algosec

Secure application connectivity.
Anywhere.

Whitepaper

Your network is a maze. Time to create a path of awareness.

A guide to application-centric security and compliance management

Your network is a maze.
Time to create a path of awareness.

An AlgoSec Whitepaper

In today's fast-moving digital world, business applications are like vital energy centers—driving innovation, growth, and competitive momentum. But as organizations scale, their security practices must become more conscious and aligned. The convergence of cloud and data center environments calls for harmony, while the rapid pace of application deployment introduces complexity and noise.

Without a clear understanding of how business applications connect and flow within your network, maintaining security becomes a struggle.

This white paper explores a mindful approach to security — evolving toward an **application-centric awareness** in policy management. By anchoring security practices in the reality of business applications, rather than viewing them as isolated technical elements, organizations can bring clarity to their environment, improve posture, reduce operational burden, and create space for effortless compliance.

Key security challenges facing organizations

- **Fragmented visibility:** According to the *State of Network Security Report 2025*, "71% of security teams struggle with visibility, delaying threat detection and response as cloud adoption increases."
- **Maintaining security in a hybrid infrastructure:** With a mix of firewalls, cloud security groups, and segmentation technologies, businesses must enforce consistent security policies.
- **Zero Trust implementation:** Enterprises must implement a Zero Trust strategy within their organizations, but often fail due to a lack of visibility into what's running in their hybrid networks.
- **Complex change management:** The pace of network policy changes is increasing, leading to potential misconfigurations and security risks. Security teams experience inability to focus on the most critical vulnerabilities amid noise
- **Compliance and auditing:** Regulations such as PCI-DSS, SOX, and GDPR require organizations to document and justify security controls, making manual compliance efforts time-consuming and prone to errors. Poor planning and communication lead to misconfigurations and downtime

Transitioning with intention: The application-centric path

Organizations need a better way to manage security policies and connectivity while reducing complexity. This can be achieved through a structured approach focusing on four key areas:

See clearly: Visualizing application connectivity

Awareness starts with presence. To protect what matters, you must see what exists. By automatically discovering and mapping business applications, visualization enables security teams to gain a unified view of application flows across hybrid environments, including on-premises data centers and multi-cloud infrastructures. Application discovery helps identify endpoints and flow accurately, eliminating blind spots. Additionally, displaying blocked connections and security zones enables proactive investigation of connectivity issues.

Respond, don't react: Prioritize based on context

Security teams often face an overwhelming number of alerts, making it difficult to focus on the most pressing threats. By mapping network security risks, misconfigurations, and vulnerabilities to business applications, teams can assess risks in context. Categorizing critical applications, such as crown jewels or compliance-sensitive workloads, helps prioritize protection.

A risk scoring mechanism further refines this process, ensuring that the most critical risks are addressed effectively.

Better 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.

Stay aligned: 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. Real-time 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.

Understanding business applications and their connectivity

What is a business application?

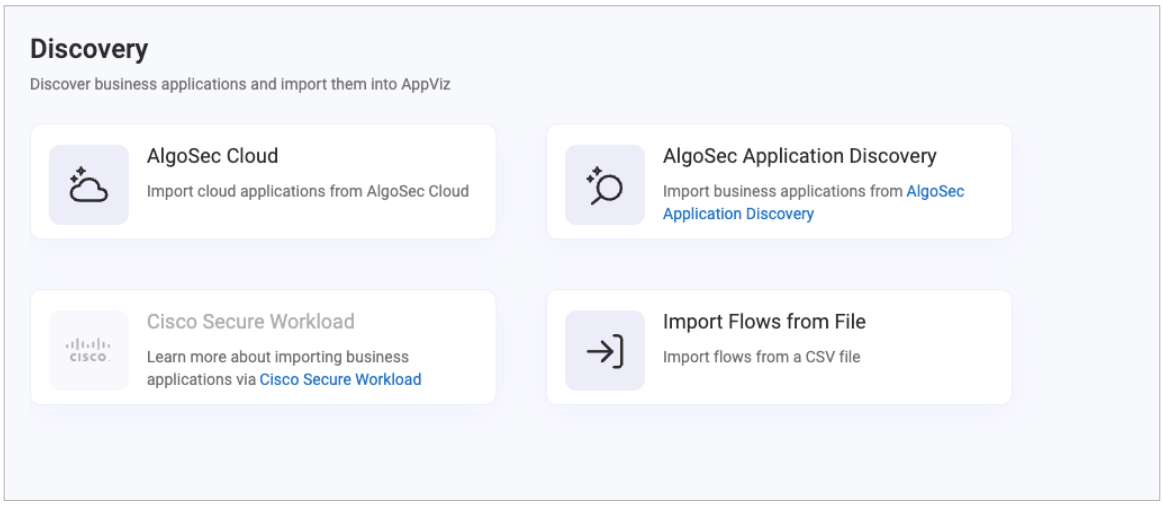
A business application is a software or set of computer programs designed to support and enhance various business functions within an organization. These applications are specifically developed to meet the needs of companies – automating processes, managing data, and facilitating decision-making. Consider a typical application, such as a customer account portal, which may interact with numerous other systems like SAP, Exchange, or mobile banking. Each application has specific connectivity requirements that must be understood and managed.

