algosec

Secure application connectivity.
Anywhere.



Whitepaper

The business case for Horizon AlgoSec

Transitioning from fragmented tools to a unified platform for secure application connectivity

A customer-centric white paper for enterprise security leaders, cloud and network operations teams, risk and compliance stakeholders, existing customers, and channel partners.

Executive summary

From reactive firefighting to secure application connectivity

Enterprises are no longer managing simple north-south firewall changes. They are governing application connectivity across public cloud, private cloud, SDN, data centers, remote access, and third-party ecosystems. The operating model has changed faster than many policy-management processes have evolved.

For many organizations, the security team already owns a large portfolio of enforcement points and consoles. The pain is not a lack of tools. The pain is that those tools often do not share the same application context, risk context, workflow history, and audit evidence. When a customer-facing application is disrupted or a new service must launch quickly, teams still fall back into war rooms, spreadsheets, manual approvals, and rule-by-rule analysis.

AlgoSec Horizon gives customers and partners a platform-first narrative: secure application connectivity across hybrid environments by bringing visibility, risk analysis, policy-change automation, object governance, cloud controls, and compliance evidence into a unified operating model.



Six enterprise takeaways

Takeaway	Customer outcome
Hybrid is here to stay	Applications and workloads span data centers, public cloud, private cloud, and SDN. Policy governance must follow the application, not the location.
Visibility must become application-centric	Security teams need to understand what business service a rule supports, who owns it, and what risk it introduces.
Manual change is the weak link	Manual approvals, handoffs, and implementation steps slow delivery and raise the chance of rework or misconfiguration.
Compliance is continuous	Auditors and regulators increasingly expect evidence that controls are accurate, traceable, and maintained over time.
Automation must be risk-aware	Enterprises should automate the changes that can be validated safely, while preserving governance for high-risk exceptions.
Partners can lead with services	Assessments, cleanup, integration, application mapping, migration support, and managed governance create repeatable partner value.

From fragmented policy operations to a unified connectivity platform

Use in customer discovery: map the tools, workflows, evidence sources, and application owners involved in one high-value change.



Figure 1. The enterprise shift from fragmented tool operations to a unified application-connectivity platform.

Market context

Why the Horizon conversation is timely

Hybrid and multi-cloud security has entered a consolidation phase. Cloud adoption continues to grow, but data centers have not disappeared. Flexera reported in its 2025 State of the Cloud coverage that more than half of workloads are already in public cloud, while workload repatriation also continues. The practical implication for enterprise teams is that both cloud expansion and data centers must be governed together. [1]

At the same time, cloud security teams are under pressure to consolidate and integrate. Palo Alto Networks reported in its 2025 State of Cloud Security research that 97% of organizations prioritize consolidating their cloud security footprint and 89% say cloud and application security must be fully integrated with the SOC. [2]

Regulatory pressure is also rising. DORA has applied in the EU financial sector since January 17, 2025, with a focus on digital operational resilience and the ability to withstand, respond to, and recover from ICT disruptions. [3] NIS2 establishes a unified cybersecurity framework across 18 critical sectors in the EU and introduces risk-management and reporting expectations for medium-sized and large entities in scope. [4]

The financial stakes are high. IBM reported the global average cost of a data breach at USD 4.4 million in its 2025 Cost of a Data Breach Report, and linked year-over-year improvement to faster identification and containment. [5] While security policy automation does not eliminate breach risk, it can help enterprises reduce preventable exposure, validate changes before they reach production, and shorten the path to root cause when connectivity or policy issues occur.

Enterprise implication

Market pressure	Why it matters to Horizon conversations	Executive question
Cloud and data center coexistence	Teams need consistent application-connectivity governance across enforcement points, not another siloed console.	Can we answer which policies support our most critical applications across all environments?
Security-tool consolidation	Buyers increasingly want platforms that reduce handoffs, duplicate data, and context gaps.	Which tools overlap today, and which workflows would improve if data and approvals were unified?
SOC and cloud integration	Cloud findings, connectivity risks, and change evidence must reach operations teams in usable context.	Can operations connect a cloud risk to the business application it affects?
Regulatory resilience	Policy change, compliance status, and remediation evidence need to be traceable and repeatable.	How quickly can we prove that a control is enforced and that a risky change was reviewed?
Cost and outage exposure	Policy errors can consume engineering time, delay launches, and create customer-visible impact.	What is the annual cost of rework, war rooms, emergency changes, and audit preparation?

