidate and analyze these events, providing alerts and reports.
DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	Cato monitors personnel activity and technology usage across the network for suspicious or policy-violating behavior. ZTNA and SWG logs capture user access to apps and web activity. CASB monitors SaaS activity, identifying shadow IT and unsanctioned cloud services. DLP inspects data usage patterns to detect risky or unauthorized transfers. All activity is correlated in CMA and optionally escalated through MDR SOC review.
DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	Cato monitors external service provider activity by inspecting and logging all related traffic flows. CASB provides visibility into third-party SaaS use, including sanctioned and unsanctioned applications. FWaaS/IPS logs record and analyze traffic to supplier systems and external partners. MDR/XDR can correlate external service traffic with threat intelligence to detect risks.

Adverse Event Analysis (DE.AE)

Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.

Subcategory	Cato SASE Platform Approach
DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	Cato provides both automated and human-led analysis of potentially adverse events. Single Pass Cloud Engine inspects all flows, correlating network, security, and identity data. XDR analytics analyze anomalies such as lateral movement, C2 communication , or data exfiltration attempts. MDR SOC analysts review suspicious events to validate true positives and understand attacker activity.
DE.AE-03: Information is correlated from multiple sources	Cato correlates diverse telemetry sources. Cato XDR correlates data across FWaaS , IPS , NGAM , DNS Security , ZTNA , CASB , SWG , and DLP logs . Threat intelligence feeds are integrated into detection models for additional context. MDR SOC is enriched with cross-customer intelligence and attack pattern recognition.
DE.AE-04: The estimated impact and scope of adverse events are understood	Cato provides technical scoping and assists in estimating potential impact. XDR contextualizes the scope (i.e., which user, device, site, or SaaS app is affected). MDR provides post-event reports detailing severity, lateral spread, and business impact.
DE.AE-06: Information on adverse events is provided to authorized staff and tools	Cato ensures adverse event information is distributed to authorized personnel and systems. • CMA dashboards present events to security administrators. • APIs/SIEM/SOAR integrations forward events to enterprise tools. • MDR SOC communicates validated incidents directly to customer teams.
DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	Threat intelligence is deeply integrated into analysis and prevention. Threat intelligence feeds (malware signatures, domain/IP blocklists, exploit detection) continuously update IPS/NGAM/DNS . Cato Threat Research Unit (TRU) enriches detections with contextual intelligence.

Subcategory	Cato SASE Platform Approach
DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	Cato can escalate adverse events into declared incidents based on detection thresholds and SOC review . XDR analytics apply rules and thresholds to determine whether an event escalates to an incident. MDR SOC validates detections against incident criteria and formally escalates incidents to the customer with recommended actions.



RESPOND (RS): Actions regarding a detected cybersecurity incident are taken

Incident Management (RS.MA)

Responses to detected cybersecurity incidents are managed.

Subcategory	Cato SASE Platform Approach
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	Cato enables the execution of IR plans in coordination with internal and external stakeholders by providing validated incidents and data. MDR SOC analysts coordinate with customer security/IT teams once an incident is confirmed. Incidents involving suppliers or cloud services are informed by CASB and ZTNA visibility into third-party usage. APIs/SIEM integrations ensure that third-party IR tools receive incident data in real time.
RS.MA-02: Incident reports are triaged and validated	Automated triage and human validation are core Cato capabilities. XDR analytics perform automated triage using AI-driven correlation across FWaaS , SWG , IPS , NGAM , DNS , CASB , and ZTNA telemetry . MDR SOC analysts review events to validate true positives and remove false positives.
RS.MA-03: Incidents are categorized and prioritized	Cato provides incident categorization and prioritization natively. Incidents are categorized by threat type (e.g., malware, C2, DLP violation, SaaS misuse). MDR SOC assigns severity levels based on observed scope and potential business impact. CMA dashboards highlight priority incidents for faster customer response.

Subcategory	Cato SASE Platform Approach
RS.MA-04: Incidents are escalated or elevated as needed	Cato provides escalation mechanisms for both human and automated response pathways. MDR SOC escalates incidents to customer IR teams when thresholds are met. Incidents can also be consumed into SIEM platforms for broader enterprise escalation workflows.
RS.MA-05: The criteria for initiating incident recovery are applied	Cato enforces containment and provides guidance, but the customer's IR plan governs the initiation of full recovery. MDR SOC guidance advises customers when to initiate recovery actions. CMA enforcement ensures containment until recovery steps are implemented. Final recovery criteria and execution remain a joint responsibility between Cato SOC and the customer's governance teams.