Unified awareness: Visibility that matters

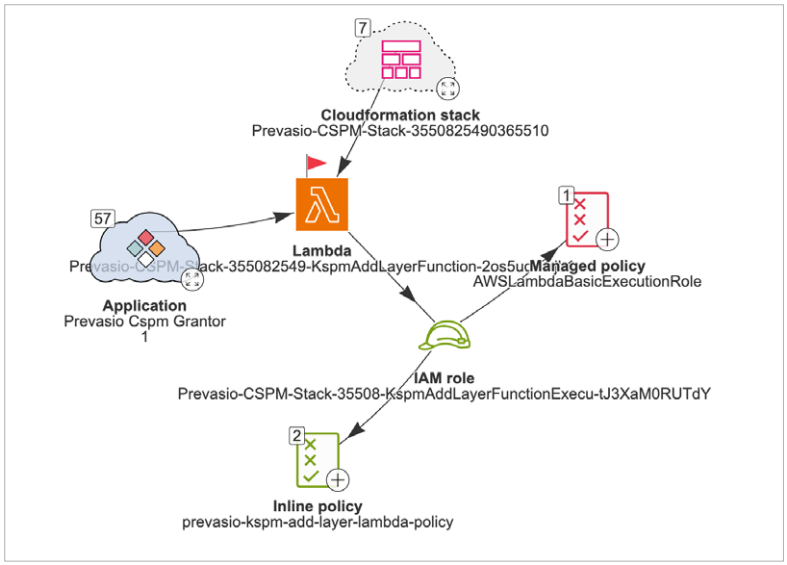
To enable you to understand application connectivity, AlgoSec provides a unified view of the entire application landscape across a hybrid environment, automatically mapping connectivity flows and dependencies across cloud and on-premises infrastructures and identifying business services. AppViz highlights blocked connections for compliance and empowers admins with its visual flows for quick issue investigation and decision-making, thus providing business owners, developers, and technology teams with a unified language to understand the applications' connectivity.

Three tiers of mindful application visibility

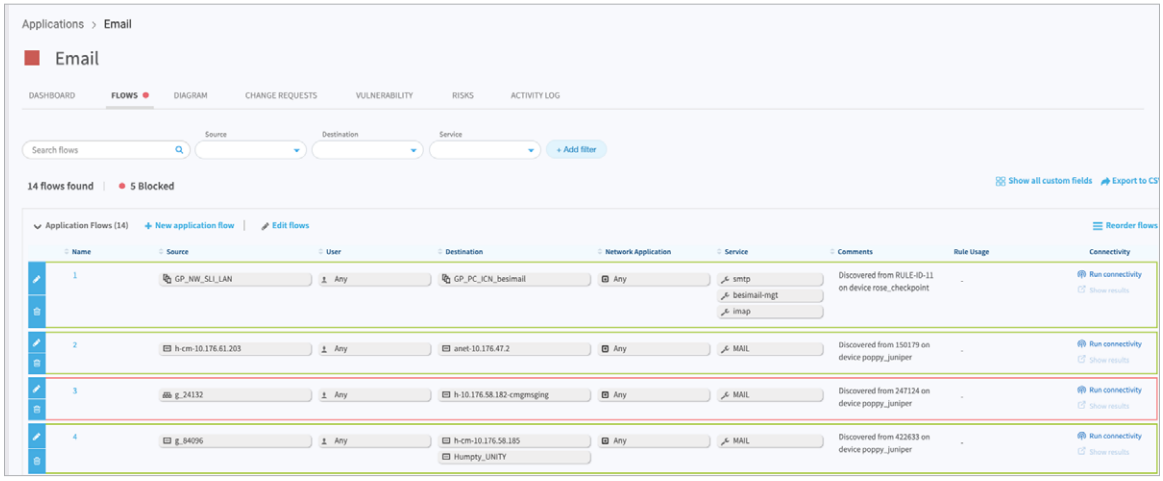
The highest level of visibility is identifying which applications are running on your network. AppViz provides various techniques to determine which applications are currently active. This identification includes not only detecting an application's presence but also pinpointing its specific name, offering clarity into what exactly is running in your environment.



