SOLUTION BRIEF

# Fortinet and Axonius Security Solution

## Together, Fortinet and Axonius Provide Your Security and IT teams With Unparalleled Visibility Across All Networks, Devices, and Users to Reduce Your Attack Surface

### Executive Summary

Fortinet and Axonius have partnered to deliver comprehensive asset inventory for heterogenous deployments, helping uncover security coverage gaps and automate security policy validation and enforcement. By seamlessly connecting with the Fortinet FortiGate, FortiClient EMS, FortiEDR, and FortiPortal adapters in Axonius, IT and security teams can uncover risky devices, users, and network connections to continuously reduce the attack surface.

### Joint Solution Description

Organizations have many tools that know something about their attack surface, but what's needed is a correlator—something that can make sense of how every asset is configured and whether it poses a security risk.

Together, Fortinet and Axonius provide your security and IT teams unparalleled visibility across all networks, devices, and users in heterogenous, multi-vendor environments, giving them the ability to instantly identify security coverage gaps, unsanctioned software, and vulnerabilities that introduce risk.

### Joint Solution Components

Utilizing the Axonius Cybersecurity Asset Management Platform, IT and security teams gain a unified view into all assets to accelerate strategic decision-making and demonstrably reduce cyber risk. Through connected Fortinet Adapters, in addition to the 500+ other adapters, Axonius provides a de-duplicated, normalized, and correlated view into any asset, allowing security conditions, policies, and gaps to be continuously identified and enforced.

The Axonius Cybersecurity Asset Management Platform correlates asset data from existing solutions to provide an always up-to-date inventory, uncover gaps, and automate action—giving you the confidence to control complexity.

In summary, the Axonius platform:

- Connects with Fortinet and over 500 third-party IT and security tools via adapters
- Aggregates, de-duplicates, normalizes, and correlates asset data to deliver a truly accurate asset inventory
- Provides comprehensive visibility of all assets in your environment—whether on-premises or in the cloud
- Continuously surfaces security risks, vulnerabilities, and gaps
- Automates policy enforcement
- Measurably reduces the attack surface and mean time to detect and respond

### Joint Solution Benefits

- **Reduce Mean Time Inventory:** Axonius correlates data from all sources to provide a continuous, up-to-date inventory of all unique assets.
- **Discover Coverage Gaps and Surface Risk:** Understand when assets are missing critical security controls and when they have unsanctioned or vulnerable software.
- **Validate Policies and Automate Response:** Whenever assets deviate from policies or desired states, the Axonius Security Policy Enforcement Center is used to notify personnel, enrich data, or configure assets automatically.
- **Advanced Protection:** Gain unparalleled security protection provided by the Fortinet Security Fabric.

FORTINET FABRIC-READY

Fortinet FortiGate Next-Generation Firewalls deliver industry-leading enterprise security for any edge at any scale with full visibility and threat protection. Organizations can weave security deep into their hybrid IT architecture and build security-driven networks to achieve:

- Ultrafast security, end-to-end
- Consistent real-time defense with FortiGuard Services
- Optimized user experience with Fortinet's patented SP7 security processing units
- Operational efficiency and automated workflows

Fortinet FortiEDR delivers innovative endpoint security with real-time visibility, analysis, protection, and remediation. As proven in MITRE Evaluations, FortiEDR proactively shrinks the attack surface, prevents malware infection, detects and defuses potential threats in real time, and automates response and remediation procedures with customizable playbooks. FortiEDR identifies and stops breaches automatically and efficiently. And it does so without a slew of false alarms or disrupting business operations.

Fortinet FortiClient is a Fabric Agent that delivers protection, compliance, and secure access in a single, modular, lightweight client. A Fabric Agent is endpoint software that runs on an endpoint, such as a laptop or mobile device. It communicates with the Fortinet Security Fabric to provide information, visibility, and control to that device. It also enables secure, remote connectivity to the network.

Fortinet FortiPortal provides comprehensive security management and analytics within a multi-tenant, multi-tier management framework. This enables MSSPs to give their customers controlled access to configuration and analytics. Organizations can use FortiPortal to delegate a limited set of management and analytic capabilities to business units, departments, colleges, organizational units, etc.

## Solution Integration

The Axonius integrations with Fortinet FortiGate, FortiEDR, FortiClient, and FortiPortal fetch device and network data, helping customers understand the state of assets connected to their network. By delivering a complete asset inventory, Axonius allows organizations to unify assets with internal security controls, helping reduce their total attack surface. IT and security teams use Axonius to understand the entire state of their technology environment, identify missing security and IT software deployments, and reduce the attack surface through continuously identifying risky devices, users, and applications.