I. Introduction

The high cost of fragmented visibility

Before shifting to a unified platform, many enterprise teams operate in a state of reactive firefighting. Network, cloud, security, compliance, and application teams each have valid data, but the data does not always tell the same story. That is where delays, rework, risk, and audit friction begin.

Consider a composite enterprise scenario: a security team manages more than 800 workloads across public cloud, private cloud, SDN, and data center environments. When a customer-facing application goes down, the network, cloud, security, and application teams enter a multi-hour war room. Each team looks at a different console. One team can see a rule. Another can see a route. Another sees a cloud security group. Another sees the application owner. No single view explains the business service, the connectivity path, the policy intent, the change history, and the risk impact together.

In that environment, even a standard policy change can take days. Manual change processes require back-and-forth clarification, security review, implementation, validation, documentation, and evidence collection. Audit preparation becomes a separate project because teams must reconstruct what changed, who approved it, why it was allowed, and whether it still supports a valid business application.

The problem: tool sprawl is now an operational and financial burden

Pain area	How it appears in enterprise operations	Business impact
Operational friction	Teams manually reconcile data between firewalls, cloud controls, SDN platforms, CMDBs, ticketing systems, and spreadsheets.	Staff capacity is consumed by coordination instead of risk reduction or application enablement.
Visibility blind spots	Disconnected tools make it difficult to identify which policies support which applications, owners, and dependencies.	Changes are approved with incomplete context, raising the risk of outage, over-permission, or audit exception.
Change bottlenecks	Manual design, risk review, approval, implementation, and validation steps slow routine requests.	Application delivery slows, change windows close, and teams rely on emergency workarounds.
Audit scramble	Evidence is assembled after the fact from multiple systems and owners.	Audit preparation becomes labor-intensive and confidence in completeness declines.
Cloud drift	Cloud-native controls evolve quickly and may not follow the same governance process as data center controls.	Policy inconsistency grows across environments, especially during migration or rapid deployment.
Object sprawl	Duplicate, unused, misaligned, or unattached objects accumulate across firewalls and SDN.	Rules become harder to understand, change risk increases, and cleanup becomes harder over time.

II. The Horizon solution

A unified architecture for secure application connectivity

Horizon is more than a naming update or product bundle. It is a platform architecture for how enterprises govern secure application connectivity across hybrid and multi-cloud environments.

AlgoSec describes Horizon as an application-centric security management and automation platform for hybrid networks, built to provide visibility into security and compliance issues, discover business applications across multi-cloud and data center environments, automate application connectivity changes, prioritize risk based on business context, and support application-centric compliance. [6]

The platform advantage comes from shared context. When visibility, policy analysis, change workflow, cloud enforcement, object management, and audit evidence share the same application-centric view, teams can move from manual interpretation to informed action.

Horizon capability chain: secure application connectivity

The value is not only each capability, but the shared context between them: application, risk, policy, workflow, and evidence.