The second level of visibility involves understanding the resources an application depends on to operate. In cloud environments, resource visibility is broad and includes insights into virtual machines, containers, serverless functions, storage, task lists, identity components, and more. In contrast, on-premises environments typically confine resources to the physical or virtual servers that host the application. This level of visibility gives all stakeholders a comprehensive understanding of the application's operational requirements.



The third level addresses the application's network and security requirements. To function, applications establish numerous network connections. With AppViz, we convert thin flows into thick flows, making connectivity information easier to manage on a per-application basis. We can monitor the status of each flow, identify security devices along the path, and drill down to the specific policy rules that govern connectivity. Additionally, AppViz visualizes application zones and traversal paths, delivering an always up-to-date architecture diagram out of the box.



Sources of insight: How AppViz discovers connectivity

AppViz employs multiple methods to discover business applications and their connectivity data, ensuring comprehensive visibility into your network's application landscape. Here's an overview of these methods:

AlgoSec Applications Discovery tool

AppViz's Application Discovery tool automatically detects business applications and their connectivity flows that are running across data centers, cloud providers, cloud provider regions, and multiple cloud accounts. This tool collects user traffic logs across your network and maps them to business services, enabling you to import these services as applications into AppViz.

AI-driven applications discovery

Leveraging artificial intelligence, AppViz enhances the applications discovery process by identifying and suggesting applications for onboarding. This AI-driven feature analyzes data, from change management ticketing system and comments made on rules, to recommend applications that may not have been manually identified, streamlining the discovery process.

Integration with micro-segmentation solutions

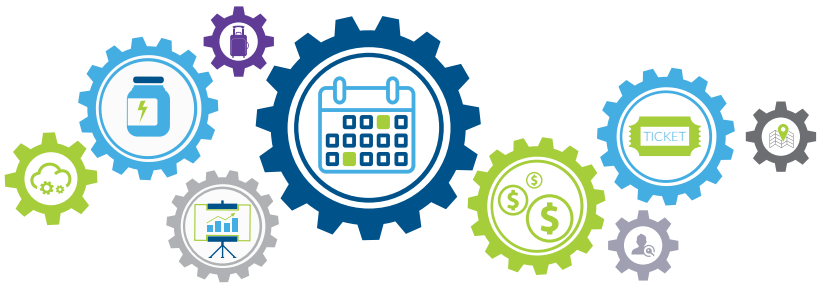
AppViz can connect to micro-segmentation solutions including Cisco Secure Workload (formerly Tetration), Illumio (PS API), and Guardicore to discover applications and their associated network flows. By integrating with these tools, AppViz imports flow data, providing insights into application dependencies and communication patterns.

Importing flows from CSV files

For environments where automated discovery tools may not capture all applications, AppViz allows the import of application flows from prepared CSV files. This method is particularly useful when the organization already has some level of documentation that can enrich AlgoSec findings.

AlgoSec Cloud

AppViz enables the import of cloud applications discovered by the AlgoSec Cloud Enterprise (ACE) Cloud App Analyzer.



Utilizing these diverse discovery methods, AppViz ensures a thorough and accurate mapping of business applications and their connectivity data, facilitating effective network security policy management.

