
FlowGuard
Comprehensive Security
Assurance Platform

FlowGuard is a comprehensive security assurance platform engineered to give enterprises end-to-end visibility, control, and resilience across complex environments.

FlowGuard

FlowGuard is an comprehensive security assurance platform engineered to give enterprises end-to-end visibility, control, and resilience across complex environments.

At its core, FlowGuard unifies three powerful modules Firewall Assurance, Network Assurance, and Vulnerability Control to provide a comprehensive defenses approach which is complemented by its operations module. By continuously mapping hybrid networks, simulating attack paths, analysing security policies, and correlating vulnerabilities with real exposure, FlowGuard enables security teams to eliminate blind spots, optimize configurations, and prioritize remediation.

With built-in compliance automation and policy optimization, FlowGuard ensures organizations stay secure, audit-ready, and operationally efficient.

Unified Console

A single, intuitive GUI for data collection, analysis, and reporting, with full automation of management tasks.

Secure & Scalable Architecture

Encrypted communications, role-based access control (RBAC), and multi-factor authentication ensure secure operations across distributed and air-gapped sites.

Flexible Deployment Options

Available as software, virtual appliance, or hardware appliance, with active/passive resiliency and next-business-day hardware replacement.

Powerful Analytics & Search

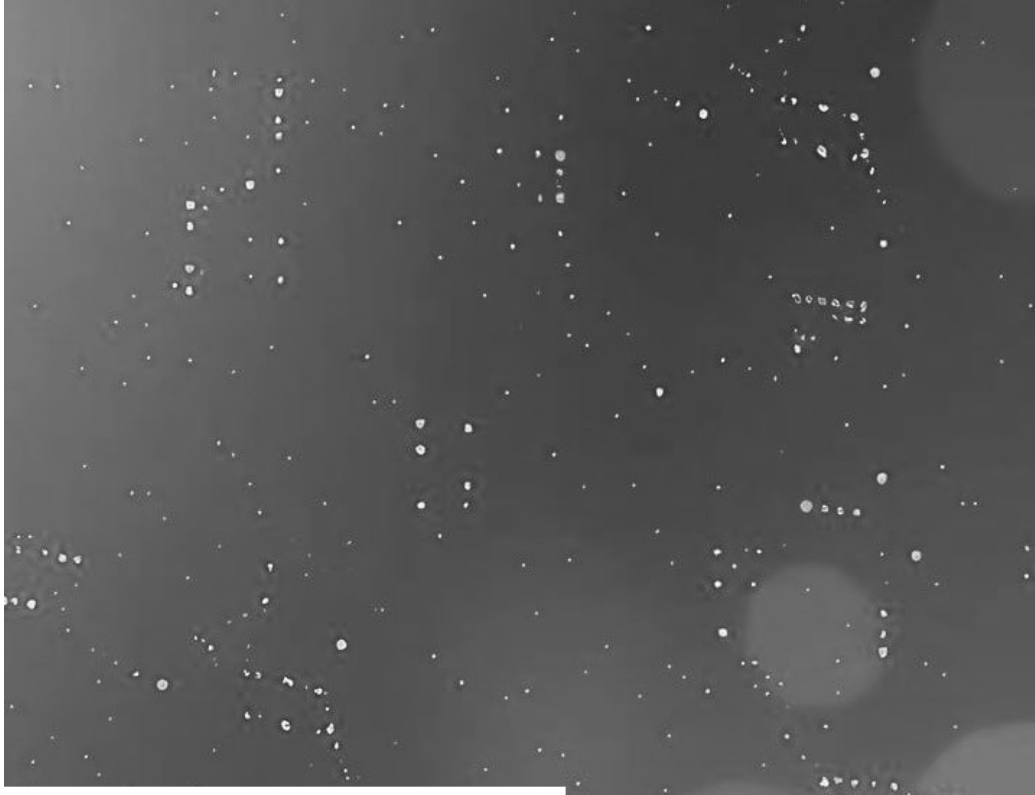
Built-in search engine with dual databases for optimized analysis and reporting, supporting advanced search, dashboards, and PDF exports.

Extensive Ecosystem Support

Integrates with 130+ platforms, supports Skybox and Splunk indexing, and enables seamless GRC integration.

Autonomous Collectors

Deployed at remote or air-gapped sites to minimize data transfer and ensure secure, sequential processing before central analysis.



FlowGuard

FlowGuard is designed not only to secure complex infrastructures but also to simplify operations and deliver measurable business value. By combining visibility, automation, and risk intelligence, it empowers organizations to stay ahead of evolving threats while reducing cost and complexity.

- Complete Visibility Across Hybrid Environments
- Reduced Attack Surface & Risk Exposure
- Prioritized, Business-Context Remediation
- Faster Compliance & Audit Readiness
- Optimized Security Operations
- Stronger Zero Trust & Segmentation Validation
- Lower Cost of Security Operations

Core Components of FlowGuard

Firewall Assurance – Gain full visibility and control over multi-vendor firewall policies to detect misconfigurations, optimize rules, and enforce compliance.

Network Assurance – Continuously map and validate your hybrid network, simulate attack paths, and ensure segmentation and Zero Trust principles are effective.

Vulnerability Control – Prioritize vulnerabilities by business impact and exposure, correlate with network context, and drive efficient, risk-based remediation.

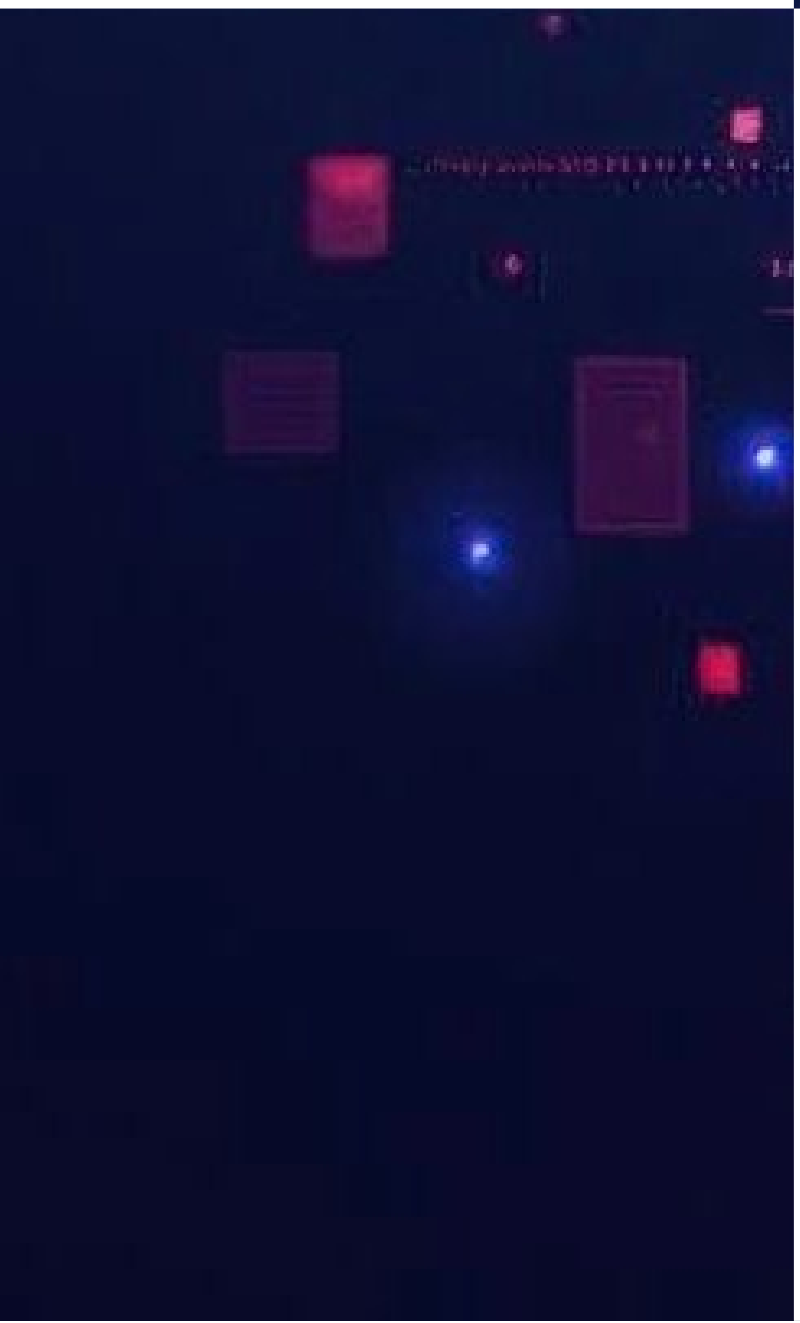
FlowGuard

FIREWALL ASSURANCE

Full visibility and optimization of multi-vendor firewall policies.

Firewall Assurance

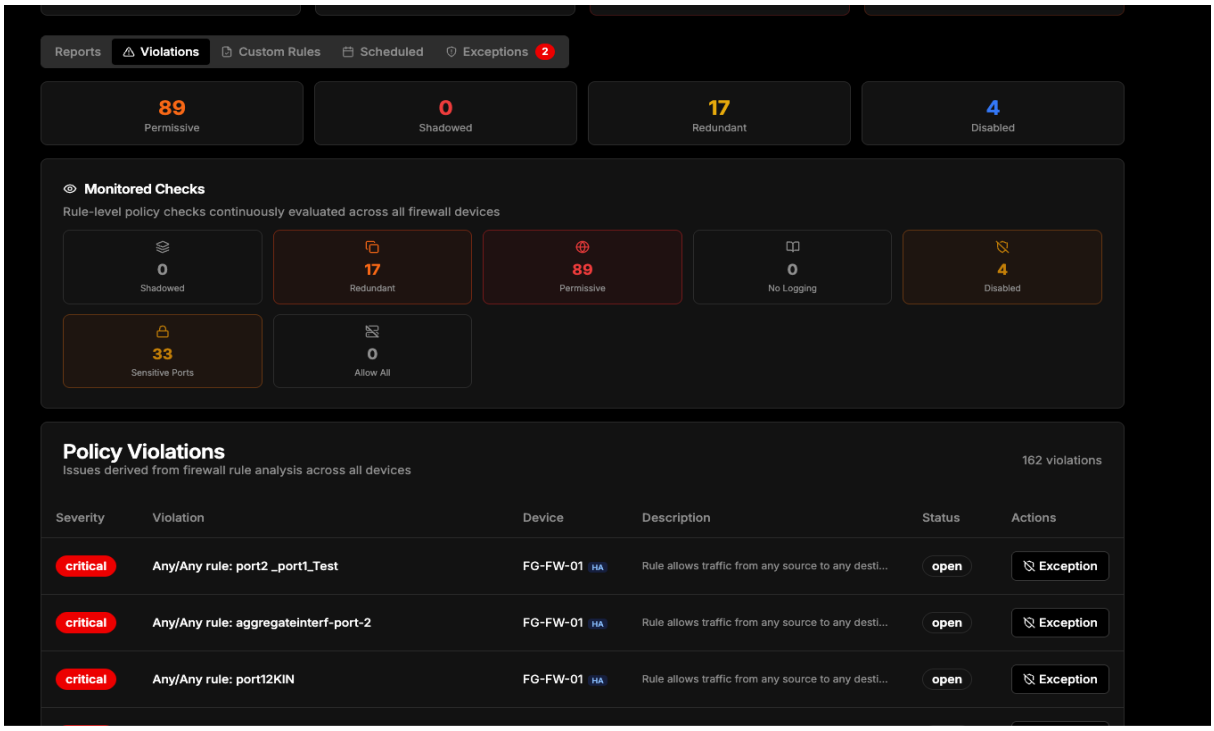
Firewall Assurance is the foundation of FlowGuard's policy management capability, delivering complete visibility and control over firewall configurations across multi-vendor environments. It ensures that security policies remain optimized, compliant, and aligned with organizational needs, while reducing operational complexity.



- Multi-vendor firewall rule analysis with detection of redundant, shadowed, and conflicting rules.
- Automated policy optimization to streamline rule sets and enhance performance.
- Continuous compliance checks against regulatory frameworks and internal standards.
- Change validation workflows to assess the impact of proposed rule changes before implementation.
- Centralized visibility into all firewall policies across distributed environments.

