algosec

Horizon AppViz

Automation & AI: What our customers think

AlgoSec report - 2026



Table of content

Executive summary 3

The rise of Application-Centric Security 4

Advancing Security Through Automation 6

Smarter Application Discovery with AI 8

Conclusion 10

Methodology 10

About Horizon Appviz 10

About AlgoSec 11

Executive summary

Modern enterprise networks are barely recognizable from a decade ago. Applications now span on-premises infrastructure, multiple cloud environments, containers, SaaS platforms, and third-party services, creating connectivity patterns that are far more dynamic than traditional network architectures were ever designed to support. At the same time, security teams are under growing pressure to manage this complexity while enabling the speed and agility the business expects. Gartner identifies generative AI, digital decentralization, supply chain interdependencies, and persistent cybersecurity talent shortages as four of the defining trends shaping security strategies in 2025[1], highlighting just how rapidly operational demands are changing.

To better understand how organizations are responding, AlgoSec surveyed more than 100 Horizon AppViz customers about application visibility, automation, and AI. The findings reveal three clear themes.

First, application visibility has become a shared operational capability that supports security, networking, cloud, and DevOps teams alike. Customers identified application connectivity mapping, self-service firewall requests, and application-centric change management among the most valuable use cases, highlighting the growing importance of understanding application context across increasingly complex environments.

Second, automation has become firmly established within security operations, with most organizations already automating key activities such as firewall rule implementation, compliance reporting, and risk analysis. At the same time, many organizations continue to rely on manual processes when onboarding and discovering applications, suggesting there remains significant scope to extend automation into application lifecycle management.

Finally, customers see AI as an opportunity to strengthen existing workflows rather than replace them. Respondents expressed the strongest interest in capabilities that improve application understanding, integrate with existing enterprise tools, and provide intelligent recommendations, demonstrating that successful AI depends on accurate application context as much as advanced models.

Naturally, this is redefining the role of network security. Visibility into applications, their dependencies, and the policies that govern them is becoming increasingly important, providing the context needed to automate routine processes, simplify change management, and make more informed security decisions. Gartner predicts that by the end of 2026, 40% of enterprise applications will include task-specific AI agents, up from fewer than 5% in 2025[2], while identifying AI-ready data as one of the most important foundations for successful AI adoption. Together, these trends point towards a future where understanding application context becomes just as important as managing the infrastructure itself. This report reflects the experiences of organizations already navigating these challenges in practice, offering insight into the priorities, opportunities, and obstacles shaping the next generation of application-aware security.



[1] Gartner Identifies the Top Cybersecurity Trends for 2025 (Source)
[2] Gartner Predicts 40% of Enterprise Apps Will Feature Task-Specific AI Agents by 2026, Up from Less Than 5% in 2025 (Source)

The rise of Application-Centric Security

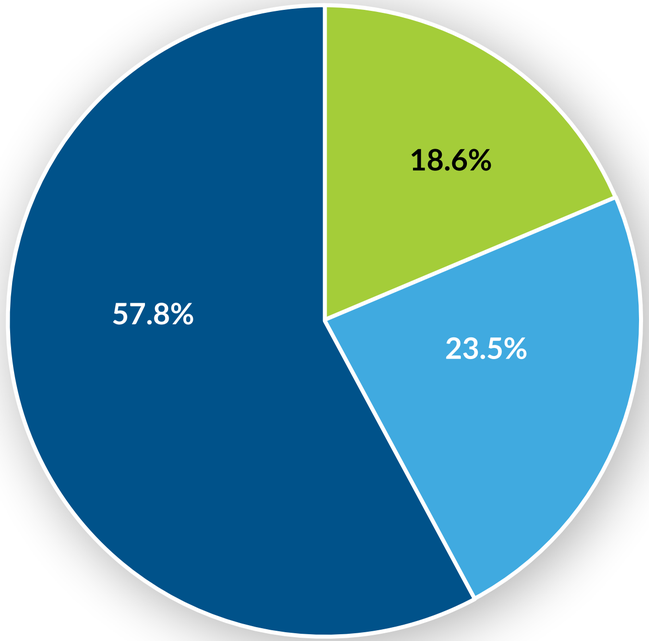
Security teams are expected to make rapid, well-informed decisions about connectivity, policy changes, compliance, and risk, yet many are still working without a complete picture of how business applications communicate or what dependencies exist between them. Every firewall change, access request, cloud migration, and segmentation initiative ultimately exists to support an application, making that application context an increasingly valuable source of operational insight.