Incident Analysis (RS.AN)

Investigations are conducted to ensure an effective response and support for forensics and recovery activities.

Subcategory	Cato SASE Platform Approach
RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	Cato provides both automated and analyst-driven root cause analysis for network- and SaaS-based incidents. XDR analytics correlate telemetry across FWaaS, IPS, NGAM, SWG, ZTNA, CASB, DNS, and DLP to provide a comprehensive understanding of an attack. MDR SOC analysts validate alerts, analyze event timelines, and identify the likely root cause of incidents.
RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	Cato ensures investigative actions are logged with integrity and traceability. All investigative actions taken in CMA are logged with timestamps and the administrator's identity. MDR SOC actions and escalations are documented in incident reports provided to the customer. Logs are immutable within the CMA and can be exported to a SIEM to preserve provenance.
RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	Cato provides incident data and metadata collection with preserved integrity and provenance. Cato Single Pass Cloud Engine generates full metadata for every flow. Security events are logged with contextual metadata. Logs are stored securely in the CMA and can be exported to external systems for audit integrity.

Subcategory	Cato SASE Platform Approach
RS.AN-08: An incident's magnitude is estimated and validated	Cato provides scope and magnitude estimation validated by SOC experts. XDR correlates the number of users, devices, applications, and data flows affected to estimate the scope. MDR SOC analysts validate severity and potential business impact based on observed lateral spread or exfiltration attempts. CMA dashboards present prioritized incidents with impact context.

Incident Mitigation (RS.MI)

Activities are performed to prevent the expansion of an event and mitigate its effects.

Subcategory	Cato SASE Platform Approach
RS.MI-01: Incidents are contained	Cato actively stops lateral movement and malicious communication to contain incidents across the entire network. Inline inspection blocks malicious sessions, malware downloads, exploit attempts, and C2 communication in real time. ZTNA limits compromised users to only their authorized apps; sessions can be terminated instantly to cut off attacker movement. DLP and CASB prevent exfiltration of sensitive data to unsanctioned apps or destinations. XDR automation can trigger policy actions based on correlated detections. MDR SOC validates incidents and guides customers on containment actions.
RS.MI-02: Incidents are eradicated	Cato ensures active threats are removed from the environment by cutting off adversary communication channels and preventing re-entry. Cato's inspection engines drop ongoing malicious sessions. NGAM blocks malicious payloads and prevents reinfection. ZTNA policies and IdP integration revoke unauthorized user sessions immediately. MDR SOC analysts provide post-validation steps such as blocking persistent IoCs globally across all Cato PoPs .



RECOVER (RC): Actions and operations affected by a cybersecurity incident are restored

Incident Recovery Plan (RC.RP)

Restoration activities are performed to ensure the operational availability of systems and services affected by cybersecurity incidents.

Subcategory	Cato SASE Platform Approach
RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process	Cato enforces the network security aspects of the recovery plan once initiated. Once recovery is triggered, CMA policies can be adjusted to restore normal operations while maintaining security. MDR SOC provides guidance on removing temporary containment rules and returning traffic to standard policy baselines.
RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	Cato enables recovery actions at the policy and connectivity levels, prioritized according to business and SOC guidance. MDR SOC works with customers to scope recovery actions. CMA global policy orchestration ensures prioritized recovery steps (e.g., restoring critical business applications first) are implemented consistently across all sites and users.
RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	Cato provides visibility and enforcement to re-establish secure operational baselines after incidents. CMA dashboards and analytics provide visibility into post-recovery traffic and user activity, ensuring that the risk posture is aligned with governance decisions. MDR SOC delivers post-incident reports with recommendations to refine policies and support the updated operational norms.
RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed	Cato supports incident documentation and helps customers confirm recovery criteria have been met from a network and security perspective. MDR SOC provides final incident reports, documenting the recovery process, observed traffic normalization, and recommendations for future improvements. Cato logs provide audit-ready evidence for governance review.

