Secure application connectivity across your hybrid environment

An AlgoSec eBook

algosec

Secure application connectivity.

Secure the applications that run your business

Visualize application connectivity

Securely **automate** application connectivity changes

Maintain continuous **compliance**

Easily discover and **manage risk**

Table of content

About AlgoSec

Founded in 2004

2200+ enterprise customers

Serving 20 of the Fortune 50

24/7 support via 3 global centers

ISO 27001 Certified

Passionate about customer satisfaction

Proudly serving the world's largest and most complex enterprise organizations

NCR, IBM, AT&T, gm, Chevron, American Express, experian, Unilever, EY, Dominion Energy, DELTA

Morgan Stanley, Hewlett Packard Enterprise, usbank, sanofi, United Nations, Schneider Electric, ATRUVIA, Lufthansa Systems, orange

Emirates, Bell, LOWE'S, ERICSSON, SONY, ING, nab, euroclear, FAB First Abu Dhabi Bank, BT, ENBRIDGE

Applications are at the core of business growth

Applications are the backbone of modern business, driving growth, innovation, and competitive advantage. However, the rapid acceleration of application deployment and network complexity—what we call the **100x revolution**—has created unprecedented challenges. Applications are now interconnected across multiple clouds and on-premises systems, increasing both operational complexity and security risks.

To address these challenges, a **convergence between cloud and datacenter security teams** is redefining how organizations manage their hybrid infrastructures. This alignment bridges gaps between historically siloed teams, enabling unified policy enforcement, streamlined governance, and consistent threat management across environments. By adopting a converged approach, businesses can:

- Reduce inefficiencies and operational silos
- Respond faster to threats with centralized visibility
- Maintain consistent compliance across cloud and on-premises systems
- Support the agility required to meet evolving business demands

Your applications are growing, and so are their needs. They're no longer just facilitating tasks—they're driving new revenue streams, accelerating business growth at unprecedented speeds, and modernizing operations in a digital-first world.

However, this **100x growth** introduces its own set of risks. As companies increasingly deploy cloud and on-premises systems to meet rising business demands, the complexity of managing interconnected applications, ensuring consistent compliance, and securing hybrid environments has become a critical challenge.

The convergence of cloud and datacenter security is no longer optional—it is essential to addressing these risks while enabling the security, compliance, and connectivity needed to keep pace with the demands of the **100x revolution**.

Development and networks are changing

With companies relying on more applications, connections, and layers, networks are now 100x more complex. Development teams adopt cloud technologies and automation to accelerate deployments, while security teams grapple with managing threats across hybrid environments. To meet these challenges, organizations are embracing **platformization** to unify security operations, automate policies, and enhance visibility across infrastructures.

At the same time, **a convergence of cloud and datacenter security teams** is enabling seamless policy enforcement, improved threat management, and consistent compliance across on-premises and cloud systems. Together, convergence and platformization are transforming how organizations address Scale, Speed, and Security, ensuring agility and resilience in an interconnected world.

Development

To keep up with the business and market demands, development teams are adapting by:

- Leveraging cloud technologies for speed and scale
- Utilizing automation for rapid deployments
- More IT system integrations
- Increasing the frequency of changes and updates

Networks

There is a technology transition happening:

- Applications have more layers and connections
- New network components - SASE, SD-WAN, Cloud FWs, NGFWs, FWaaS
- New infrastructure and workload solutions
- Convergence of on-premises and cloud environments, creating seamless integration for application connectivity and security

The need for change

Speed and complexity are a dangerous combination for companies today and create increased risk. And by making frequent changes in this fast, dynamic, and complex network can lead to:

Application downtime

- Bad configurations to a small part of an application can block it from working
- Complex networks cause troubleshooting difficulties
- Poor network visibility makes it difficult to avoid configuration mistakes

Security breaches

- Complex Cloud and network infrastructure that support applications are high risk attack surfaces
- Security policies aren't mapped for applications so understating risk is difficult
- Investigations risk and vulnerabilities requires development to halt and slows down growth

Compliance

- Rapid changes need continues monitoring and constant adaptation to stay compliant
- Difficulty following current violations that exist cross complex and dynamic networks
- Gathering evidence and preparing audits is difficult and time consuming

With the result of all these being

Loss of revenue, damage to the company reputation, heavy fines, and other legal problems.

Whether it's cloud, on-premises, or a hybrid of both, reshaping and managing your security policies and connectivity is essential to preventing misconfigurations, limiting downtime, and reducing compliance risks. **Convergence between cloud and datacenter security teams** addresses these challenges by aligning strategies, unifying policy enforcement, and ensuring consistent security across hybrid environments.

At the same time, **platformization** provides centralized tools that streamline operations, automate processes, and enhance visibility—empowering organizations to adapt to change with confidence. This approach not only prevents disruptions but also aligns your development and security teams. Our vision is simple: embed security into the development stage—**security before you need it**.

Paradigm shift

- Traditional manual processes can't address the complexity
- Old processes can't keep up with the rate and number of changes
- Meeting compliance regulations now takes more time and effort
- Basic policy management tools miss the business application context

Increased risk has an increased cost

Your organization's operational integrity and data safety are at risk. Whether it's protecting sensitive data or securing public-facing servers, every aspect of your network security requires a proactive and strong approach.

As security caused IT failures are becoming more and more problematic, several companies have faced significant operational disruptions. Sainsbury's and Tesco, Greggs and even McDonald's are among the list of companies who suffered from severe IT meltdowns. Leading to downtime and bad press.