Prioritizing risk mitigation with presence and purpose

AppViz shifts the focus from the maze of infrastructure to what's at the heart of the organization. AppViz doesn't just show vulnerabilities; it reveals them through a **business lens**, mapping them directly to the critical applications that underpin a company's operations.

The security team is dealing with endless lists of vulnerabilities. It's overwhelming, disjointed, and lacks clarity. But with AppViz, these vulnerabilities are no longer isolated points of concern. Instead, they are woven into the fabric of each business application, providing context that's essential for smart decision-making.

AppViz seamlessly integrates with all AlgoSec solutions, enabling the aggregation of risks stemming from compliance violations, network vulnerabilities, custom network zone violations, cloud asset and identity misconfigurations, cloud container misconfigurations, cloud asset vulnerabilities, and malware.

In addition, AppViz integrates seamlessly with leading vulnerability scanners: Qualys, Rapid7 Nexpose, Tenable Nessus gathering and correlating data from multiple sources. What once was a fragmented view transforms into a **comprehensive map**, where every vulnerability is tied to a specific application. No more guesswork, no more blind spots.

But AppViz doesn't stop there. It introduces **tags and categorization**, identifying crown jewels and high-priority applications that require immediate attention.

With this **application-first approach**, AppViz empowers organizations to prioritize risks effectively. It evaluates not just the severity of a vulnerability, but also its impact on business-critical assets. This means that security teams are no longer chasing every possible issue; they are focusing on the vulnerabilities that could disrupt the very core of the business.

As a result, AppViz transforms the way organizations manage risk. It brings clarity, efficiency, and precision to the complex world of hybrid network security, ensuring that what matters most, the applications that power the business, are always protected.

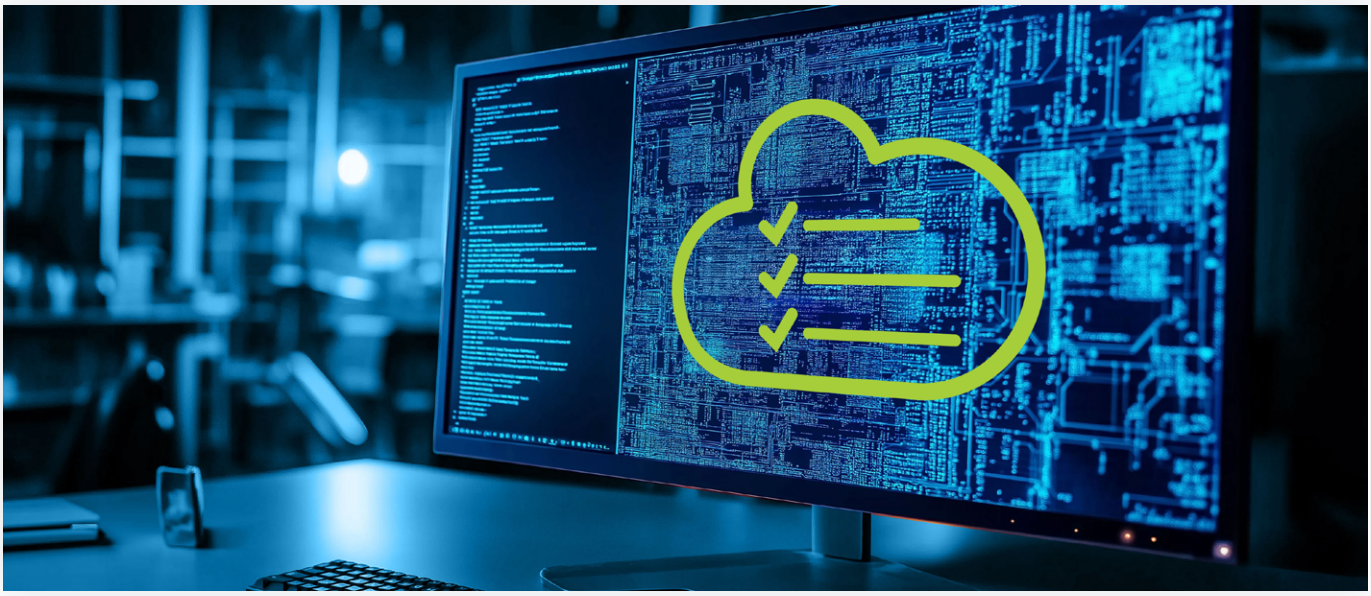
Staying in flow with application-centric compliance

Application recertification is a critical process that involves periodically reviewing and validating applications' connectivity needs. This process is essential for enhancing security by removing unnecessary or excessive connectivity, which reduces the risk of unauthorized access and potential security breaches. It also plays a key role in meeting compliance requirements by providing evidence during audits, as many regulatory standards mandate regular reviews of user access.