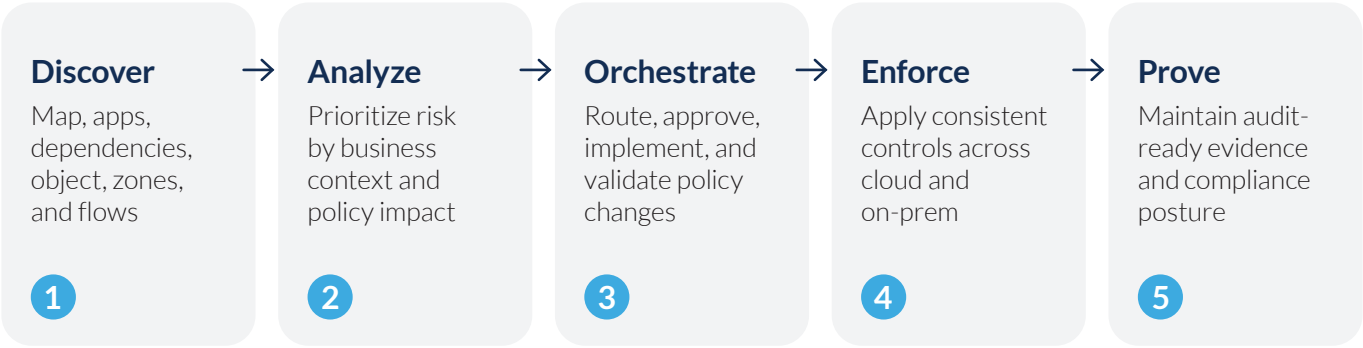


Figure 2. Horizon connects discovery, risk analysis, workflow automation, enforcement, and compliance evidence.

From tool-centric to application-centric

Traditional question	Horizon-style question
Which firewall rule needs to change?	Which application needs connectivity, who owns it, and what risk is introduced?
Which console has the answer?	What is the single business view of the application, dependencies, flows, policies, risks, and evidence?
Can someone approve this ticket?	Can the workflow validate the lowest-risk path, preserve approvals, and implement consistently?
Which rule caused the issue?	Which application, path, object, control, or change event explains the business impact?
Can we prepare for the audit?	Can we continuously show who changed what, why, when, and with what control evidence?

Horizon module map

How Horizon capabilities connect to enterprise pains

The Horizon business case becomes stronger when each module is tied to a customer pain, an operational outcome, and a partner services opportunity.

Horizon capability	Customer pain addressed	Value narrative	Partner or expansion motion
Horizon Security Analyzer	Fragmented hybrid topology, risky rules, unclear policy impact, audit pressure.	Visualize the hybrid network, understand policy impact on traffic, troubleshoot connectivity, run what-if analysis, identify compliance gaps, and prioritize risky rules by business value. [7]	Assessment, rule review, compliance readiness, segmentation validation, firewall refresh support.
Horizon FireFlow	Manual change requests, slow approvals, inconsistent validation, weak evidence trail.	Automate and orchestrate policy changes with proactive risk analysis, validation, auditing, and workflow control to prevent errors and save time. [8]	Workflow design, ITSM integration, automation readiness, standard-change catalog.
Horizon AppViz	Application owners and security teams lack a shared map of dependencies and flows.	Use AI-powered application discovery to identify application candidates and dependencies, connect applications to policies, prioritize risk in business context, and support application-centric compliance. [9]	Application onboarding, migration planning, app dependency mapping, recertification services.
Horizon ACE / AlgoSec Cloud Enterprise	Cloud controls and data center controls are governed separately.	Provide cloud network security capabilities for multi-cloud environments, including visibility, consistent policy enforcement, automated change management, compliance management, and risk mapping to applications. [10]	Cloud migration, cloud governance, zero-trust guardrails, managed cloud policy operations.
Horizon ObjectFlow	Duplicate, unused, misaligned, and unattached objects slow changes and increase risk.	Centralize network object management across data centers and hybrid-cloud estates, automate object changes, and identify object hygiene issues that create policy risk. [11]	Object cleanup, hygiene assessment, standardization, post-merger consolidation.
Partner ecosystem and services	Customers require a strategic partner to identify operational gaps and implement the integration, automation, and scaling necessary to achieve their target future state.	AlgoSec highlights partner enablement, co-selling, growth support, and services opportunities across consulting, architecting, auditing, customization, implementation, and post-sales support. [12]	Services packages, managed governance, account expansion, renewal support.

The platform advantage

- One application-centric view: connect applications, flows, rules, zones, objects, risks, owners, and evidence.
- Risk-aware automation: automate repeatable, validated changes while escalating exceptions through governance.
- Continuous compliance posture: shift from audit reconstruction to ongoing evidence and reporting.
- Hybrid consistency: align cloud and data center connectivity decisions under a common operating model.
- Partner leverage: create repeatable high-value services around assessment, cleanup, integration, migration, automation, and managed governance.

III. The financial case

Calculating ROI: move the discussion from tools to outcomes

The financial case for Horizon should be built from customer-specific baseline data. Generic ROI claims can open a door, but enterprise buyers and channel partners win trust by quantifying the customer environment: change volume, hours per task, audit frequency, tool spend, critical application exposure, incident history, and planned cloud or zero-trust initiatives.