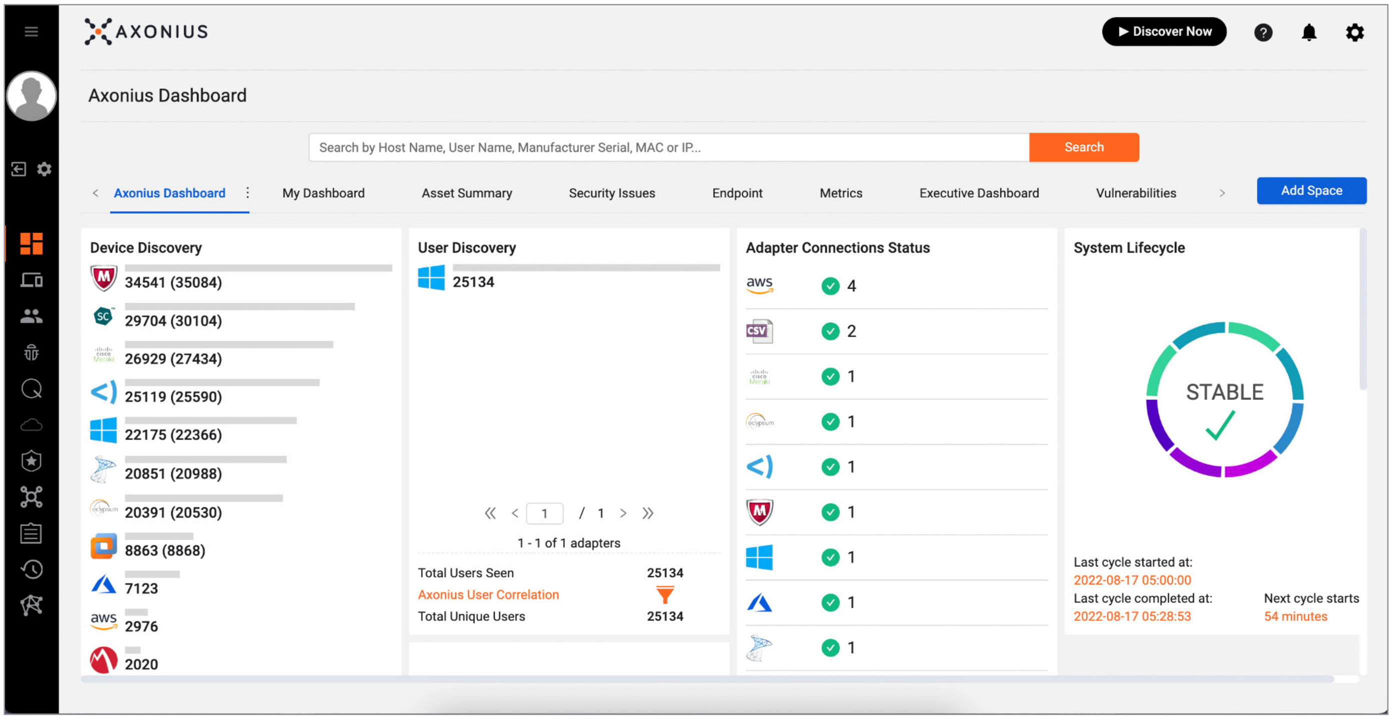
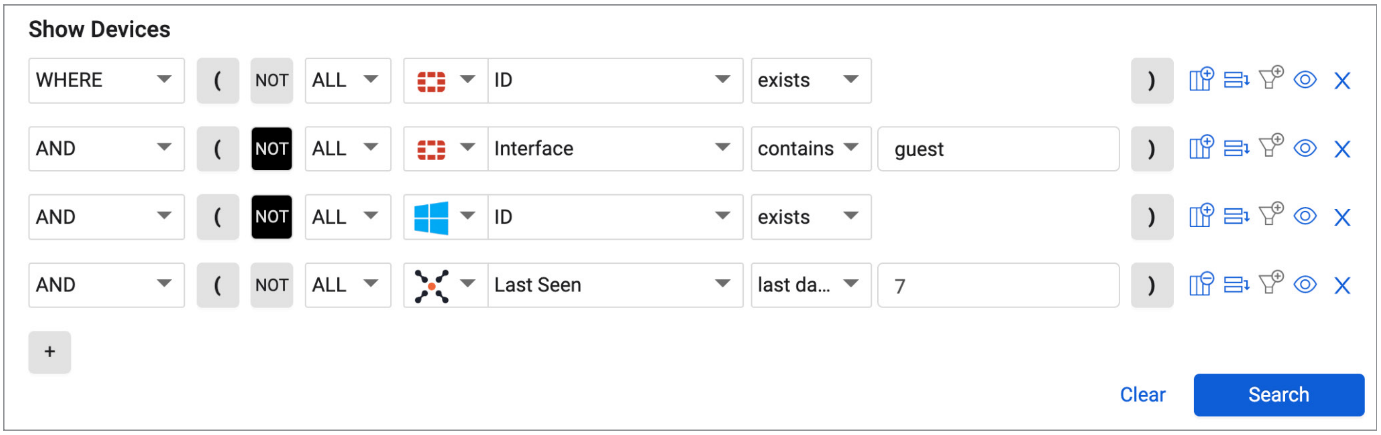