Recertification helps reduce risks by minimizing the attack surface and addressing insider threats or compromised accounts. It contributes to operational efficiency by streamlining policy management, which can improve system performance.

AppViz simplifies the application recertification process, making it easier to manage applications nearing or past their expiration dates. This approach offers several advantages over traditional rule recertification efforts required by regulatory standards:

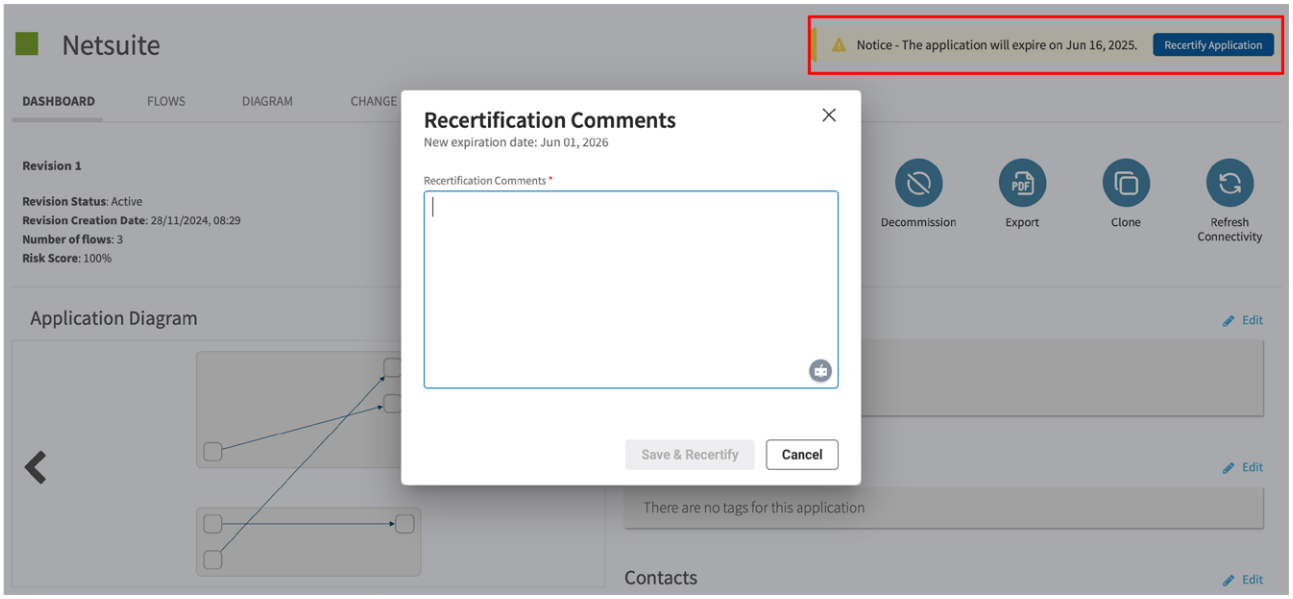
- **One-click recertification:** Users can initiate the recertification process by clicking the "Recertify Application" button directly from the notification.
- **Flexible expiration dates:** By default, the expiration date is set to 12 months after the recertification date, but users can modify this to a later date if needed.
- **Mandatory comments:** The system requires users to provide recertification comments, ensuring proper documentation of the process.
- **Instant confirmation:** Upon completion, a confirmation notification appears, and recertification details are immediately added to the application's Dashboard.



This streamlined process contrasts with traditional rule recertification efforts, which can be time-consuming and costly. By automating the recertification process, AppViz helps organizations:

- Reduce manual effort and associated costs
- Ensure timely recertification of applications
- Maintain compliance with regulatory standards
- Improve overall security posture by keeping application access up to date

This approach aligns with the growing trend of applying automation to rule recertification, which helps network administrators easily map business owners to rules and orchestrate the rule review process across the organization.