AlgoSec provides ROI calculators as examples of how customers can model potential value based on their own assumptions. [13] The right posture is consultative: baseline the current operating model, model conservative improvements, agree on success metrics, then measure realized value after deployment.

Build the business case from measurable value pools

Recommended practice: baseline costs first, model conservative improvements, then validate realized value.

Labor capacity

Change engineering, policy review, rule cleanup, and evidence collection hours returned to the team.

Tool rationalization

Reduced duplicate licensing, support, infrastructure, and administration across overlapping tools.

Downtime avoidance

Fewer policy-related incidents, faster troubleshooting, and better pre-change validation.

Audit readiness

Continuous reports, evidence trails, and recertification workflows that reduce audit scramble.

Risk reduction

Prioritized remediation based on applications, exposure, compliance, and business criticality.

Partner services

Assessments, migrations, cleanup, automation design, and managed policy governance.

Figure 3. Horizon ROI should be modeled across labor, consolidation, downtime, audit readiness, risk, and partner services.

ROI model: categories and formulas

Value pool	Suggested formula	Inputs to collect
Policy-change labor capacity	(Current hours per change - target hours per change) x changes per month x fully loaded hourly cost x 12.	Monthly change volume, median and p90 cycle time, effort by role, rejection and rework rate.
Audit preparation savings	(Current audit-prep hours - target audit-prep hours) x hourly cost x audits per year.	Audit frequency, evidence sources, hours by team, number of controls and environments.
Tool rationalization	Retired license cost + support + infrastructure + admin overhead.	Overlapping tools, renewal dates, support contracts, admin effort, report duplication.
Downtime and emergency change avoidance	Avoided incident hours x business impact per hour x conservative attribution factor.	Policy-related incident history, critical app impact, MTTR, emergency change count.
Risk and compliance exposure reduction	Qualitative risk score reduction plus avoided remediation effort.	Risk register, compliance findings, risky rules, open exceptions, control gaps.
Cloud and migration acceleration	Reduced migration delay x application value or project cost burn rate.	Migration waves, app criticality, dependency mapping time, change backlog.

Illustrative assumptions to replace with customer data

Business-case input	Conservative example	How to validate
Change volume	200 policy changes per month.	Export 6-12 months of ticketing and change-management data.
Manual effort reduction	1.5 hours saved per standard change after workflow automation and validation.	Time-study 20 recent changes across request, design, review, implementation, validation, and evidence.
Hourly cost	USD 90 fully loaded blended engineering rate.	Use finance-approved labor rates by role and region.
Audit evidence effort	300 hours reduced annually through automated reports and evidence trails.	Review last audit prep project plan and evidence requests.
Tool rationalization range	USD 40,000-100,000 in potential annual duplicate-tool spend identified during review.	Compare current contracts, report use, admin ownership, and renewal timelines.
Standard-change acceleration	Repeatable low-risk changes move from days of queue time to hours or minutes when governance rules permit.	Run a pilot on predefined low-risk change types and measure cycle time end to end.

IV. Operational transformation

The Horizon effect: from policy tickets to policy intelligence

The shift to Horizon is not only a technology change. It changes how teams plan, approve, implement, validate, and audit application connectivity. The goal is to make secure connectivity a repeatable business capability rather than a sequence of manual, tool-specific tasks.

Operating model	Before Horizon	With Horizon
Visibility	Network, cloud, and application context live in separate tools.	**Teams use a shared application-centric view of connectivity, risk, and policy impact.**
Change management	Requests move through manual handoffs, interpretation, and implementation.	**Policy changes are routed through risk-aware workflows with validation and evidence.**
Application delivery	Application teams wait for security translation and troubleshooting.	**Application context is mapped to connectivity needs and policy requirements earlier.**
Risk prioritization	Risks are reviewed as technical findings or rule exceptions.	**Risks are prioritized based on application criticality, exposure, compliance, and business context.**
Compliance	Evidence is reconstructed for audits from multiple systems.	**Evidence is maintained as part of the change and governance lifecycle.**
Partner services	Projects are sold as one-time tool deployments.	**Partners can deliver lifecycle services: assessment, cleanup, migration, automation, governance, and managed operations.**