Figure 1: Axonius dashboard



Show Devices

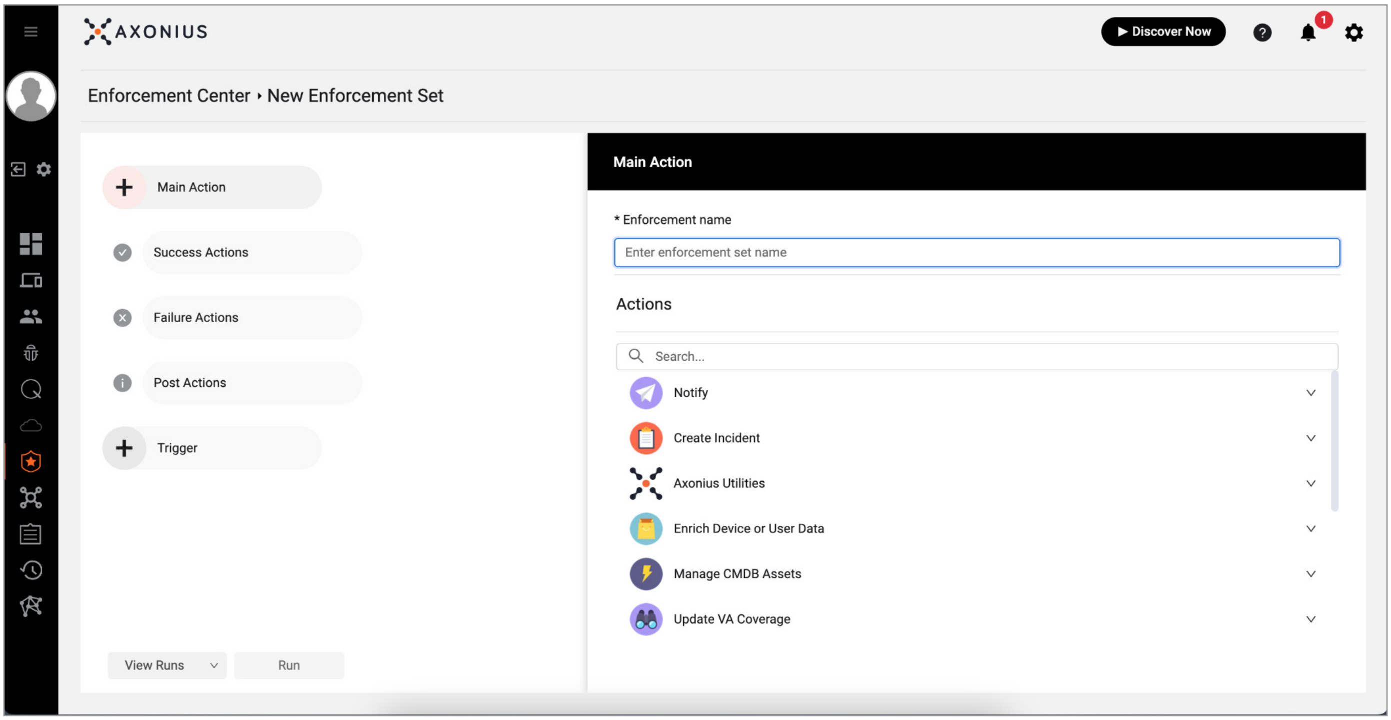
WHERE ( NOT ALL ID exists )

AND ( NOT ALL Interface contains guest )

AND ( NOT ALL ID exists )

AND ( NOT ALL Last Seen last da... 7 )

Figure 2: Axonius Query Wizard highlighting Fortinet connections



* Enforcement name: Enter enforcement set name

Figure 3: Axonius Enforcement Center

## Use Cases

### Use Case 1: Comprehensive Attack Surface Management

**The Challenge:** IT and security teams struggle to gain full visibility into all IT assets. An accurate understanding of all assets alongside an organization's security controls is needed to gain a true view of your attack surface.

**The Solution:** Connecting the Fortinet adapters in Axonius gives you visibility into external assets alongside other connected data sourced on the Axonius platform. This view delivers a full view of all your IT assets, making it easier to identify and mitigate potential security risks across your entire attack surface.

### Use Case 2: Security Control Validation

**The Challenge:** Security controls that are misconfigured increase the attack surface and leave organizations open to exploitation. Without a view into all company assets, IT and security teams struggle to deploy and configure security controls effectively.

**The Solution:** Connecting the Fortinet adapters in Axonius allows customers to identify external-facing assets with missing or misconfigured security controls, such as public-facing assets missing vulnerability scans, assets with default account credentials, or poorly configured network devices.

## About Axonius

Axonius gives customers the confidence to control complexity by mitigating threats, navigating risk, automating response actions, and informing business-level strategy. With solutions for both cyber asset attack surface management (CAASM) and SaaS management, Axonius is deployed in minutes and integrates with hundreds of data sources to provide a comprehensive asset inventory, uncover gaps, and automatically validate and enforce policies. Cited as one of the fastest-growing cybersecurity startups, with accolades from CNBC, Forbes, and Fortune, Axonius covers millions of assets, including devices and cloud assets, user accounts, and SaaS applications, for customers around the world.

September 2, 2022 12:14 AM
1740477-0-0-EN