Approaching compliance with clarity and intention

AppViz enhances the completeness of audit reports for standards like PCI-DSS by providing comprehensive visibility into applications and vulnerabilities within the PCI zone. Here's how AppViz supports this process:

- **PCI zone configuration:** AppViz enables organizations to specify servers in the PCI zone, enabling more detailed security information for PCI applications.
- **Vulnerability mapping:** When integrated with ACE or external vulnerability scanners like Qualys, Rapid7 Nexpose, or Tenable Nessus, AppViz associates vulnerabilities directly with specific business applications in the PCI zone.
- **Application tagging:** AppViz automatically tags network objects and applications that intersect with the PCI zone, providing clear visibility into which systems are subject to PCI-DSS requirements.
- **Vulnerability threshold setting:** Users can set a vulnerability level threshold in AppViz, determining which applications are considered vulnerable in PCI reports based on their security scores.
- **Comprehensive reporting:** AppViz contributes to the detailed assessment results required in PCI Reports on Compliance (ROC), including information about the reviewed environment, vulnerability scans, and specific security controls.
- **Continuous monitoring:** AppViz supports real-time monitoring of the PCI environment, helping organizations maintain ongoing compliance and detect potential security threats promptly.

By providing these features, AppViz significantly enhances the completeness and accuracy of PCI-DSS audit reports, ensuring that organizations can demonstrate comprehensive compliance across their application landscape and PCI zone.

Navigating change management without disruption

Security and IT teams typically lack full application connectivity visibility, resulting in poor planning, misconfigurations, downtime, communication gaps, and error-prone manual processes.

Understanding the connectivity of business applications is crucial for handling connectivity change requests effectively. Firewall rules, cloud SGs/NSGs, and SDN policies control the flow of network traffic, and any changes to these rules must be carefully managed to maintain security and ensure that business applications function as intended.

AppViz improves the handling of connectivity change requests in the following ways:

Risk assessment

- Knowing how different applications within the business interact helps in assessing the potential impact of firewall, cloud security group, and Software-Defined Networking (SDN) technology policy changes proactively.
- Understanding the criticality of each application allows for more informed risk assessment before making changes to the policy configuration.

Minimizing impact on operations

Awareness of application dependencies helps in minimizing the impact on operations when making firewall changes. One of the most important data points in assessing the operational risk of a connectivity change, is the business applications affected.

When a vulnerability is being researched, AppViz allows searching for the specific CVE and discovering all impacted applications and their relevant building blocks. Providing business context to a vulnerability being mitigated enables focusing on the most critical business services and speeding remediation.

Change planning

Comprehensive knowledge of application connectivity enables:

- Better planning of firewall changes.
- Scheduling changes during low-traffic periods or implementing fallback mechanisms if unexpected issues arise.

Documentation and communication

- Clear documentation of application connectivity is essential for effective communication between IT teams, security teams, and other stakeholders.
- Documentation helps prevent misunderstandings and ensures that all parties involved in the change process have a shared understanding of the implications.

From chaos to clarity

As organizations navigate the complexities of hybrid environments, securing business applications effectively requires a shift from traditional network-based security to an application-centric approach. By mapping application connectivity, prioritizing risks based on business impact, automating change management, and ensuring compliance, organizations can enhance their security posture while reducing operational overhead. AppViz enables application-centric visibility across hybrid environments, leveraging AI-driven discovery and automated risk assessment to streamline secure change.

Experience AppViz in action

Let go of blind spots. See your network clearly.

Request a live demo and experience how **intentional, mindful security** through AppViz can transform your organization's approach to risk, compliance, and connectivity.

Schedule a demo

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to secure application connectivity by automating connectivity flows and security policy, anywhere.

The AlgoSec platform enables the world's most complex organizations to gain visibility, reduce risk, achieve compliance at the application-level and process changes at zero-touch across the hybrid network.

Over 1,800 of the world's leading organizations trust AlgoSec to help secure their most critical workloads across public cloud, private cloud, containers, and on-premises networks.

algosec

AlgoSec.com