Conclusion

Frameworks like **NIST CSF v2.0** provide organizations with a template for measuring readiness, prioritizing investments, and preparing for audits. **NIST** provides the strategic, risk-based view, while **CIS** offers a practical, prioritized checklist. Together, they ensure security programs are aligned to both business objectives and operational best practices.

The **Cato SASE Platform** supports the core specifications of these Cybersecurity Frameworks, bringing them to life and enabling effective identification, mitigation, and reduction of enterprise security risk. By converging networking and security into a single platform, Cato operationalizes **NIST** and **CIS** requirements in real time. The platform's security capabilities align well, providing a roadmap for customers to become compliant with these frameworks.

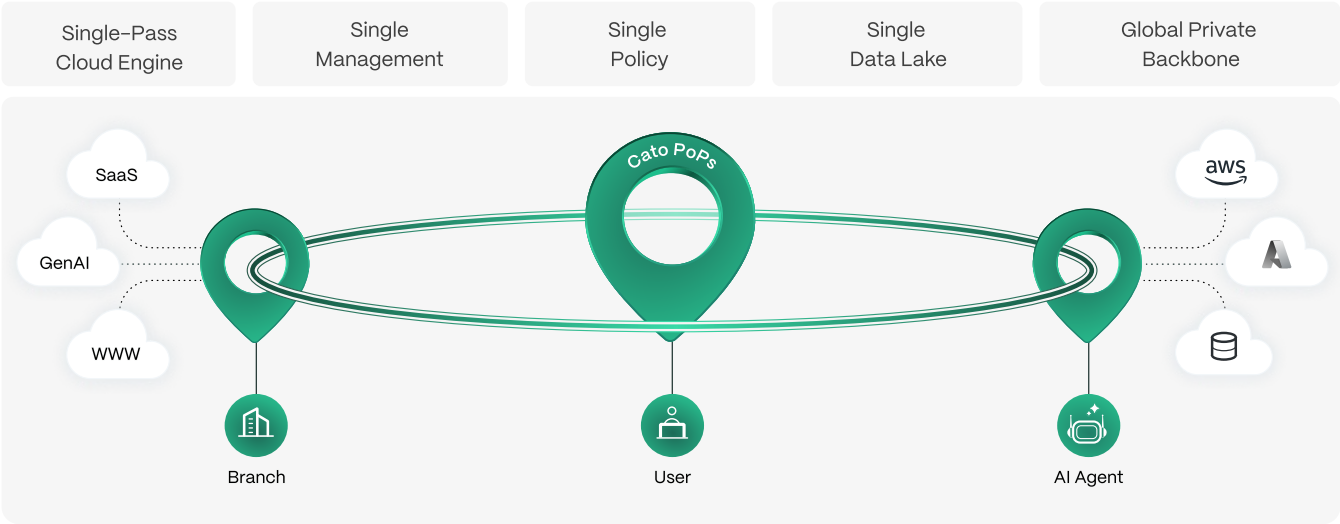
The result is that enterprises can achieve compliance, prove resilience, demonstrate audit-readiness, and protect what matters most with agility and confidence.

About Cato Networks

Cato Networks, a leader in SASE and AI security, delivers secure, zero-trust access everywhere to thousands of customers worldwide. Built for organizations operating across all cloud and hybrid environments, the Cato Platform unifies networking, security, and access, providing them as elastic, modular capabilities that organizations can easily adopt and grow over time. Cato combines the Cato Cloud, a purpose-built global network, with simplified operational experience, all delivered across a robust, AI-driven platform. With Cato, organizations modernize confidently, operate with greater resilience, and innovate faster, without added complexity or risk.

The Cato SASE Platform

Start your networking and security transformation wherever the business need is most urgent. From there, tap into the full power of the Cato SASE Cloud: purpose-built and self-optimizing global cloud with a single-pass engine, single data lake, and single policy enforcement.



Cato SASE Platform

Solutions

Next Gen Networking

Universal ZTNA

Zero Trust Security

AI Security

SASE Convergence

Cato Use Cases

Network Transformation

MPLS to SD-WAN Migration
Global Access Optimization
Hybrid Cloud & Multi-Cloud

Security Transformation

Secure Hybrid Work
Secure Direct Internet Access
Secure Application and Data Access
Incident Detection and Response

Secure AI Adoption

Public AI Usage
Private AI Applications

Business Transformation

Vendor Consolidation
Spend Optimization
M&A and Geo Expansion

Contact Us