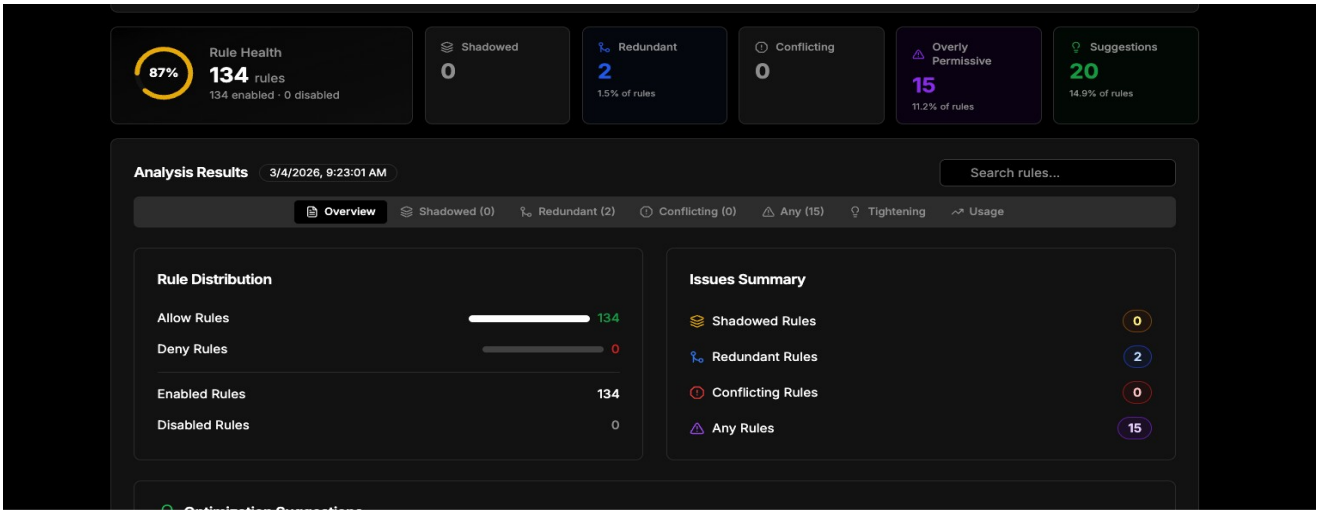
Advanced Rule & Network Modelling

The platform models complex configurations including access rules, NAT, VPNs, routing, and Policy-Based Routing (PBR). This comprehensive modelling gives security teams a realistic view of traffic flows across environments, enabling accurate impact analysis of rule changes and preventing unexpected disruptions.



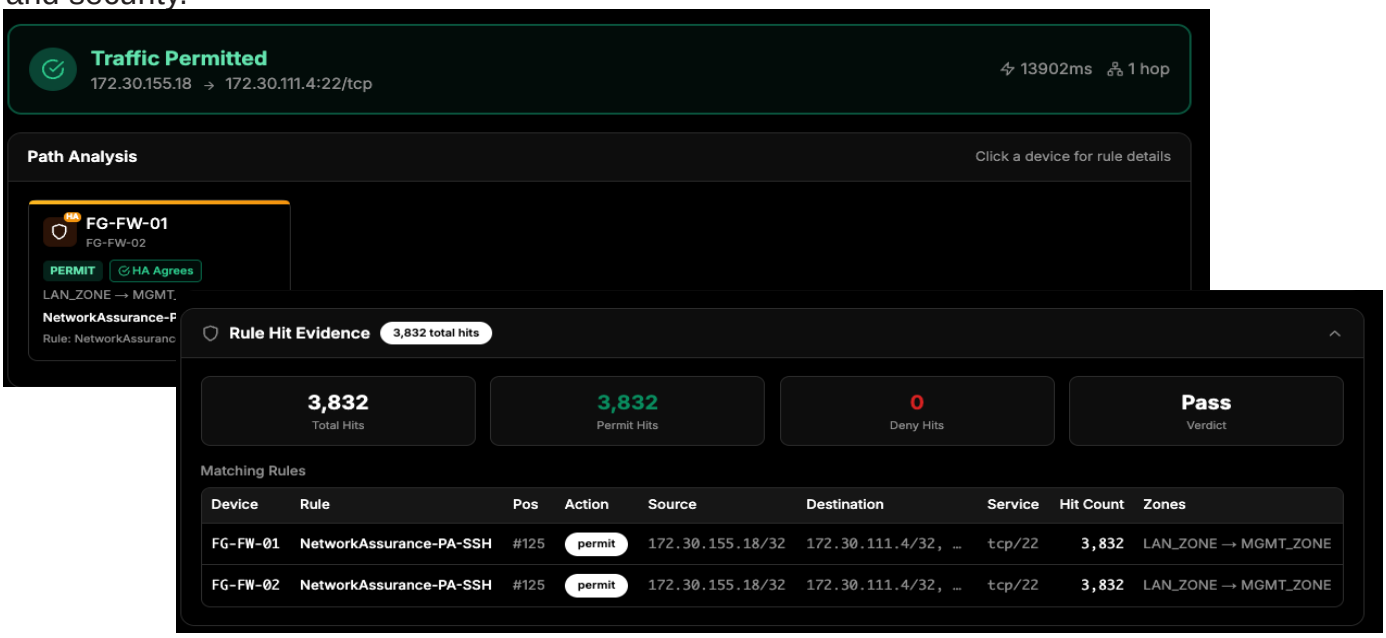
Shadowed & Redundant Rule Detection

FlowGuard automatically analyzes firewall rule bases to detect shadowed, redundant, or conflicting rules that could weaken security posture. By highlighting unused or risky rules, organizations can reduce exposure, optimize performance, and streamline audits.



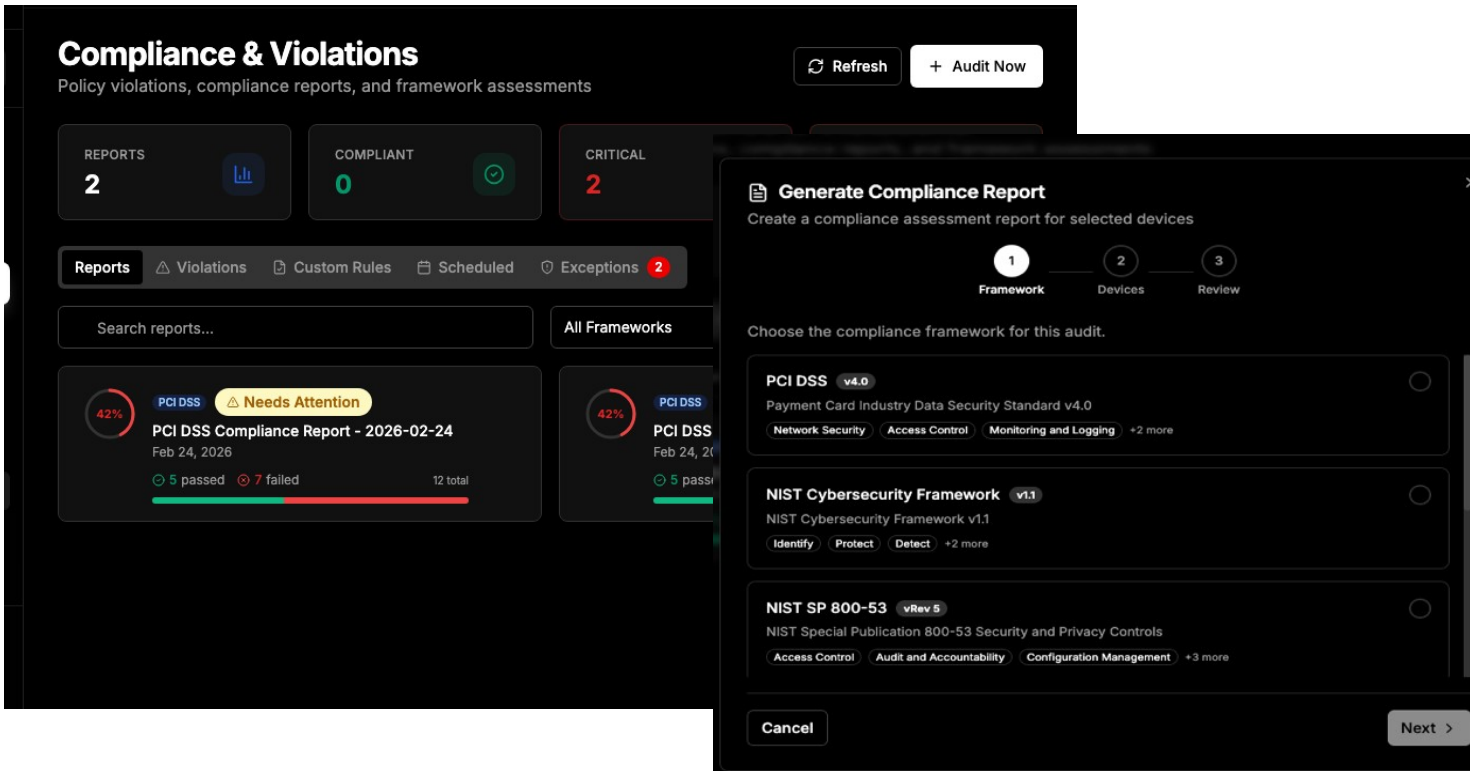
Firewall Rule Usage Analytics including VPN user access

By collecting firewall data, FlowGuard provides deep insights into actual rule usage. Security teams can identify unused or obsolete rules, assess the effectiveness of existing policies, and streamline configurations for performance and security.



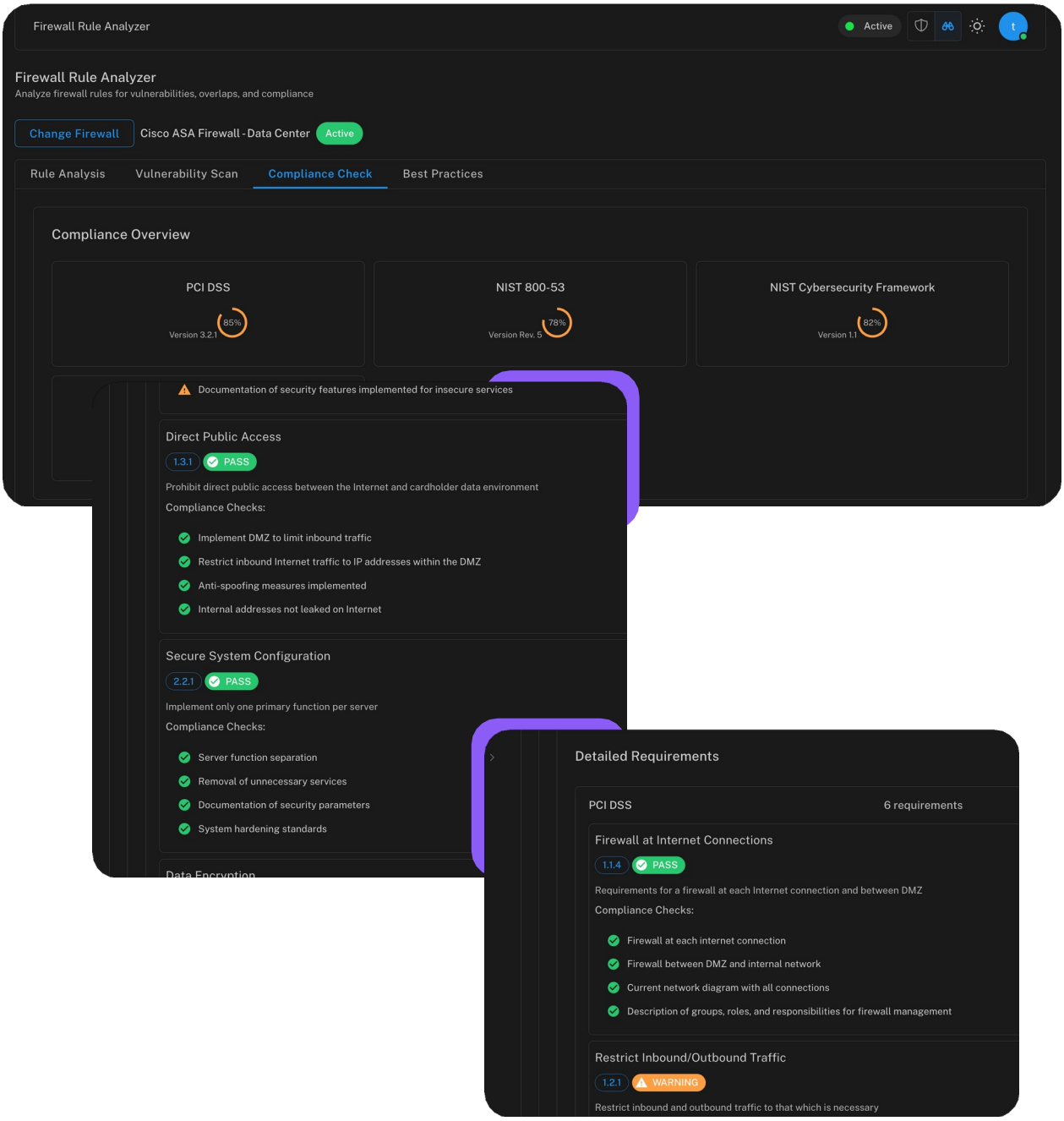
Automated Compliance Reporting

Compliance reporting is fully automated, with the ability to generate scheduled reports and forward them directly into third-party GRC platforms. This reduces manual reporting overhead and ensures auditors always have access to the latest validated data.