Governance design principles

- Start with application criticality and ownership. Automation is most valuable when business context is known.
- Define standard changes that are safe to automate. Not every change should bypass human review.
- Use risk scoring before implementation. Preventive analysis is more valuable than post-change cleanup.
- Integrate with existing systems of record. Horizon should complement ITSM, CMDB, cloud, firewall, vulnerability, SIEM, SOAR, and DevOps workflows.
- Make evidence a byproduct of work. Approvals, validation, policy impact, and compliance status should be captured as the process runs.
- Measure adoption, not only deployment. Track cycle time, rework, object hygiene, risky rules, audit hours, and application coverage.

KPI scorecard for enterprise customers and partners

Metric	Why it matters	Suggested reporting cadence
Median and typical vs. slowest policy change completion times policy-change cycle time	Shows whether the platform is improving delivery speed and predictability.	Monthly
Change rework or rejection rate	Highlights incomplete requirements, risk issues, and workflow gaps.	Monthly
Emergency change volume	Indicates whether preventive governance is reducing reactive work.	Monthly or quarterly
Risky, unused, duplicate, expired, and overly permissive rules	Shows policy hygiene and risk-reduction progress.	Monthly
Object hygiene score	Measures duplicate, unattached, misaligned, and inconsistent object cleanup.	Monthly
Audit evidence collection hours	Quantifies compliance-effort reduction.	Per audit and quarterly
Application onboarding coverage	Shows the percentage of critical applications mapped to connectivity and policy context.	Quarterly
Cloud policy drift or exceptions	Highlights misalignment between cloud and data center governance.	Monthly

Audience Playbook

How to tailor the Horizon business case

A strong Horizon conversation changes by audience. The same platform story can be framed as a risk-reduction initiative for CISOs, a delivery-speed initiative for CIOs, a resilience initiative for compliance and operations teams, and a profitable services motion for channel partners.

Audience	Primary pain	Best opening message	Recommended next step
Enterprise prospects	Fragmented tools, cloud complexity, manual change, audit friction, and lack of application context.	You can reduce the operational cost and risk of secure application connectivity by unifying visibility, workflow, and policy evidence.	Run a Horizon business-value workshop focused on one critical application or change workflow.
Existing AlgoSec customers	Value may be concentrated in analysis and reporting, with additional opportunity in automation, cloud, AppViz, and object governance.	You already have a foundation for visibility. The next value step is expanding into risk-aware automation and application-centric governance.	Review current module usage, adoption KPIs, and expansion opportunities by environment and use case.
Channel partners	Customers need help connecting security, cloud, compliance, and application-delivery initiatives.	Horizon creates a services-led platform motion: assess, map, clean up, automate, integrate, govern, and manage.	Package repeatable offers such as policy complexity assessments, cloud-governance workshops, app dependency mapping, and automation pilots.
CISO and risk leaders	Policy error, control drift, audit exposure, and lack of business context for security decisions.	Horizon helps move from reactive policy management to continuous application risk governance.	Baseline risk and compliance KPIs for critical applications and high-risk zones.
Network and cloud operations	Change backlog, handoffs, troubleshooting time, and inconsistent workflows across environments.	Horizon can reduce manual work and improve first-time-right changes by validating risk and impact before implementation.	Select low-risk standard changes for automation readiness.
Application owners	Security processes can delay launch dates and obscure connectivity requirements.	Horizon translates connectivity into application language, improving collaboration between app, cloud, network, and security teams.	Map one priority application and document its required flows, owners, dependencies, and policy status.

Discovery questions for workshops

- How many security policy change requests do you process each month, and what are the median and p90 cycle times?
- How many consoles or teams are required to answer whether a critical application has the connectivity it needs?
- How often do change requests get rejected, reworked, or rolled back because requirements or risk context were incomplete?
- Which applications have caused war rooms, emergency changes, audit exceptions, or customer-visible downtime in the last 12 months?
- How much time does audit preparation require, and what evidence is hardest to collect?
- Which firewall, cloud, SDN, ITSM, CMDB, SIEM, SOAR, vulnerability, or DevOps tools must Horizon integrate with?
- Which low-risk, repeatable change types could be automated first without increasing business risk?
- Which partner services would accelerate adoption: assessment, cleanup, implementation, integration, migration, training, or managed governance?