By understanding how applications communicate, who owns them, and which policies support them, application-centric security offers a clearer picture of how any changes will affect the wider environment. This leads to greater confidence in day-to-day decision making, fewer unexpected consequences during change processes, and a stronger foundation for security initiatives that depend on accurate visibility across increasingly connected environments.

Visibility that supports the whole organization

Horizon Appviz has been developed to help organizations build that understanding by mapping application connectivity and making complex relationships easier to visualize. Our survey findings suggest this capability is delivering value across a broad cross-section of technology teams. Almost two-thirds (61.8%) of respondents said Horizon Appviz is primarily used by Network and Security Operations, while application owners and DevOps teams were identified by 31.4% of respondents. Cloud infrastructure teams (25.5%) and application security professionals (22.5%) also featured prominently, reflecting how application visibility has become a shared operational capability that supports collaboration across multiple disciplines rather than remaining the responsibility of a single function.

Are you using AlgoSec AppViz for application connectivity mapping and management?



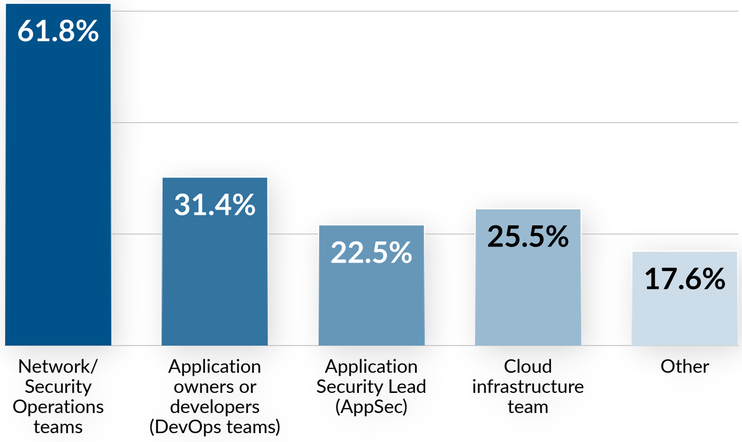
- **18.6%** Yes - currently using AppViz in production
- **23.5%** Not yet - but planning to deploy AppViz within the next 12 months
- **57.8%** No - not using AppViz

Customers are also applying Horizon AppViz in a variety of ways as they strengthen application-centric security practices. Visualizing application connectivity emerged as the most common use case, selected by 45.1% of respondents, underlining the importance of understanding how business services communicate before changes are made. Self-service firewall requests followed at 38.2%, demonstrating the growing demand for faster, more efficient workflows, while application recertification (31.4%) and application-centric change management (28.4%) highlight the need for greater visibility throughout the application lifecycle. Customers also identified Zero Trust initiatives (21.6%) and cloud migration planning (17.6%) as important areas where a clearer understanding of application dependencies helps reduce complexity and support more informed decision making.

As modern environments continue to grow in scale and complexity, understanding applications is becoming an increasingly important part of effective security operations. The experiences shared by AlgoSec customers demonstrate that application visibility is already helping organizations strengthen collaboration, improve operational confidence, and provide the context needed to support the next generation of automation and AI-driven security capabilities.

> ***"Search engine of objects in AppViz is very responsive, as well as search in Firewall Analyzer to find flows"***
>
> ★ ★ ★ ★ ★
>
> *Tommy L.*
> *(> 1000 emp.)*
>
> TL

Which teams or stakeholders in your organization use (or will use) AppViz?