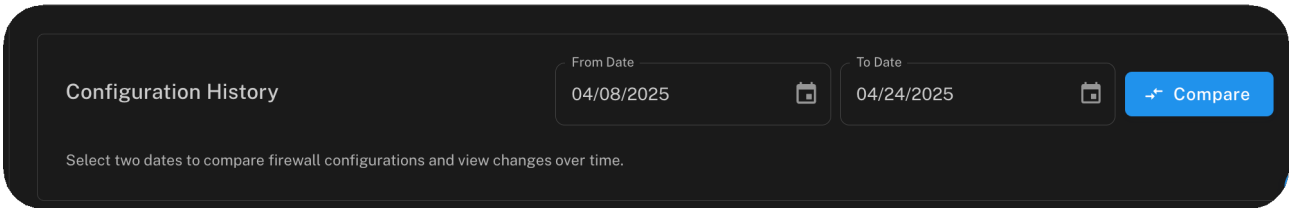
Out-of-the-Box Compliance Templates

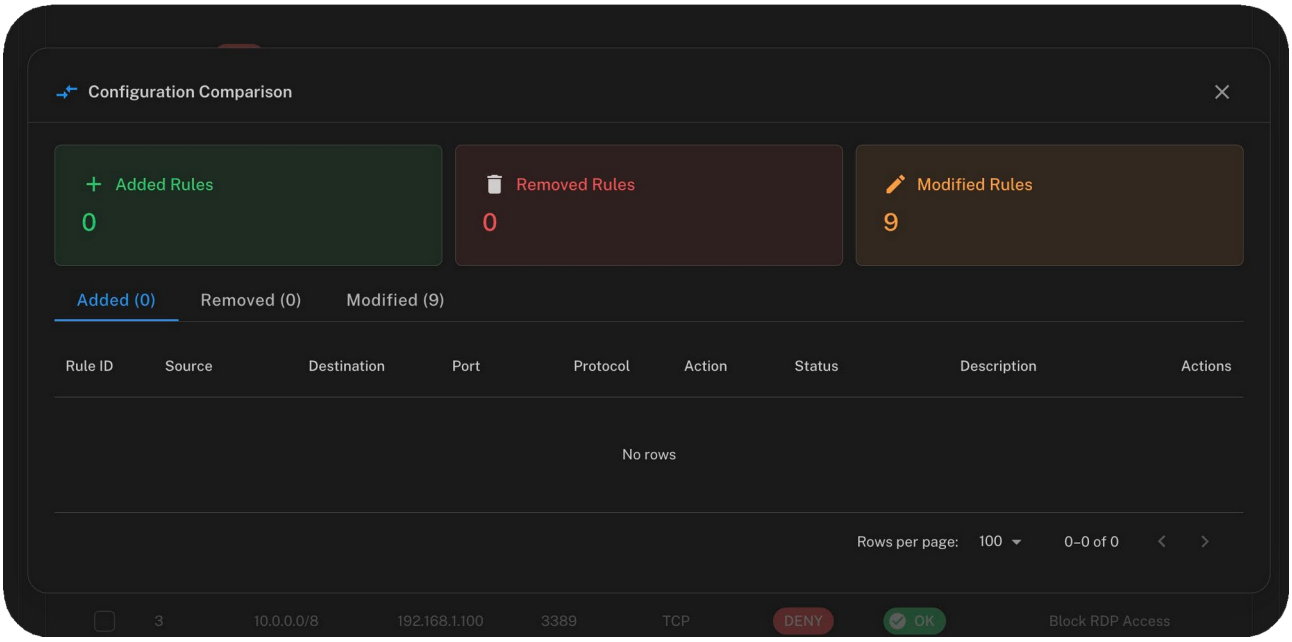
The solution comes with prebuilt compliance templates for standards such as NIST and PCI DSS. These templates accelerate deployment, simplify ongoing validation, and give organizations a quick start to achieving compliance goals without lengthy customization.

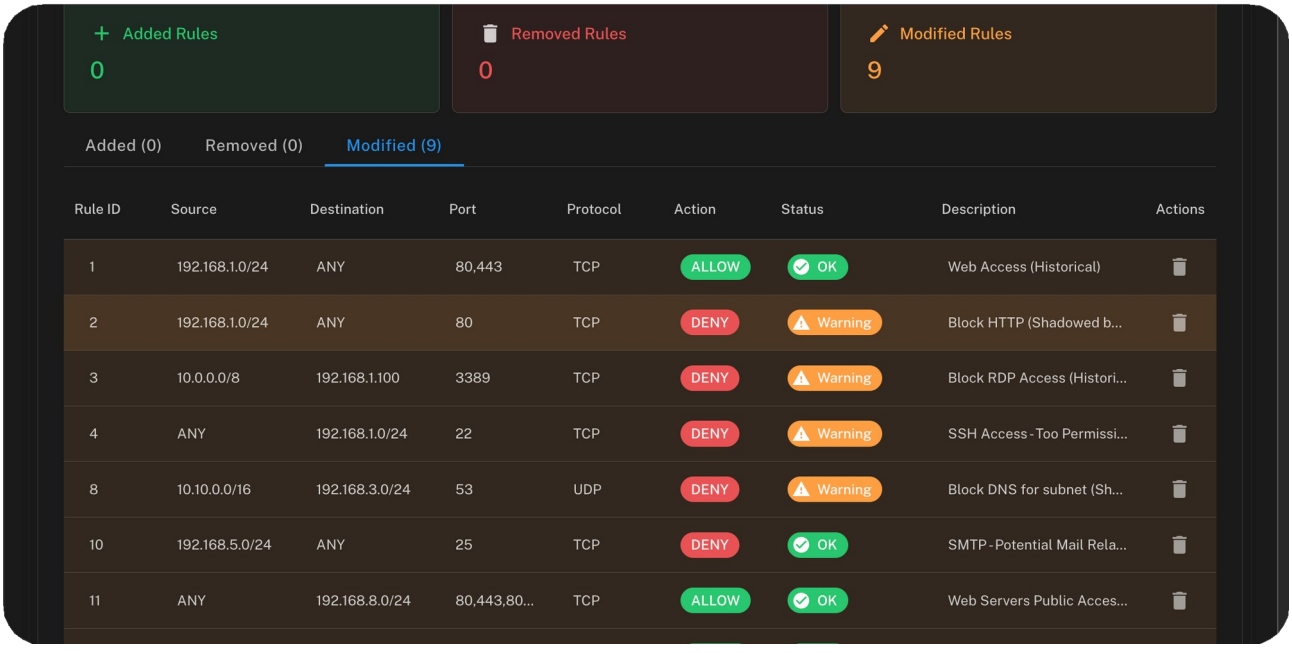


Configuration Change Analysis

Security teams can compare firewall rule bases side by side at two different points in time to identify changes in configuration. This feature simplifies troubleshooting, validates the accuracy of rule changes, and provides a clear audit trail for compliance and incident investigations.

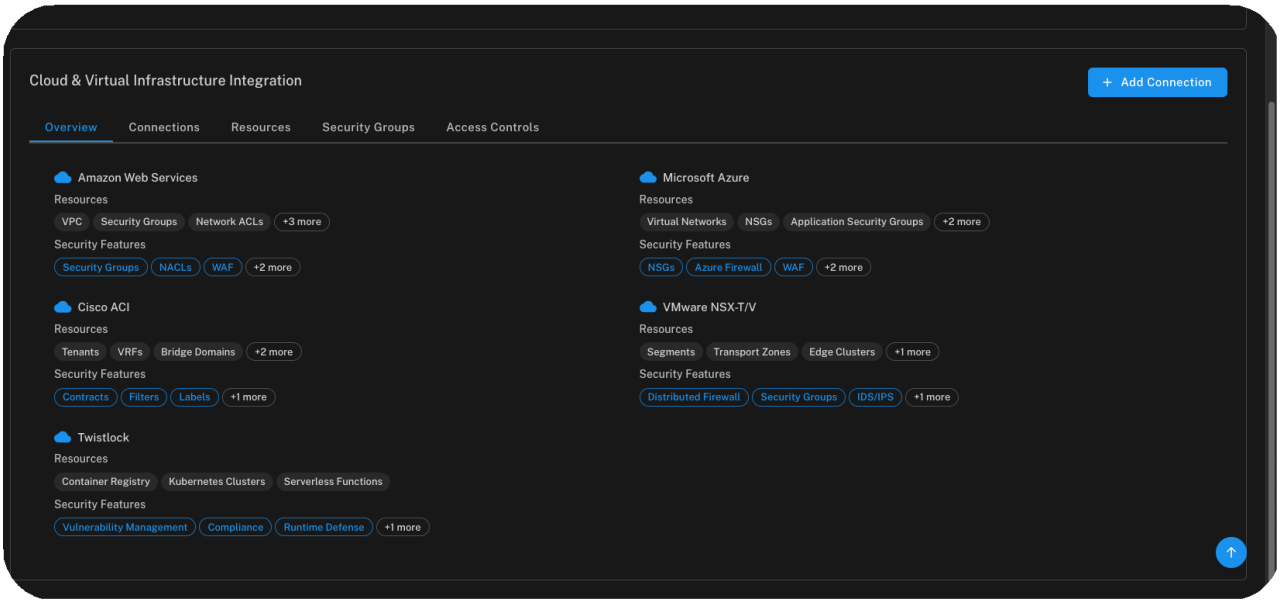


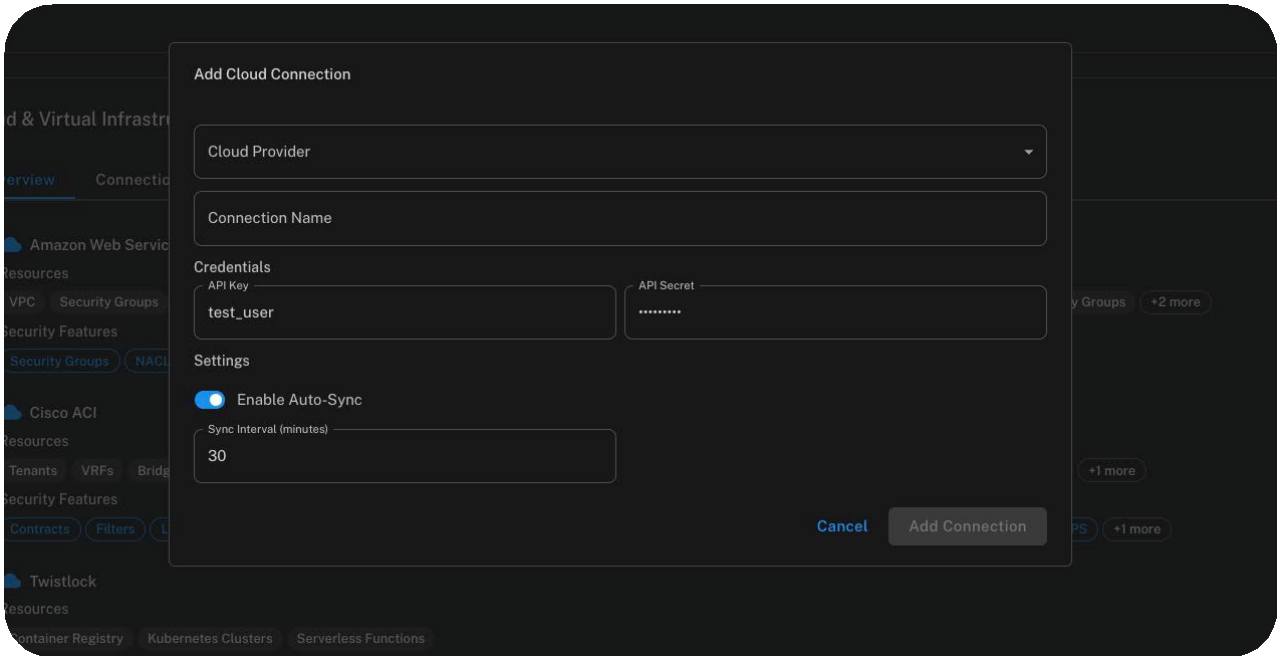




Cloud & Virtual Environment Integration

FlowGuard integrates with AWS, Azure, Cisco ACI, VMware NSX-T/V, and container environments. It models security groups, virtual infrastructure, and access possibilities across cloud and hybrid setups, ensuring firewall assurance extends to modern architectures.





FlowGuard

NETWORK ASSURANCE

Hybrid network mapping and predictive attack path simulation.

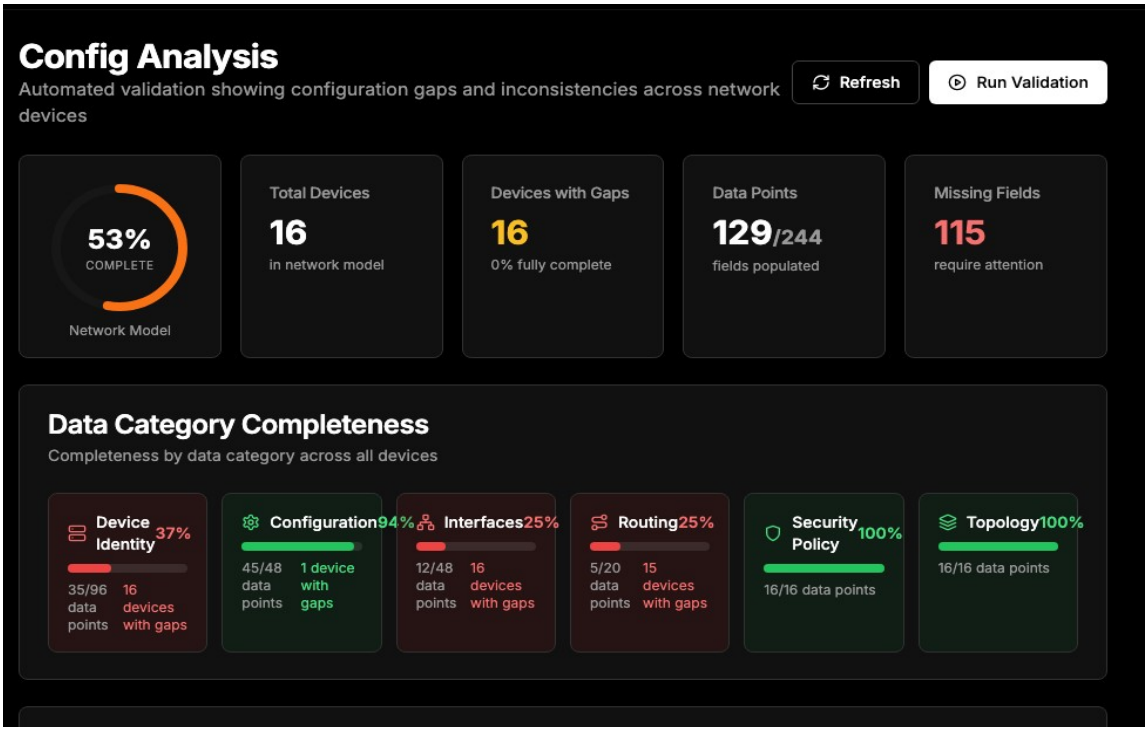
Network Assurance

Network Assurance gives enterprises complete visibility into their hybrid infrastructures, validating that network configurations, segmentation, and connectivity align with security and business requirements. By continuously modelling network topology and simulating attack paths, FlowGuard ensures that unauthorized access and lateral movement are proactively identified and contained.