Channel partner guide

Turning Horizon into a partner-ready sales motion

The most effective partner motion is consultative. Start with the customer business event, quantify the operational burden, map Horizon capabilities to measurable outcomes, and attach services that help the customer realize value faster.

Partner offer	Customer trigger	Deliverables	Expansion path
Policy complexity assessment	Firewall refresh, audit pressure, cloud migration, or recurring change delays.	Tool inventory, policy hygiene findings, risky-rule summary, object-sprawl analysis, value hypothesis.	Security Analyzer, ObjectFlow, FireFlow.
Application connectivity pilot	Critical application migration, new digital service, zero-trust segmentation program.	Application dependency map, required flows, policy gaps, risk analysis, governance recommendations.	AppViz, FireFlow, Horizon ACE.
Automation readiness workshop	Change backlog, ITSM modernization, staffing constraints, incident remediation pressure.	Standard-change catalog, workflow map, approval model, integration plan, KPI baseline.	FireFlow and ITSM integration services.
Cloud governance package	Multi-cloud growth, cloud audit findings, inconsistent security groups, cloud migration waves.	Cloud policy posture review, app-to-risk mapping, guardrail recommendations, remediation backlog.	Horizon ACE and managed cloud governance.
Audit and compliance readiness	DORA, NIS2, PCI DSS, internal audit, regulatory remediation.	Evidence map, reporting workflow, control alignment, remediation plan, continuous reporting model.	Security Analyzer, AppViz, FireFlow.
Managed policy governance	Lean internal staff, global operations, complex change volume, partner-led support model.	Ongoing KPI reporting, policy cleanup, workflow tuning, governance reviews, quarterly business review.	Multi-year services and renewal support.

Objection handling

Objection	Response angle
We already have firewall management tools.	Horizon is not only about managing firewalls. It connects policy, application context, risk, workflow, cloud controls, objects, and compliance evidence.
Automation feels risky.	The recommended approach is risk-aware automation. Start with standard, low-risk, validated changes and route exceptions through governance.
Our cloud team uses its own tools.	The goal is not to replace every cloud-native tool. The goal is consistent policy governance and application context across cloud and data centers.
We are not ready for a platform project.	Start with a business-value workshop or limited pilot around one critical application, one migration wave, or one repeatable change type.
The ROI is hard to prove.	Use customer-specific baselines: change volume, cycle time, rework, audit hours, tool costs, incident history, and migration delays. Then measure actual outcomes after deployment.

Action Agenda

A 90-day path from fragmented visibility to measurable value

This sequence lets a customer prove value without waiting for a full enterprise rollout.

Days 1-30
Baseline and prioritize

- Inventory controls and integrations
- Select high-value applications
- Document current change and audit flow

→

Days 31-60
Pilot and prove

- Map dependencies and risks
- Automate low-risk repeatable changes
- Create initial compliance evidence pack

→

Days 61-90
Scale and govern

- Expand to additional apps and clouds
- Publish KPI dashboard
- Define partner or managed services motin

Figure 4. A practical 90-day path for prospects, existing customers, and partner-led engagements.

Recommended workstreams

Workstream	First 30 days	Days 31-60	Days 61-90
Application focus	Select 1-3 critical applications or migration workloads.	Map dependencies, flows, owners, and risk.	Expand coverage to the next application tier.
Policy and object hygiene	Baseline risky, duplicate, unused, expired, and overly broad rules and objects.	Prioritize cleanup by business impact and change risk.	Operationalize cleanup and reporting cadence.
Automation	Identify standard, low-risk changes and approval paths.	Pilot workflow automation and validation.	Scale automation and measure cycle-time improvement.
Compliance evidence	Map current evidence sources and audit pain points.	Create initial automated report package.	Define continuous compliance operating rhythm.
Integration	Inventory ITSM, CMDB, cloud, firewall, SDN, SIEM, SOAR, vulnerability, and DevOps tools.	Prioritize integrations for the pilot.	Document production integration roadmap.
Governance and KPIs	Agree on executive scorecard.	Publish pilot metrics.	Create QBR rhythm and expansion roadmap.