- **61.8%** Network/Security Operations teams
- **31.4%** Application owners or developers (DevOps teams)
- **22.5%** Application Security Lead (AppSec)
- **25.5%** Cloud infrastructure team
- **17.6%** Other

experian
AT&T
gm
Chevron
LOWE'S
IBM
AMERICAN EXPRESS
Dominion Energy
NCR
sanofi

Advancing Security Through Automation

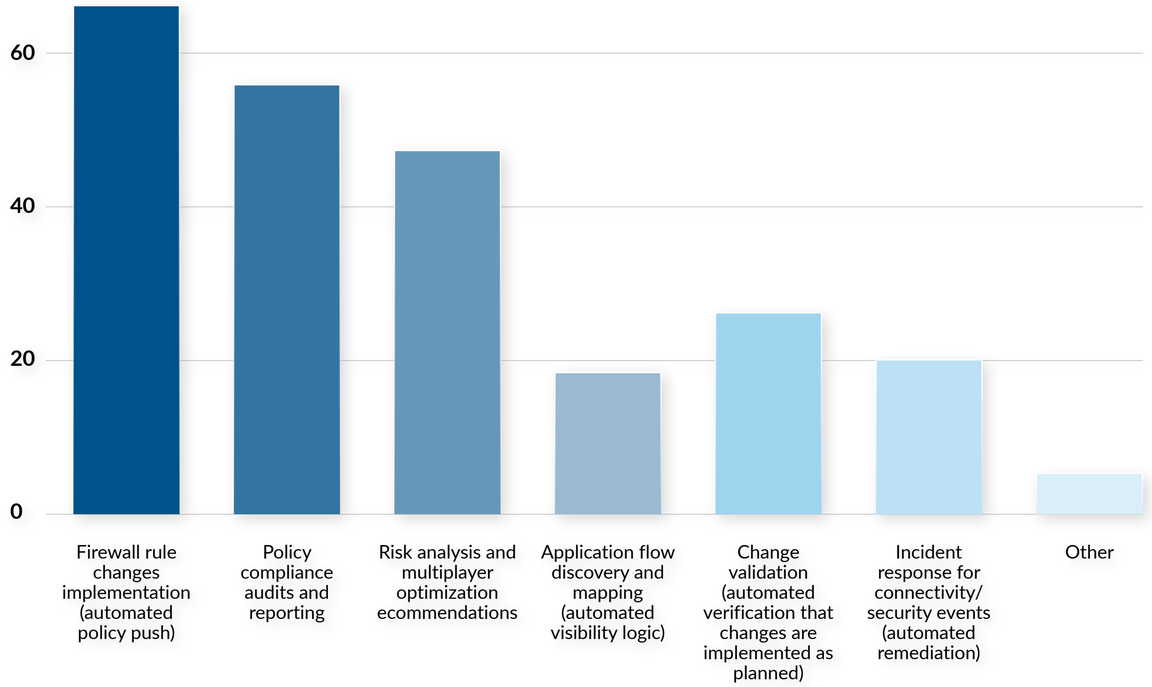
As network footprints continue to expand, organizations are increasingly looking for opportunities to automate, so teams can spend less time on repetitive administrative tasks and more time making informed decisions about risk, policy, and change.

The survey findings suggest that many organizations have already embarked on this journey. More than half of respondents described their security operations as either highly automated (13.4%) or moderately automated (43.3%), while 35.1% said automation remains relatively limited and 8.2% reported having no automation in place at all. This tells us that automation is becoming increasingly common across security operations, while also highlighting significant opportunities for organizations to extend its reach.

Building on strong foundations

When asked where automation delivers the greatest value, customers pointed first to firewall rule implementation, chosen by 66% of respondents. Compliance reporting followed at 54.6%, with risk analysis identified by 43.3%. Customers also highlighted change validation (34%) and incident response (27.8%) as important areas where automation helps improve operational efficiency and consistency. This suggests that organizations are focusing their automation efforts on processes that are both repetitive and operationally critical, enabling security teams to work more efficiently while maintaining confidence in policy decisions.