- End-to-End Topology Mapping – Builds an always up-to-date model of your on-prem, cloud, and Operational Technology networks.
- Segmentation & Zero Trust Validation – Confirms that security zones and policies are enforced as designed.
- Attack Path Simulation – Identifies possible lateral movement or misconfigurations that could expose critical assets.
- Change Impact Analysis – Predicts how proposed network changes will affect security and connectivity.
- Continuous Compliance – Validates networks against regulatory frameworks and internal segmentation policies.

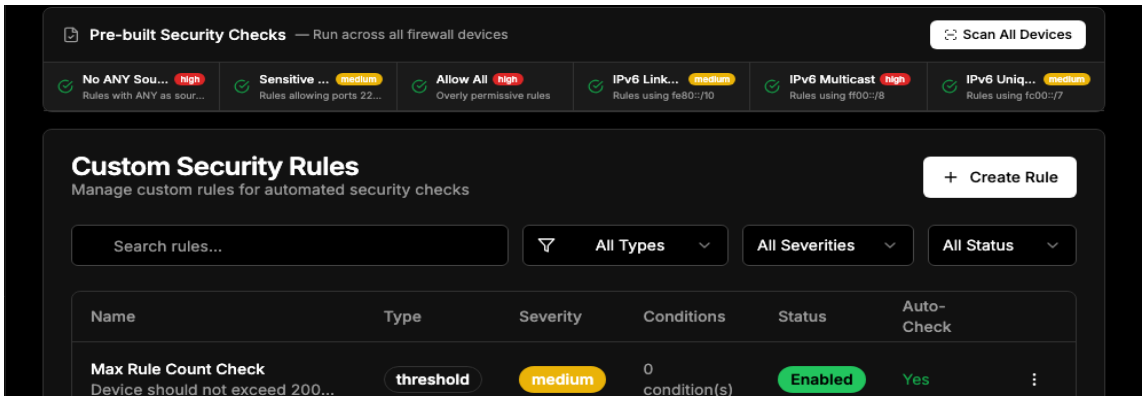
Configuration Compliance Reporting

FlowGuard Network Assurance continuously audits configurations across all supported network devices and vendors, producing clear, actionable compliance reports. Deviations are highlighted with severity, control references, and remediation guidance.



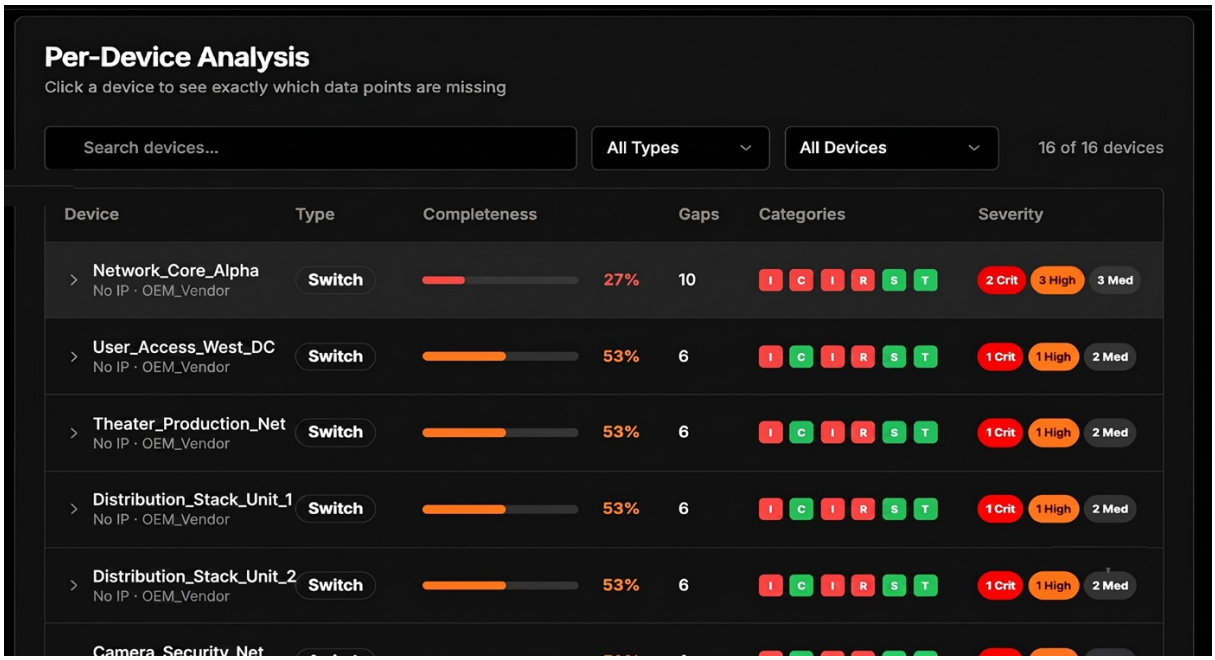
Custom Compliance Policies

Define your own configuration baselines and checks to reflect internal standards or architectural patterns. Custom rules (including regex) let you validate exactly what matters in your environment.



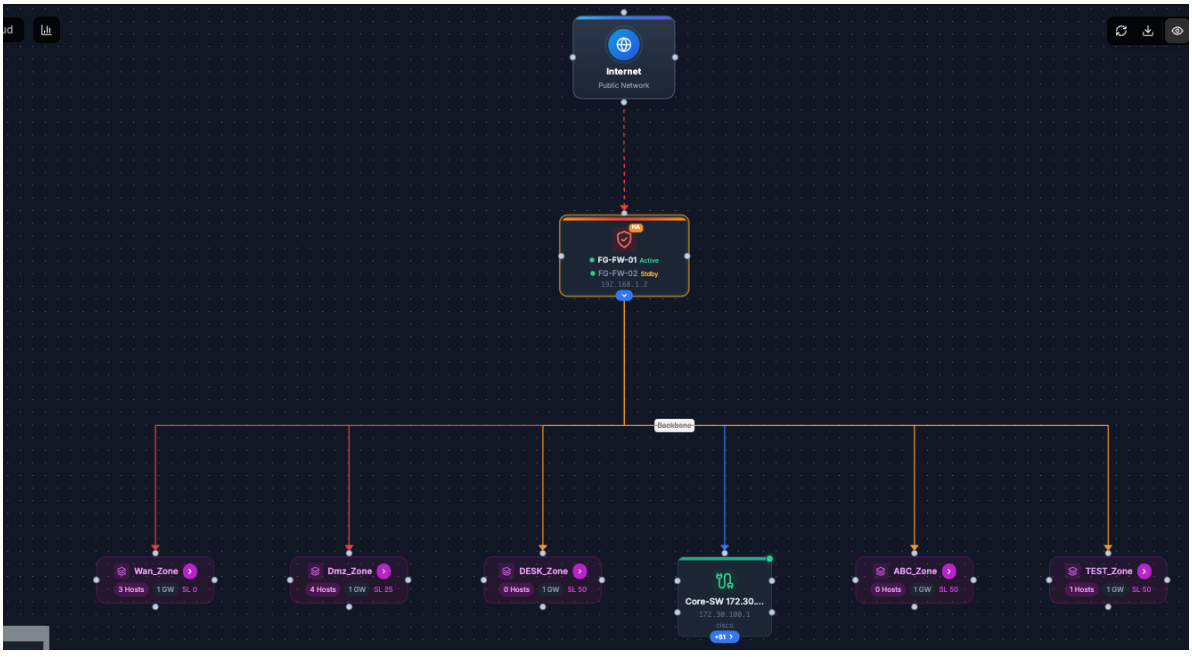
Security Zone Path Visibility

Map paths between security zones (e.g., PCI, DMZ, OT) to validate segmentation and prove that sensitive environments are properly isolated.



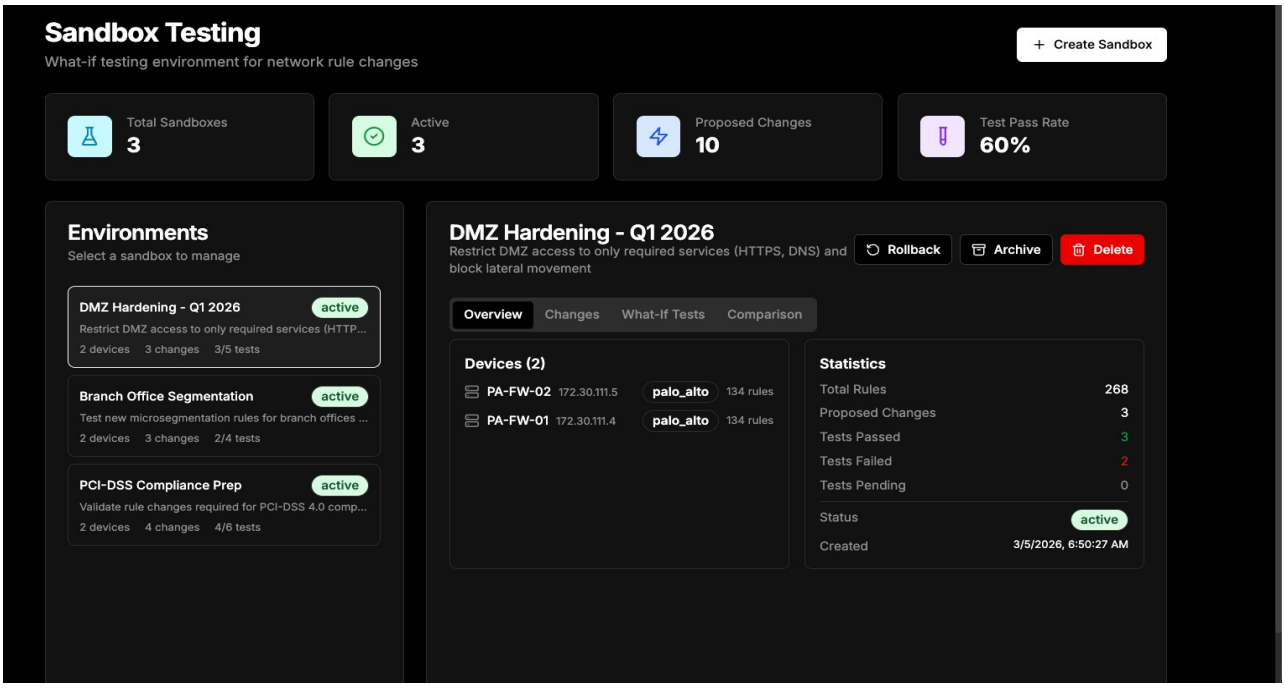
Connectivity & Topology Visualization

Query the model and render an interactive topology with explicit allowed and denied paths, accelerating troubleshooting and design reviews.



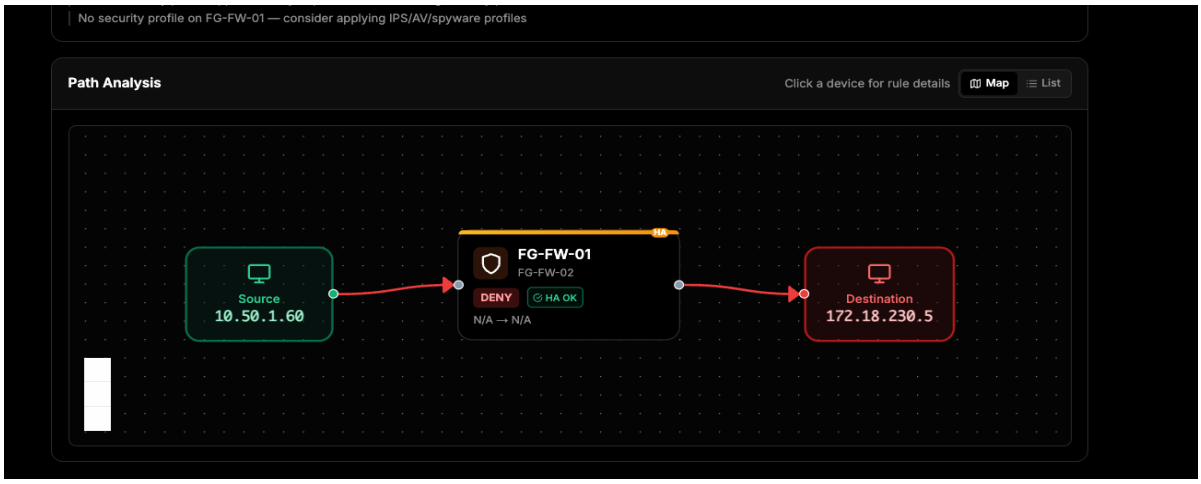
Scheduled “What-If” Simulations

Answer questions like “what’s reachable from the internet?” on demand or on a recurring schedule to track exposure trends over time.



