algosec

Secure application connectivity.
Anywhere.



Horizon AppViz

Enforce security policies based on application needs

Modern businesses are powered by applications that serve customers, partners, and internal users alike. However, traditional network-based security models can't keep pace with the agility and complexity of today's hybrid infrastructures. Horizon AppViz addresses this challenge by decoupling application connectivity requirements from the underlying network infrastructure. This allows organizations to enforce security policies based on application needs, rather than being constrained by the complexity of network design.

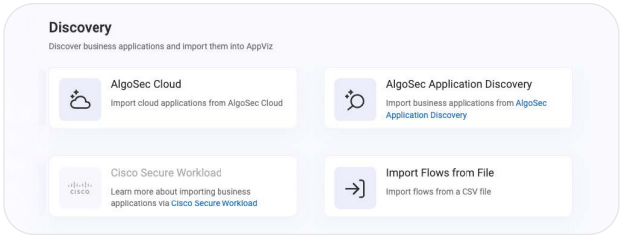
Horizon AppViz gives you the power to:

- Automatically discover and map application flows across on-premises data centers and multi-cloud environments.
- Gain real-time, end-to-end visibility into how applications connect, communicate, and are protected.
- Identify security gaps, blocked connections, and misconfigurations across complex infrastructure.
- Decouple application logic from network complexity, enabling scalable policy enforcement that aligns with business intent.

With a clear visual map of your environment, you can eliminate blind spots and make smarter, faster decisions.

Visualize and secure application flows across hybrid environments

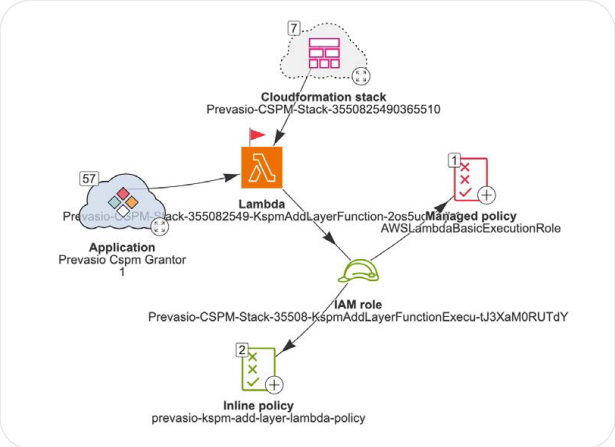
With thousands of risks across sprawling hybrid environments, knowing where to focus is critical. Horizon AppViz delivers unified visibility into application flows, dependencies, and connectivity issues—highlighting what's running, what it relies on, and how it communicates. By correlating this data with security controls and blocked connections, Horizon AppViz helps teams cut through noise, isolate true risk, and act with confidence.



Three layers of visibility for real risk clarity

Horizon AppViz delivers multi-dimensional visibility that goes beyond surface-level asset tracking. It helps security teams understand exactly what's running, what it depends on, and how it connects—so they can focus on risks that matter, not just alerts that surface.

- **Identify what's running:** Gain precise visibility into active applications across the environment—by name, role, and business function.
- **Understand what they rely on:** Map each application's resource dependencies across cloud and on-prem, from containers and VMs to storage and identity components.
- **See how they connect:** Visualize and analyze every network flow, security device, and policy rule involved—transforming fragmented data into a clear, per-application connectivity map.
- **Eliminate guesswork:** Horizon AppViz delivers a live architecture view that surfaces real risks and simplifies decision-making at every layer of application visibility.



With layered visibility into every application, flow, and dependency, Horizon AppViz gives you the clarity to cut through complexity and act with precision.