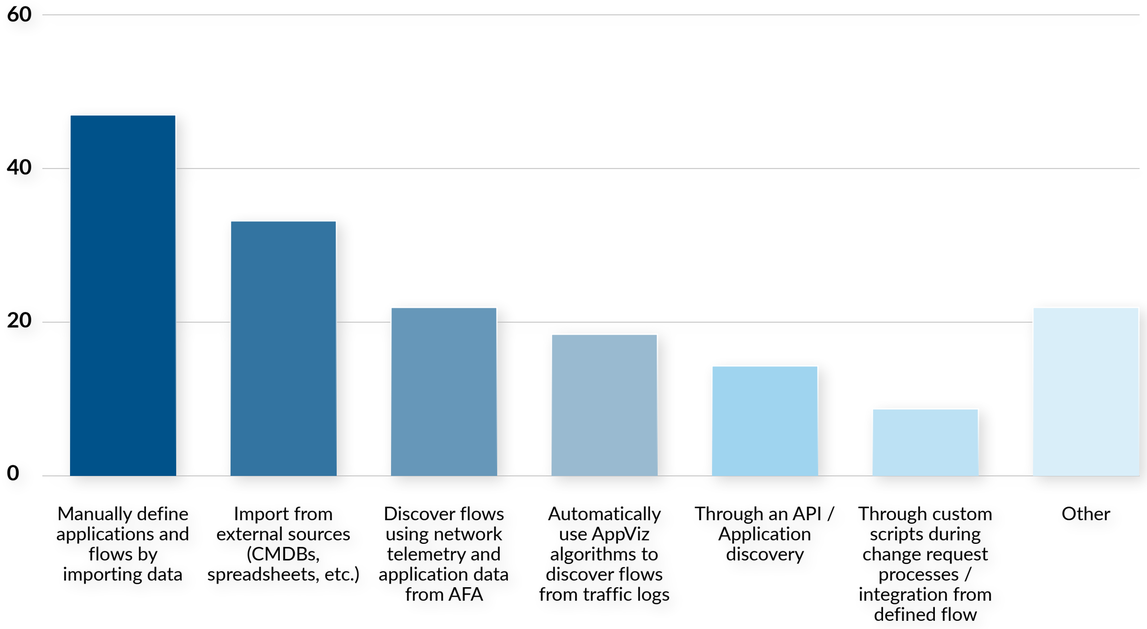
Security Processes Automation:
Which network/security operations have you automated or plan to automate?



The survey also reveals where other opportunities can be found. Nearly half of respondents (46.8%) said applications are still defined manually during onboarding, while 31.9% continue to rely on spreadsheet imports. By comparison, only 19.1% currently use automated application discovery. This gap highlights one of the next stages in security automation - extending automation beyond policy execution to improve how organizations discover, understand, and manage the applications those policies are designed to protect. Greater application visibility provides the context needed to make these processes faster, more accurate, and easier to scale as environments continue to evolve.

All told, these findings suggest that automation is no longer confined to isolated operational tasks, but is becoming an increasingly connected capability that depends on accurate, up-to-date application context. As organizations continue expanding their automation strategies, a clearer understanding of application relationships will play an important role in supporting more efficient workflows, reducing manual effort, and enabling security teams to operate with greater confidence.

Application Onboarding Method:
How do you populate or onboard applications into AppViz?



Bell nab FAB First Abu Dhabi Bank Hewlett Packard Enterprise bradesco bbi YES BANK Morgan Stanley United Nations Schneider Electric orange

"I like using AppViz. It's great for viewing the applications and better understanding the network rules behind them."

★ ★ ★ ★ ★

Fatima O.
(> 1000 emp.)