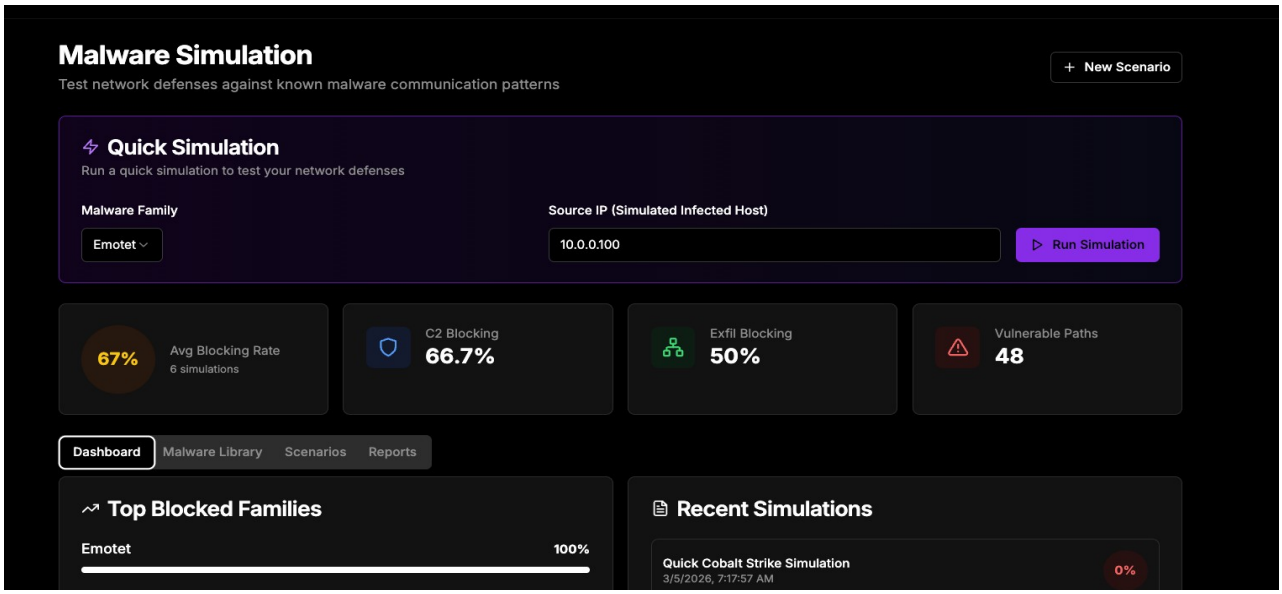
Advanced Behavior Modeling

Accurately model VPNs, NAT, load-balancers, and device-specific logic so simulated paths match real-world outcomes.



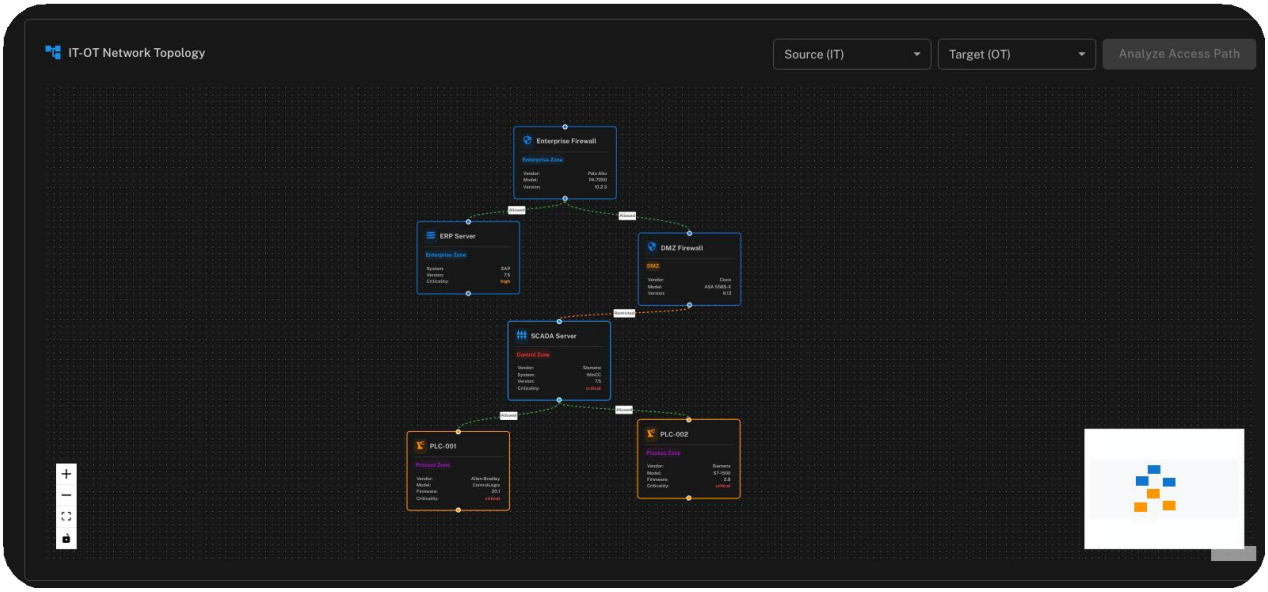
Malware Defense Planning (Scenario Templates)

Use predefined or custom malware scenarios to test containment strategies and verify that existing controls disrupt spread and data loss.



Unified IT/OT Modeling

Model OT networks alongside IT in a single view for end-to-end assurance across converged environments and critical infrastructure.



FlowGuard

VULNERABILITY CONTROL

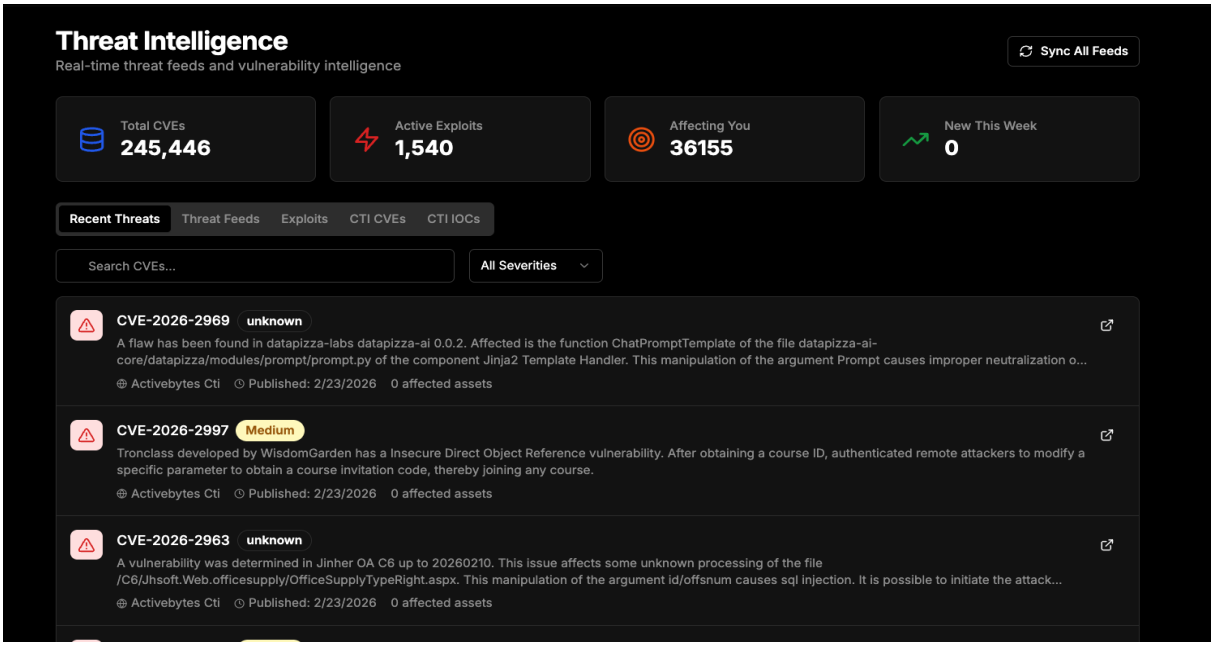
Prioritizing exposure by business impact and network context.

Vulnerability Control

Vulnerability & Control Module extends the platform's assurance capabilities by continuously identifying, assessing, and prioritizing security exposures across on-premise, cloud, and hybrid environments. It goes beyond basic vulnerability scanning by correlating threat intelligence, asset criticality, and network reachability to determine the real business risk of each vulnerability. With automated risk scoring, remediation guidance, and compliance alignment, this feature enables organizations to focus on the vulnerabilities that matter most, reduce their attack surface, and demonstrate measurable improvements in security posture.

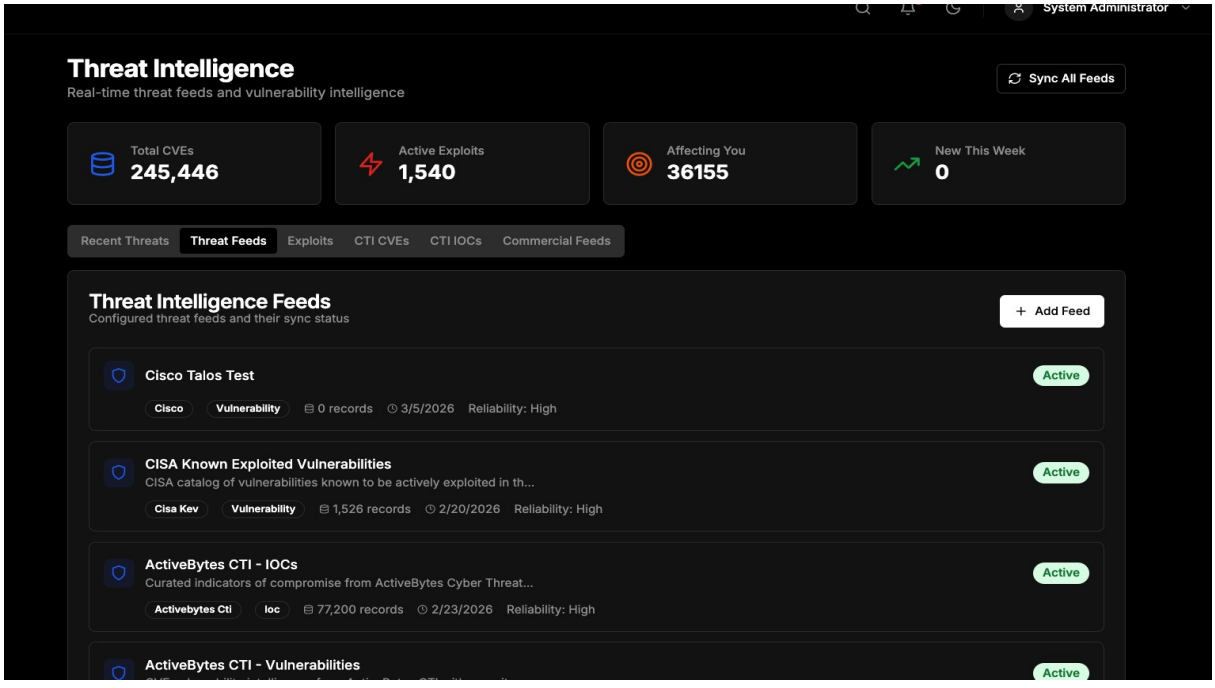
Native Threat Intelligence Feed

The Vulnerability Control provides its own technical threat intelligence feed, ensuring up-to-date coverage of vulnerabilities and exploits relevant to your environment.



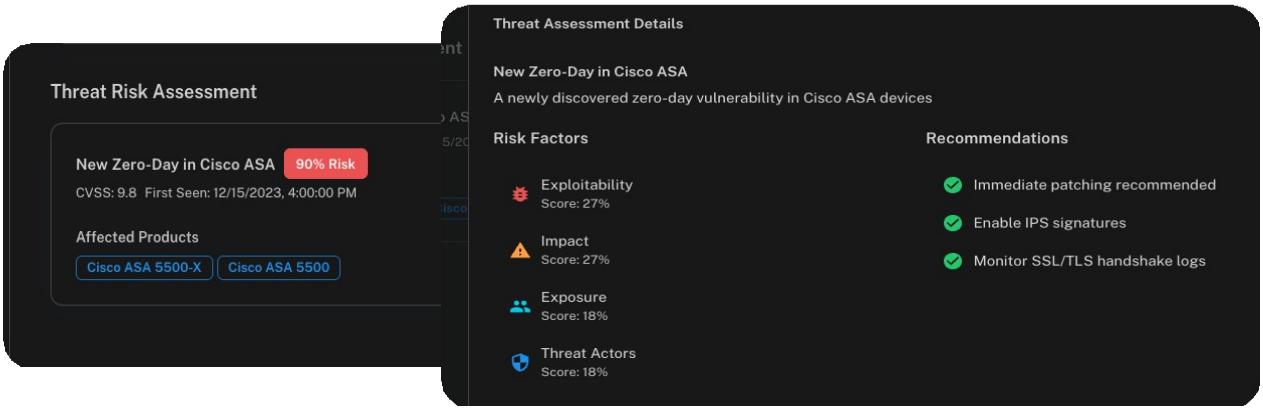
Comprehensive Threat Sources

FlowGuard, Vulnerability Control aggregates intelligence from over 30 sources, including NVD, vendor bulletins, third-party feeds, and published vulnerability databases, creating a unified and reliable source of actionable threat information.