Executive scorecard template

Outcome	Baseline metric	Target example	Owner
Accelerate secure application delivery	Median and p90 change cycle time.	Reduce cycle time for standard changes while preserving risk review.	Network/security operations.
Reduce policy risk	Risky rules, overly permissive rules, unvalidated changes.	Reduce high-risk policy exceptions and improve validation coverage.	CISO/risk.
Improve audit readiness	Audit evidence collection hours and findings.	Produce consistent evidence with less manual collection.	Compliance.
Strengthen hybrid governance	Controls covered across cloud and data centers.	Increase application coverage and policy consistency.	Cloud/network leadership.
Increase partner value	Services attach rate and recurring governance opportunities.	Move from implementation project to lifecycle services.	Channel partner.

Conclusion

The Horizon effect at Company X: a composite enterprise story

Before Horizon, Company X managed policy through isolated consoles and reactive processes. A customer-facing application issue could trigger a multi-hour war room. Standard changes waited in queues while teams clarified requirements, reviewed risk manually, implemented policy updates, and collected evidence. Audit preparation required weeks of reconstruction because policy intent, approvals, rules, objects, application context, and compliance status lived in different places.

After adopting a Horizon operating model, the conversation changes. Security, network, cloud, compliance, and application teams work from a shared understanding of application connectivity. Application owners see dependencies and business impact. Security teams analyze risk before policy changes are committed. Standard, low-risk changes can move through governed automation while exceptions receive deeper review. Compliance teams shift from annual evidence hunts to continuous reporting and traceability.

Most importantly, the team no longer views secure connectivity as a blocker. It becomes a business capability: faster application delivery, better risk decisions, cleaner policy, stronger audit readiness, and a more scalable operating model for hybrid and multi-cloud security.

Message map for field and partner teams

Conversation trigger	Horizon message	Proof to collect
Application launch delays	Horizon aligns security policy with application connectivity so teams can approve, implement, and validate changes faster.	Change cycle time, rework, backlog, and application owner feedback.
Cloud migration or multi-cloud growth	Horizon helps govern cloud and data center connectivity under one application-centric operating model.	Number of cloud accounts, security groups, firewalls, regions, apps, and migration waves.
Audit or regulatory pressure	Horizon helps create traceable evidence for policy intent, approvals, changes, risk, and compliance posture.	Audit hours, findings, evidence sources, and compliance scope.
Firewall refresh or consolidation	Horizon helps customers rationalize policy, clean up objects, and reduce migration risk.	Rule/object counts, risky rules, unused rules, duplicate objects, and migration timeline.
Zero-trust segmentation	Horizon helps map applications and enforce segmentation decisions with business context.	Critical applications, zones, dependencies, risk tiers, and exception process.
Managed services opportunity	Horizon gives partners a recurring governance model across visibility, cleanup, change automation, and compliance reporting.	Operational KPIs, support scope, QBR cadence, and services backlog.

Sources and notes

References used for market, product, and regulatory context

This white paper uses public product and industry references for market context, product descriptions, regulatory framing, and partner-program language. Validate final product names, packaging, availability, claims, customer examples, and financial assumptions with AlgoSec before external publication.

[1] Flexera 2025 State of the Cloud coverage

[2] Palo Alto Networks 2025 State of Cloud Security

[3] EU Digital Operational Resilience Act (DORA)

[4] European Commission NIS2 Directive overview

[5] IBM Cost of a Data Breach Report 2025

[6] AlgoSec Horizon launch announcement

[7] AlgoSec Horizon Security Analyzer/Firewall Analyzer

[8] AlgoSec Horizon FireFlow

[9] AlgoSec Horizon AppViz

[10] AlgoSec Cloud Enterprise / Horizon ACE

[11] AlgoSec Horizon ObjectFlow

[12] AlgoSec Channel Partner Program

[13] AlgoSec ROI Calculator

Publication note: Customer scenarios, ROI ranges, and operating metrics are illustrative examples for business-value discovery. They should be replaced with customer-specific data before being used in a proposal, business case, or contractual commitment.

© 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.