FQ

Smarter Application Discovery with AI

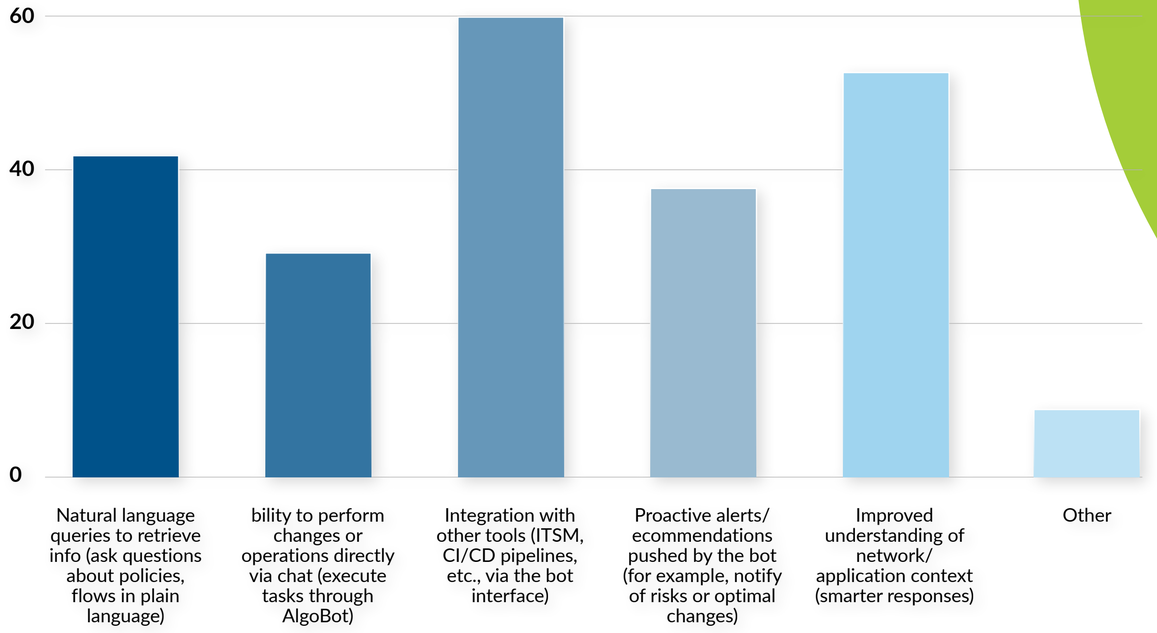
Application visibility is now an essential part of modern security operations, but building and maintaining that visibility can still require significant time and effort. As environments continue to expand, manually identifying application dependencies, understanding connectivity, and keeping information up to date is now a priority for security teams. AI offers an opportunity to simplify these processes by helping security teams discover, interpret, and act on application information more quickly, while reducing the operational burden of maintaining accurate application inventories.

The survey explored customer expectations for Algo, AlgoSec's AI-powered assistant designed to help users retrieve information, answer operational questions, surface recommendations, and interact with Horizon using natural language. Rather than asking whether AI has a role to play, the responses focused on how these capabilities can become more useful within everyday security operations. When asked which capabilities would make Algo more useful, integration with other enterprise tools emerged as the highest priority, selected by 60.2% of respondents. More than half (52.3%) also highlighted improved understanding of network and application context, reinforcing the importance of providing AI with accurate operational information. Customers also expressed strong interest in natural language queries (42.0%) and proactive alerts or recommendations (38.6%), while 29.5% saw value in performing operational tasks directly through conversational interfaces. It is safe to assume that organizations are looking for AI that fits naturally into established workflows while also helping teams work more efficiently and make better-informed decisions.

Building confidence in AI

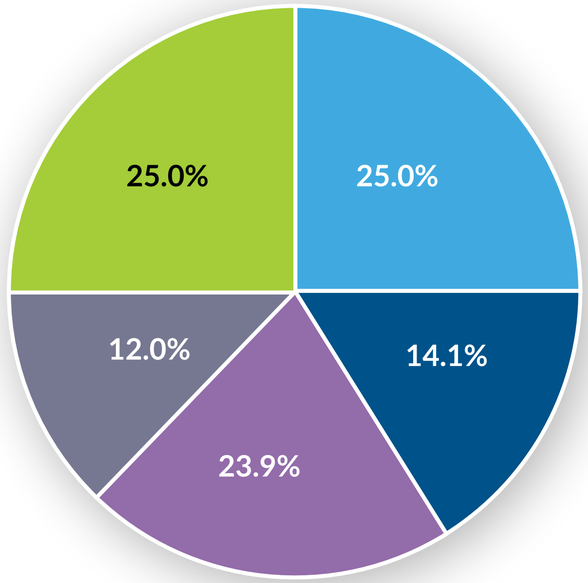
The survey also explored attitudes towards emerging AI capabilities. Around a quarter of respondents (25.0%) said they would be very interested in learning more about Model Context Protocol (MCP), while a further 23.9% said they would consider it provided security policy implications were clearly defined. Another 14.1% supported the concept with security team involvement. At the same time, 12.0% preferred traditional APIs and 25.0% indicated they were not interested. These findings reflect a measured approach to AI adoption, with customers demonstrating enthusiasm for new capabilities while continuing to place a strong emphasis on governance, security, and operational oversight.

Which capabilities would make AlgoBot more useful for you?