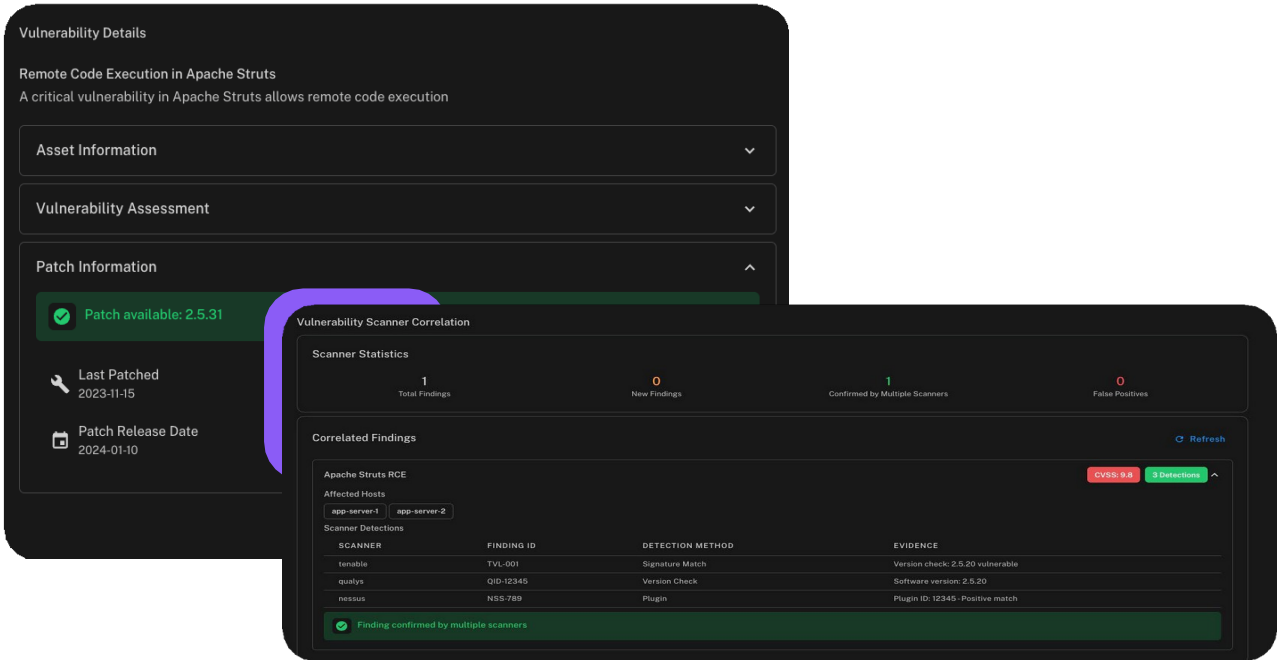
Automated Risk Assessment

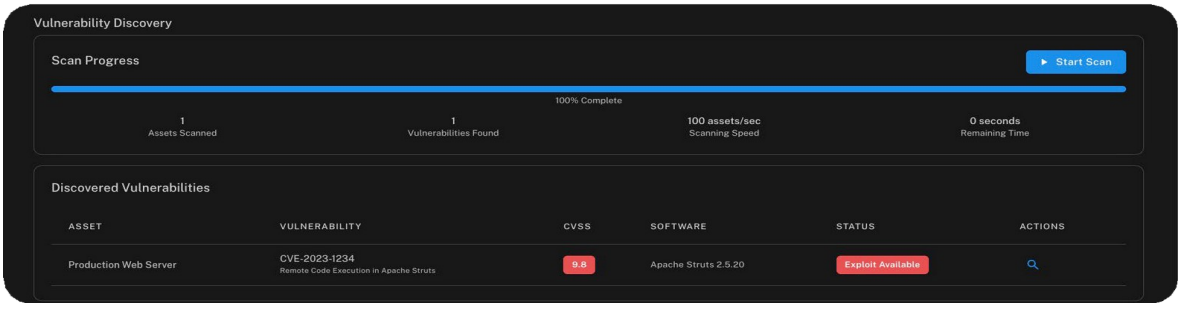
New threats are automatically evaluated against deployed assets and network topology, producing prioritized risk scores to help organizations remediate the most critical vulnerabilities first.



Threat Comparison with Repositories

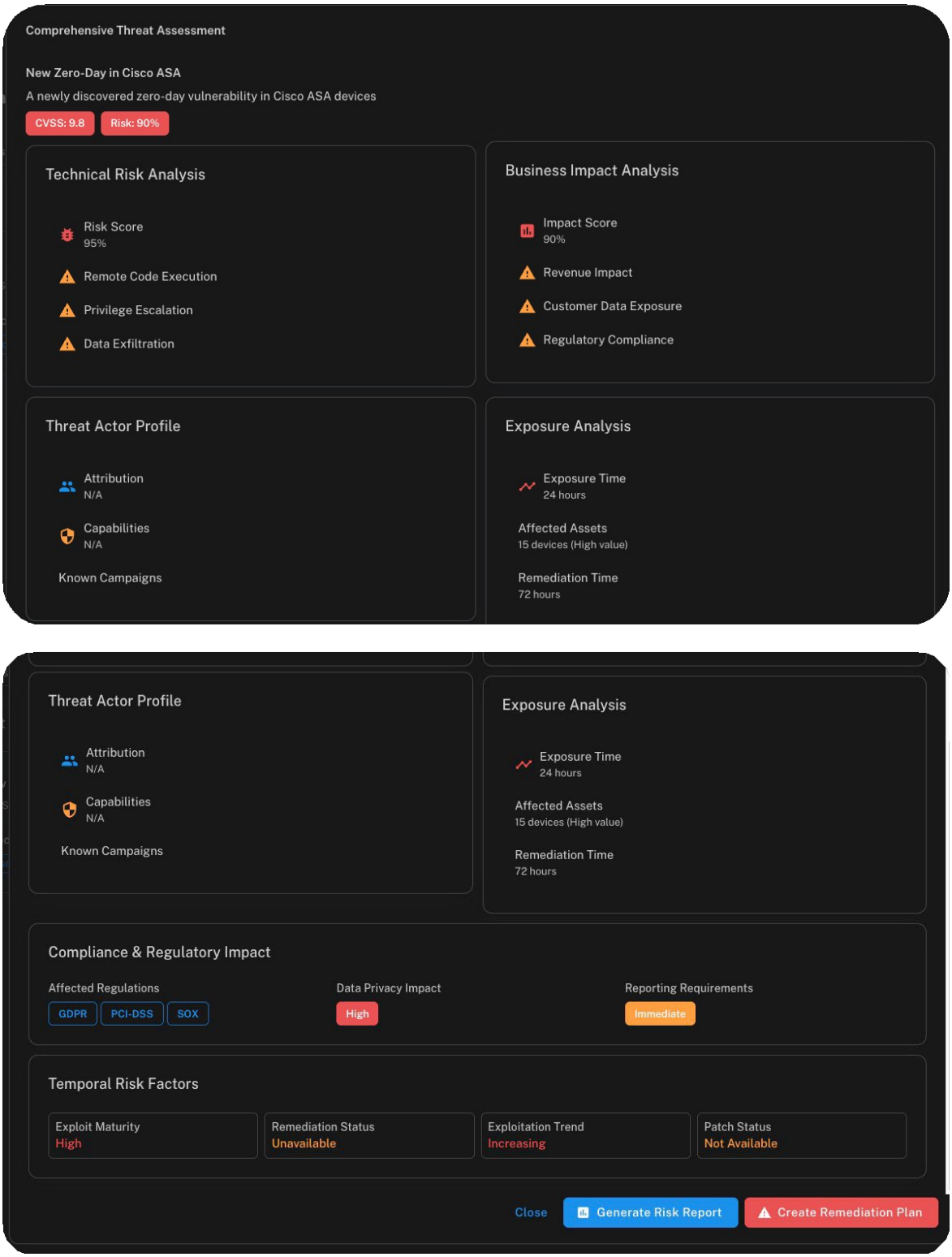
FlowGuard Vulnerability Control compares incoming threat data with patch management systems and vulnerability scanner outputs, correlating findings to identify gaps and reduce redundant remediation efforts.





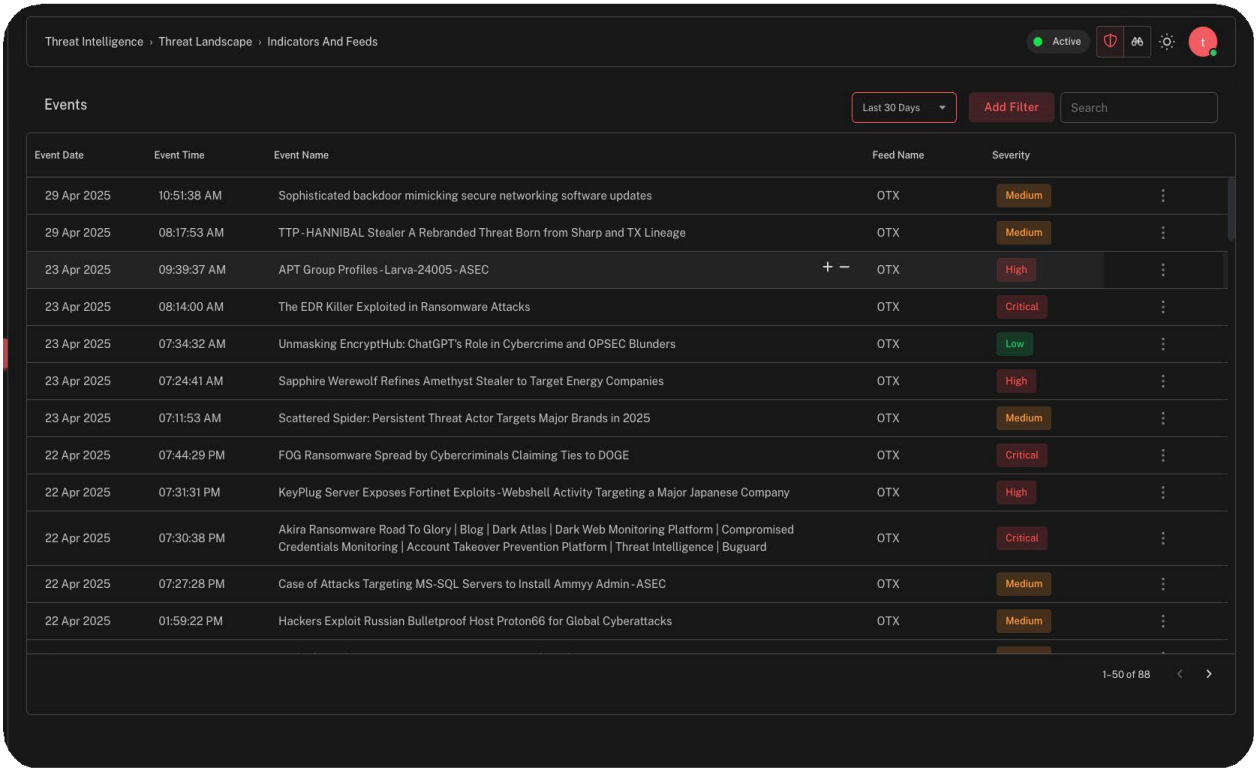
CVSS-Based Risk Assessment

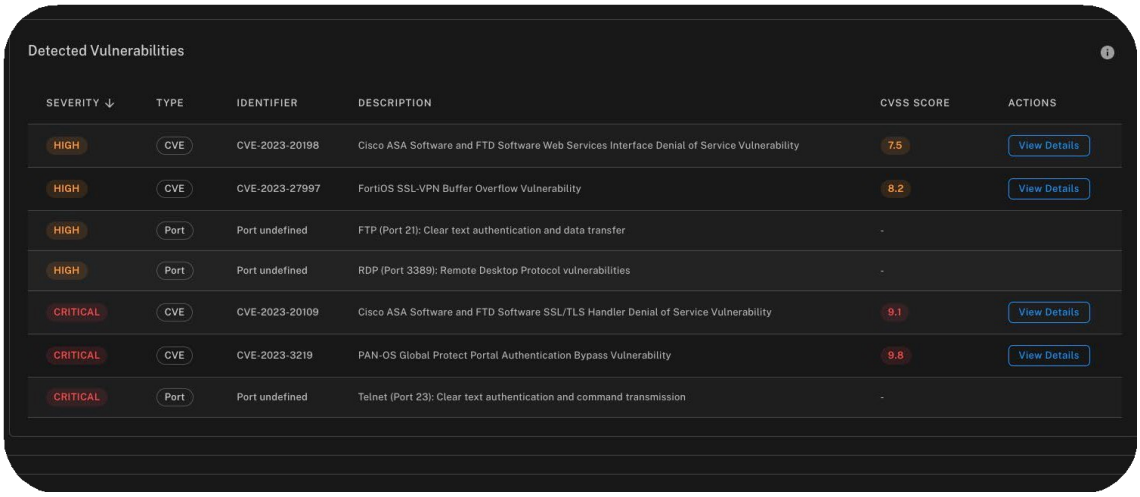
FlowGuard Vulnerability Control evaluates vulnerabilities using CVSS parameters, including Base Score, Attack Vector, Privileges Required, User Interaction, Scope, and Impact Subscores, delivering standardized, actionable risk assessments.