Prioritize risk mitigation based on business context

Horizon AppViz transforms vulnerability management by placing business applications at the center of risk analysis. Instead of overwhelming teams with fragmented data, it contextualizes vulnerabilities within the application landscape, highlighting which issues pose real threats to business operations. By integrating with leading scanners and AlgoSec solutions, Horizon AppViz unifies disparate risk sources into a clear, actionable map. With built-in tagging and prioritization, security teams can shift from chasing alerts to protecting what matters most—ensuring clarity, focus, and resilience across hybrid environments.

Not all risks are equal—Horizon AppViz ensures you're focused on the ones that matter most

- Maps security risks, vulnerabilities, and misconfigurations directly to business applications for meaningful, contextual insights.
- Identifies and categorizes critical apps, such as high-value or compliance-sensitive workloads.
- Implements a built-in risk scoring mechanism to prioritize remediation actions based on potential business impact.
- Helps teams focus limited resources on addressing high-severity risks that threaten mission-critical operations.

This enables smarter, faster decisions with business context baked into every security move.

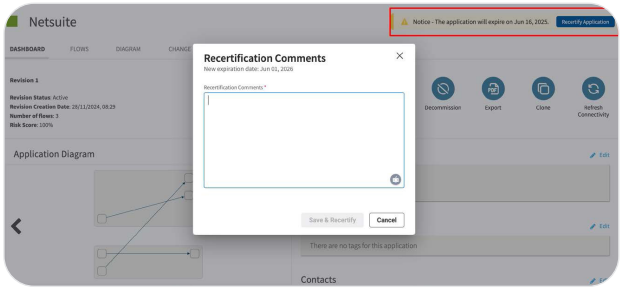
Ensure application-centric compliance

Evolving regulatory requirements make compliance management a continuous challenge. Automating audit preparation for frameworks such as PCI-DSS, NIST, and ISO simplifies compliance efforts. Realtime visibility into compliance status across hybrid environments helps organizations stay ahead of regulatory demands. Application recertification workflows ensure security teams can track compliance expiration dates without manual intervention, reducing audit preparation time by eliminating the need for rule-by-rule recertification. By adopting an application-centric approach, organizations can improve security, enhance compliance, and streamline network policy management across complex hybrid environments.

Compliance in hybrid environments

Maintaining compliance in hybrid environments requires more than manual audits and reactive checks. Horizon AppViz provides automated, application-aware compliance support that:

- Streamlines audit preparation for key standards like PCI-DSS, NIST, and ISO.
- Offers real-time visibility into compliance status across cloud and on-prem infrastructures.
- Enables automated application recertification workflows, ensuring that security teams never miss expiration dates or audit cycles.
- Eliminates manual rule-by-rule validation, significantly reducing audit prep time and effort.



By shifting to an application-centric model, Horizon AppViz simplifies governance and helps organizations stay continuously compliant at scale.

Application-centric change management

Manual change-management processes can be error-prone and inefficient. To streamline security policy updates, it is essential to analyze the impact of planned network changes before implementation. Automating security policy changes across firewalls, cloud security groups, SASE, SSE and SD-WAN platforms reduces errors and accelerates processes. Integrating security, DevOps, and IT teams into a collaborative workflow enhances efficiency, while proactively addressing security risks helps lower change-request rejection rates.

Horizon AppViz streamlines the entire workflow

Manual change-management processes are often time-consuming, error-prone, and siloed. Horizon AppViz streamlines the entire workflow by enabling security teams to:

- Simulate and assess the impact of proposed network changes before implementation, reducing risk and guesswork.
- Automate policy changes across firewalls, cloud security groups, SASE, SSE, and SD-WAN platforms, improving consistency and speed.
- Foster collaboration between Security, DevOps, and IT teams through a unified, application-centric workflow.
- Lower change-request rejection rates by proactively addressing policy misalignments and risks before they impact production.

This results in faster, safer deployments that align with business application needs while reducing operational burden.

algosec

© AlgoSec Inc. All rights reserved. AlgoSec and the AlgoSec logo are registered trademarks of AlgoSec Inc.
All other trademarks used herein are the property of their respective owners.