That measured confidence is also reflected in attitudes towards AI-driven recommendations for policy changes and risk analysis. Responses were weighted towards the positive end of the scale, suggesting customers are increasingly comfortable using AI to support decision making when it complements existing expertise and provides meaningful operational context. Rather than viewing AI as a replacement for experienced security professionals, respondents see its greatest value in accelerating application discovery, surfacing relevant information, and helping teams make faster, more informed decisions across increasingly complex environments.

MCP (Model Context Protocol) is an AI based open standard that provides a way for AI applications to integrate with various data sources and tools and extends the ability to consume system information. AlgoSec is considering to utilizing MCP in order to extend its ability to access system data. Would you be interested to hear more?



- **25.0%** Yes, very interested
- **14.1%** Yes, but needs security teams involvement
- **23.9%** We might consider assuming security policy aspects are well-defined
- **12.0%** I prefer using traditional APIs
- **25.0%** No, thanks

> ***"Key part of our network security reporting and compliance environment. shows all area where out network might be exposed"***
>
> ★ ★ ★ ★ ★
>
> *Derk D.*
> *(> 1000 emp.)*
>
> DD



Conclusion

Building the foundation for the next generation of security operations

The findings throughout this report point toward organizations placing greater emphasis on understanding the applications that power their business, using automation to simplify routine operations, and exploring how AI can help security teams work more efficiently. While each of these trends is significant in its own right, the survey suggests they are increasingly connected. Accurate application visibility provides the context that enables more informed decisions, more effective automation, and more meaningful AI-driven insights, helping organizations manage growing complexity with greater confidence.

This transition is already underway, with Horizon Appviz helping organizations bring application context to the center of their security operations. By visualizing application connectivity, supporting application-centric change management, strengthening automation workflows, and enhancing application discovery through AI, Horizon Appviz provides the visibility needed to simplify increasingly complex environments. Rather than addressing these challenges individually, it brings them together within a single operational view, enabling security teams to work faster, make better-informed decisions, and adapt with confidence as their environments continue to evolve.

Methodology

This report is based on responses from 102 AlgoSec customers and explores how organizations are approaching application visibility, automation, and AI across modern network security operations. The survey examined current operational practices, adoption priorities, and emerging technologies, providing a customer-led perspective on the opportunities and challenges shaping application-centric security. The findings presented throughout this report have been supplemented with independent industry research to place customer experiences within the broader context of evolving security and technology trends.

About Horizon Appviz

Horizon Appviz is AlgoSec's AI-powered application discovery, visualization, and security solution, designed to help organizations understand how business applications communicate across today's increasingly complex hybrid environments. Embedded within the Horizon platform, it automatically discovers application connectivity, visualizes dependencies, and provides the operational context security teams need to make faster, more informed decisions.

By bringing application context into everyday security operations, Horizon Appviz helps organizations simplify change management, strengthen governance, and reduce the manual effort traditionally associated with maintaining accurate application inventories. AI-powered discovery accelerates application onboarding, while application-centric visibility enables teams to better understand the potential impact of policy changes, prioritize risk, and support initiatives such as Zero Trust and cloud transformation.

Together, these capabilities provide a unified view of applications, connectivity, and security policy, enabling organizations to move beyond infrastructure-centric management towards a more application-aware approach to network security. As the findings throughout this report demonstrate, application visibility is becoming an increasingly important foundation for automation, AI, and the next generation of security operations. Horizon Appviz has been developed to help organizations build that foundation with greater speed, accuracy, and confidence.



About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to securely accelerate application delivery up to 10 times faster by automating application connectivity and security policy across the hybrid network environment.

With two decades of expertise securing hybrid networks, over 2200 of the world's most complex organizations trust AlgoSec to help secure their most critical workloads.

AlgoSec Horizon platform utilizes advanced AI capabilities, enabling users to automatically discover and identify their business applications across multi-clouds, and remediate risks more effectively. It serves as a single source for visibility into security and compliance issues across the hybrid network environment, to ensure ongoing adherence to internet security standards, industry, and internal regulations.

Additionally, organizations can leverage intelligent change automation to streamline security change processes, thus improving security and agility.

Learn how AlgoSec enables application owners, information security experts, SecOps and cloud security teams to deploy business applications faster while maintaining security at www.algosec.com.

algosec

For more information, visit www.AlgoSec.com