Daily Threat Intelligence Updates

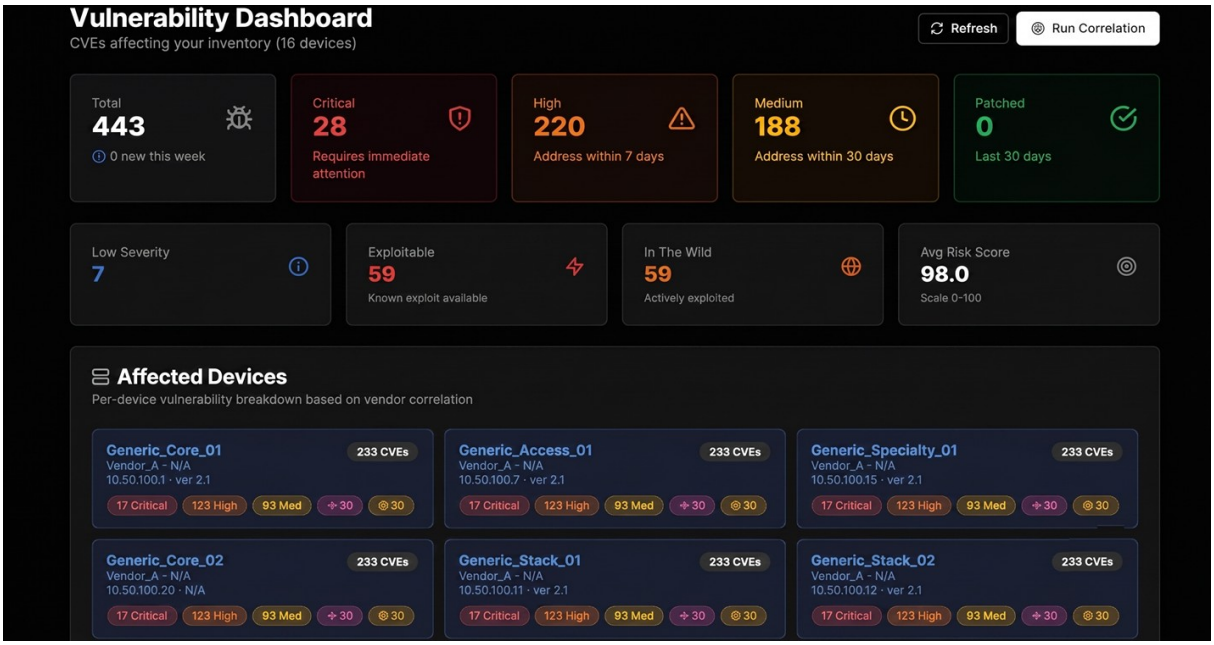
FlowGuard integrates with daily-updated threat intelligence feeds that track the latest vulnerabilities impacting firewall devices. This ensures firewall compliance analysis is always aligned with current global threat trends, reducing exposure to newly discovered risks.



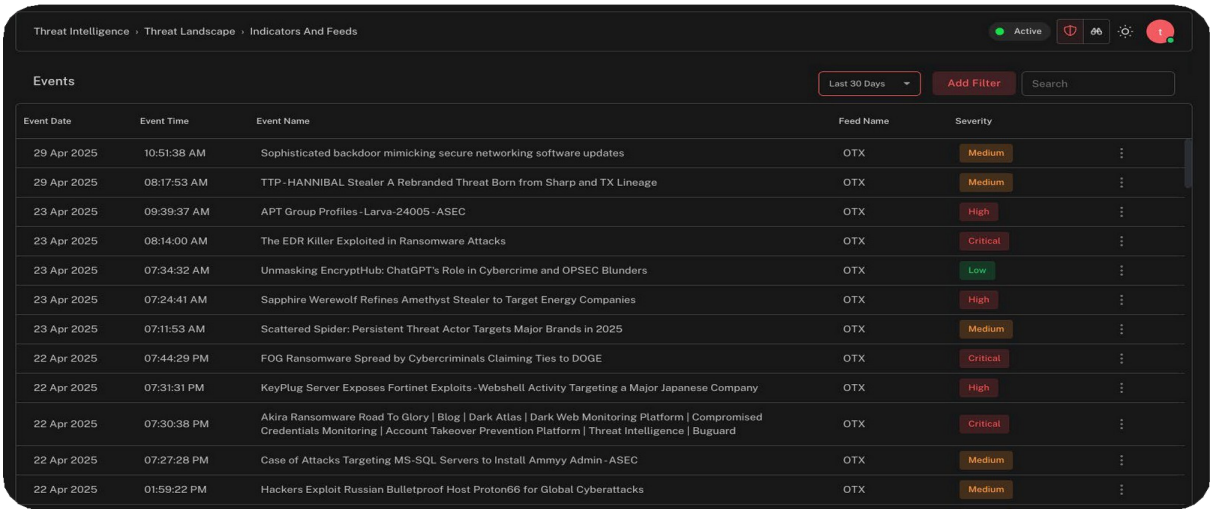


Broad Vulnerability Intelligence

The threat intelligence module is not limited to firewalls. It delivers vulnerability coverage across operating systems, business applications, developer tools, mobile and IoT devices, and network/security technologies — giving a holistic view of risks that impact firewall relevance and rule decisions.



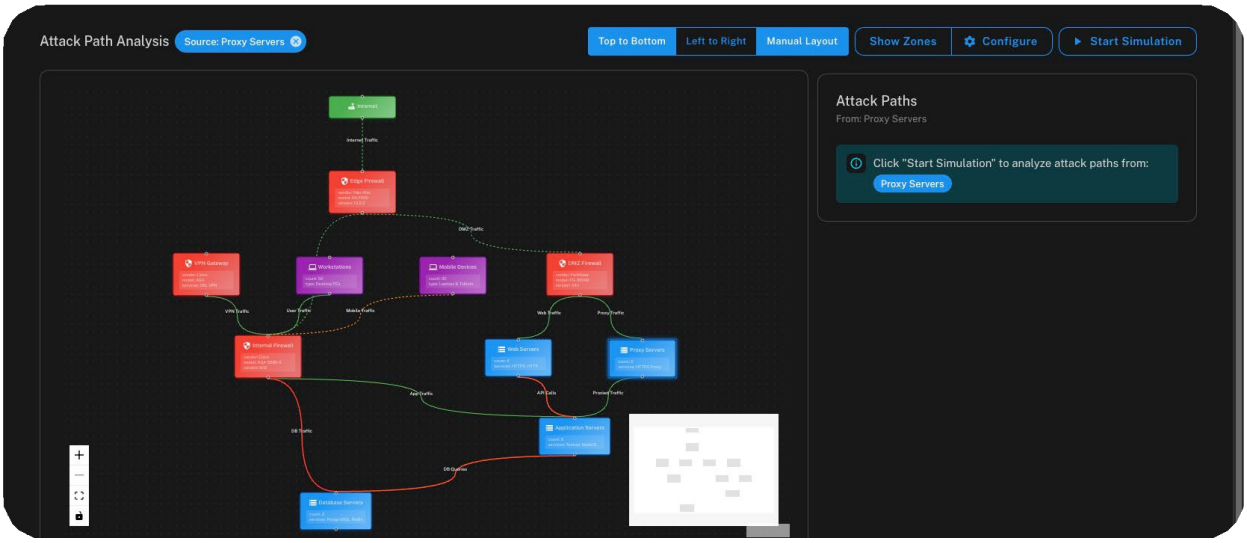
ID	Description	Severity	Score	Created on
#CVE-2025-29906	Finit is a fast init for Linux systems. Versions starting from 3.0-rc1 and prior to version 4.11 bundle an implementation of getty for the `tty` configuration directive that can bypass `/bin/login`, i.e., a user can log in as any user without authentication. This issue has been patched in version 4.11.	High	8.6	30 Apr 2025
#CVE-2025-46550	YesWiki is a wiki system written in PHP. Prior to version 4.5.4, the `/?BazaR` endpoint and `idformulaire` parameter are vulnerable to cross-site scripting. An attacker can use a reflected cross-site scripting attack to steal cookies from an authenticated user by having them click on a malicious link. Stolen cookies allow the attacker to take over the user's session. This vulnerability may also allow attackers to deface the website or embed malicious content. This issue has been patched in version 4.5.4.	Medium	4.3	30 Apr 2025
#CVE-2025-46549	YesWiki is a wiki system written in PHP. Prior to version 4.5.4, an attacker can use a reflected cross-site scripting attack to steal cookies from an authenticated user by having them click on a malicious link. Stolen cookies allow the attacker to take over the user's session. This vulnerability may also allow attackers to deface the website or embed malicious content. This issue has been patched in version 4.5.4.	Medium	4.3	30 Apr 2025
#CVE-2025-46348	YesWiki is a wiki system written in PHP. Prior to version 4.5.4, the request to commence a site backup can be performed and downloaded without authentication. The archives are created with a predictable filename, so a malicious user could create and download an archive without being authenticated. This could result in a malicious attacker making numerous requests to create archives and fill up the file system, or by downloading the archive which contains sensitive site information. This issue has been patched in version 4.5.4.	Critical	10	30 Apr 2025

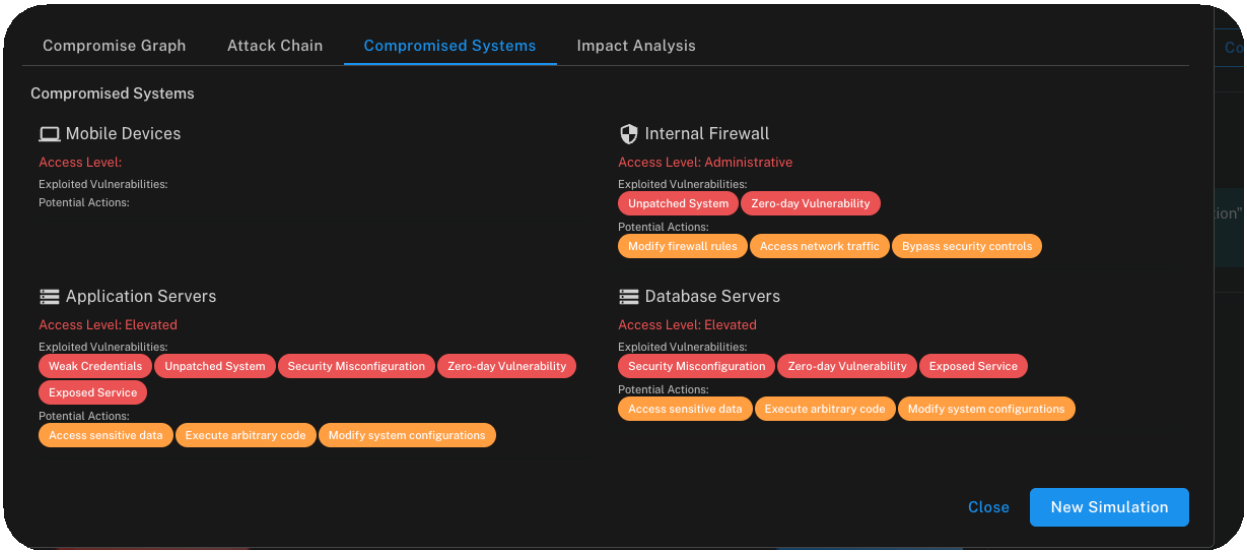


Event Date	Event Time	Event Name	Feed Name	Severity
29 Apr 2025	10:51:38 AM	Sophisticated backdoor mimicking secure networking software updates	OTX	Medium
29 Apr 2025	08:17:53 AM	TTP-HANNIBAL Stealer A Rebranded Threat Born from Sharp and TX Lineage	OTX	Medium
23 Apr 2025	09:39:37 AM	APT Group Profiles-Larva-24005-ASEC	OTX	High
23 Apr 2025	08:14:00 AM	The EDR Killer Exploited in Ransomware Attacks	OTX	Critical
23 Apr 2025	07:34:32 AM	Unmasking EncryptHub: ChatGPT's Role in Cybercrime and OPSEC Blunders	OTX	Low
23 Apr 2025	07:24:41 AM	Sapphire Werewolf Refines Amethyst Stealer to Target Energy Companies	OTX	High
23 Apr 2025	07:11:53 AM	Scattered Spider: Persistent Threat Actor Targets Major Brands in 2025	OTX	Medium
22 Apr 2025	07:44:29 PM	FOG Ransomware Spread by Cybercriminals Claiming Ties to DOGE	OTX	Critical
22 Apr 2025	07:31:31 PM	KeyPlug Server Exposes Fortinet Exploits-Webshell Activity Targeting a Major Japanese Company	OTX	High
22 Apr 2025	07:30:38 PM	Akira Ransomware Road To Glory | Blog | Dark Atlas | Dark Web Monitoring Platform | Compromised Credentials Monitoring | Account Takeover Prevention Platform | Threat Intelligence | Buguard	OTX	Critical
22 Apr 2025	07:27:28 PM	Case of Attacks Targeting MS-SQL Servers to Install Ammyy Admin-ASEC	OTX	Medium
22 Apr 2025	01:59:22 PM	Hackers Exploit Russian Bulletproof Host Proton66 for Global Cyberattacks	OTX	Medium

Attack Path Simulation

Simulate attacks originating from external networks such as the Internet or partner networks, evaluating how threats could traverse the infrastructure and which assets are at risk.





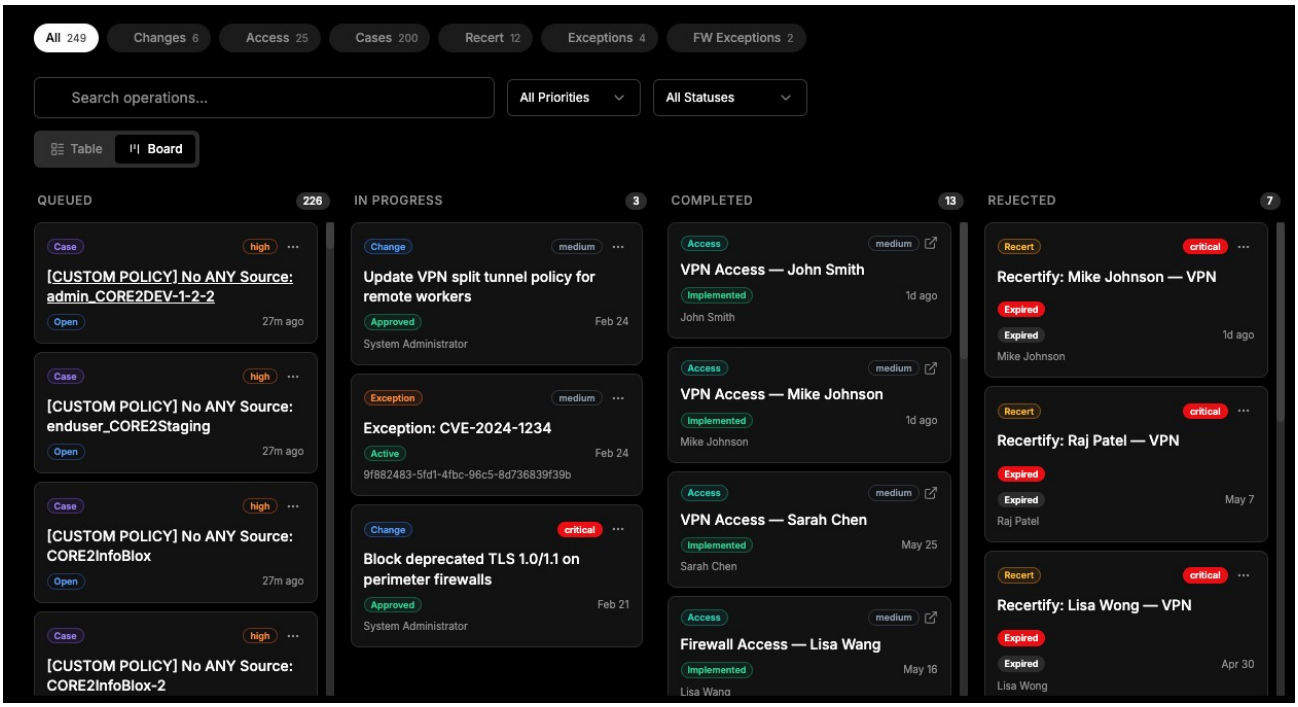
FlowGuard

OPERATIONS MANAGEMENT

Unified command for lifecycle changes and access requests.

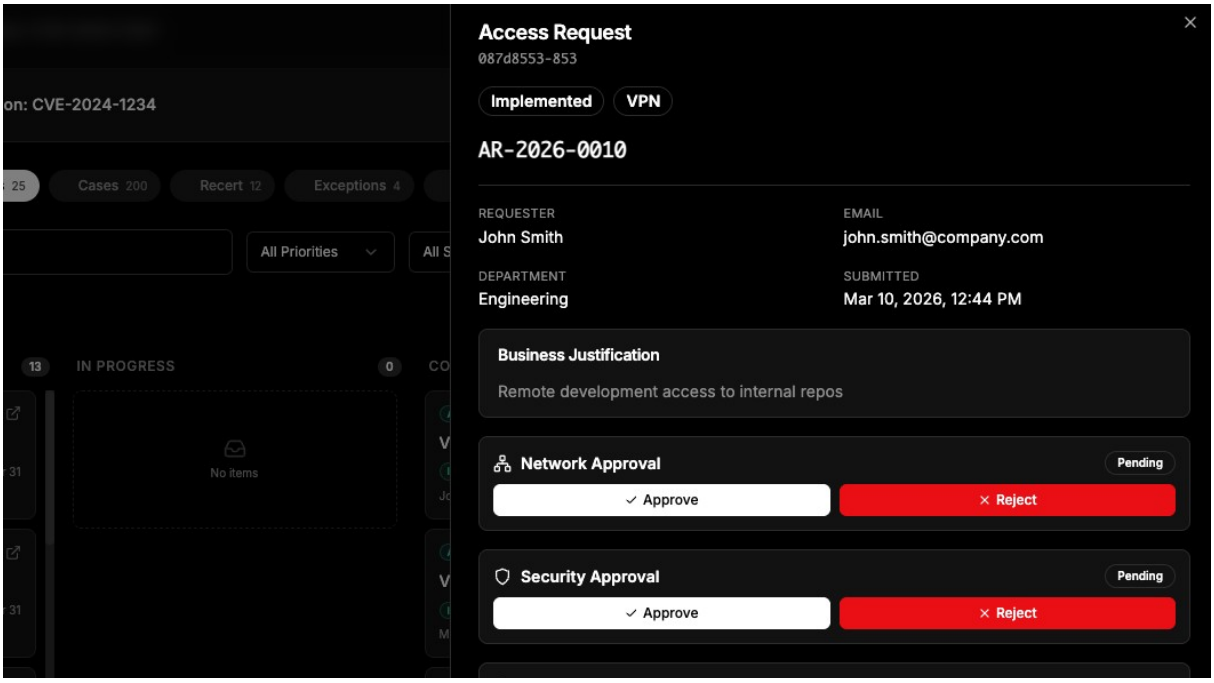
Unified Change & Exception Handling

Consolidates all policy modifications, security exceptions, and periodic firewall recertifications into a single pane of glass. It acts as the definitive system of record for all operational shifts triggered by the other FlowGuard modules.



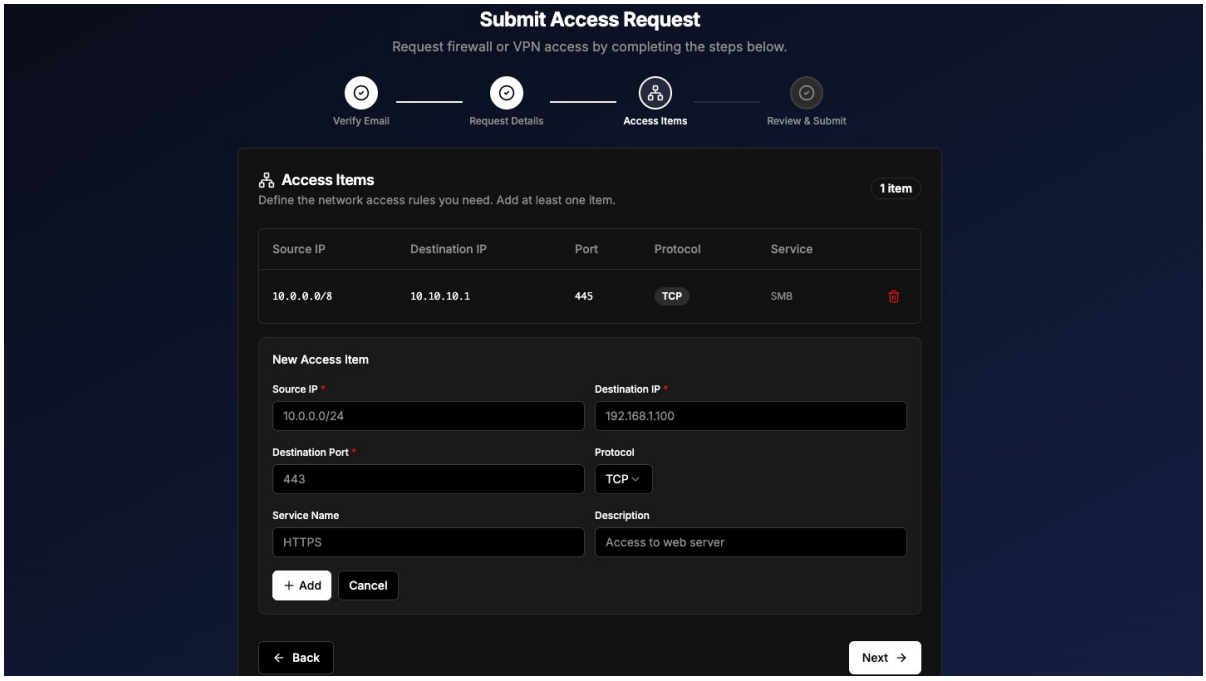
Intelligent Workflow & Lifecycle Automation

Features robust, approval and rejection workflows. The system autonomously manages the administrative burden by sending automated reminders, tracking follow-ups, and maintaining a strict, audit-ready paper trail for every decision made.



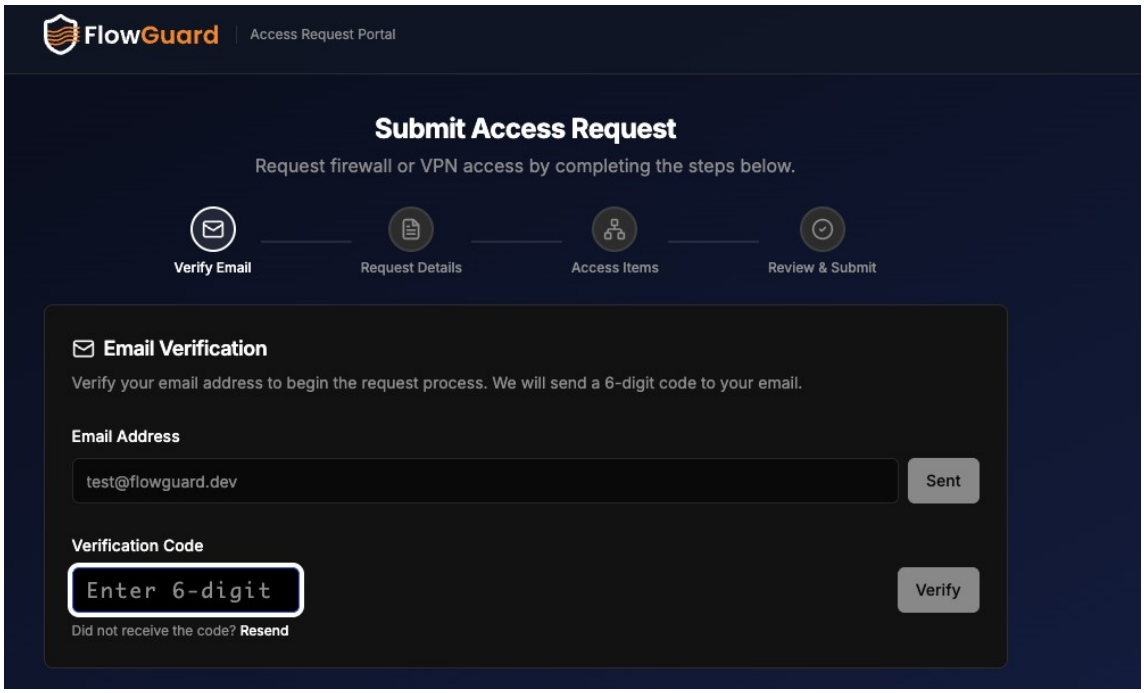
Frictionless Cross-Departmental Request Portal

A secure, streamlined extension designed specifically for non-network personnel (e.g., developers, internal staff, and external contractors). It allows users to easily submit Firewall or VPN access requests without needing complex system accounts.



Passwordless Verification & Pre-Analyzed Routing

Leveraging secure, email-based passwordless authentication, the portal verifies the identity of the requester seamlessly. Once a request is submitted, FlowGuard automatically performs a preliminary compliance and "break" analysis. The Network Team is then presented with a fully analyzed ticket, requiring only a simple, informed Approval or Rejection.



FlowGuard:
Comprehensive Security Assurance Platform

From Visibility to Actionable Security FlowGuard, developed by Analyzet, is a next-generation, unified solution designed to give organizations complete visibility, control, and confidence over their network and security posture. By combining Firewall Assurance, Network Assurance, and Vulnerability Control, FlowGuard transforms complex enterprise environments into clear, actionable intelligence.

- With Firewall Assurance, FlowGuard ensures that rule bases are optimized, compliant, and free from redundant or risky configurations, while leveraging daily threat intelligence to proactively highlight vulnerabilities.
- Network Assurance delivers a living network model that maps access paths, simulates potential attack vectors, and validates segmentation across complex environments.
- Vulnerability Control continuously identifies, assesses, and prioritizes threats, correlating asset criticality, configuration, and exploitability to produce actionable remediation insights.

Built for automation, scalability, and integration, FlowGuard connects seamlessly with GRC platforms, vulnerability scanners and SIEMs, ensuring that both technical teams and executives can track, analyse, and remediate risks efficiently. Its advanced features including attack path simulation, malware scenario modelling, and OT coverage enable organizations to reduce their attack surface, enforce zero-trust principles, and demonstrate measurable improvements in security posture.

FlowGuard empowers security teams to monitor, validate, and secure their network proactively, giving confidence that every policy, connection, and vulnerability is continuously assessed and mitigated.

Analyzet FlowGuard:
Security Assured, Risks Controlled.

Notice

This document contains information about the proprietary property of Analyzet. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of Analyzet.

Nothing in this document constitutes a guarantee, warranty, or license, express or implied. Analyzet disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to Fitness for a particular purpose; merchantability; not infringement of intellectual property or other rights of any third party or of Analyzet; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technology discussed
herein and is advised to seek the advice of competent legal counsel, without obligation of Analyzet.

Analyzet retains the right to make changes to this document at any time, without notice. Analyzet makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein.

Copyright

Analyzet

Dubai Silicon Oasis, Dubai, United Arab Emirates.
analyzet.com | contact@analyzet.com | +971 50 513 3973