Sainsbury's and Tesco cancel home deliveries after being hit by IT meltdowns

Supermarkets' technical problems understood to be unrelated and not being investigated as potential cyber attack

Are the outages of Tesco, Gregg's, Sainsbury's and McDonald's linked? Mystery as high street hit by outages

Companies refuse to give details on major technical problems – but experts say that they serve as a warning for retailers to increase their resilience

INDEPENDENT | The Independent

Greggs shops close across the UK as IT glitch causes payment issues

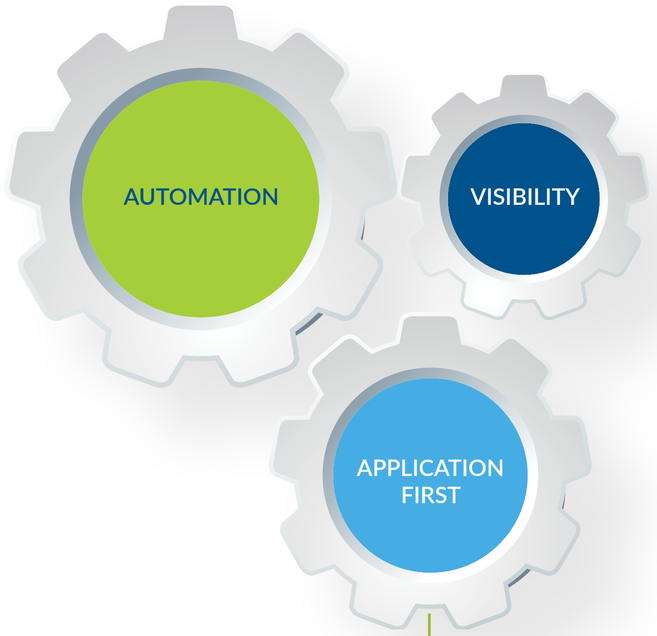
Greggs is hit by IT glitch: Stores across Britain are forced to shut or go cash-only due to 'issues accepting payments' - after Tesco, Sainsbury's and McDonalds all suffered technical meltdowns

By Mark Duell
08:03 20 Mar 2024, updated 12:53 20 Mar 2024

In the Gregg's case, customers found themselves unable to complete purchases. Now while these cases are individual incidents, a broader pattern is emerging. Companies have a need to update their application security and be prepare for 100x revolution.

The AlgoSec Horizon Platform and value

Simply put our solution isn't just for the sake of security, but security that empowers your hybrid environment and your business without interfering with your productivity. Our aims are to re-set the focus on what matters most, to keep your applications secure and running without fear of downtime.



Visible, manageable, and automated

Application-centric view

Utilizing a patented application-centric view of the hybrid-cloud network to simplify infrastructure complexity.

Application connectivity change automation

Facilitating rapid planning and execution of application connectivity and security changes with zero-touch automation, with native capabilities such as **Pushing changes** and **Remove policy.**

With our automated solutions app teams can simple place a request send it, and once approved it is automatically implanted all in real time.

Comprehensive visualization and management

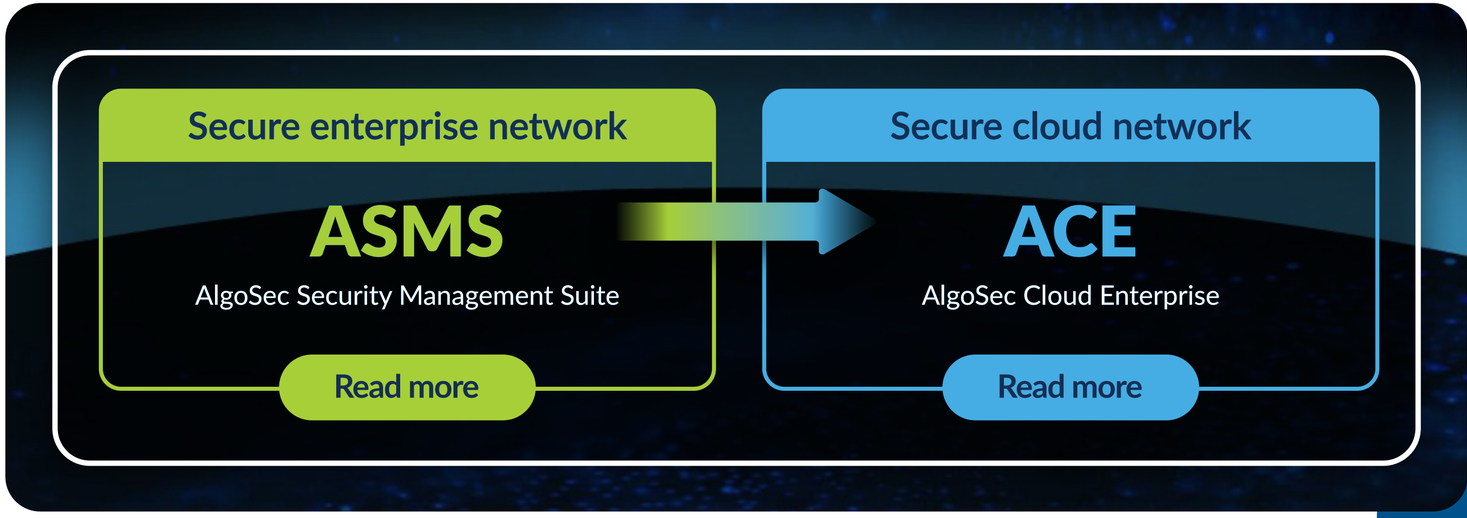
Enabling single view visualization and management of application connectivity and security policies across all environments – Cloud and On-premises or both.

AlgoSec Horizon – the industry's first application-centric platform

Why AlgoSec Horizon stands out

The first and only application-centric security management and automation platform for the hybrid network

- **Visibility that matters:** Gain a unified view of application connectivity across enterprise and cloud networks, identifying risks and dependencies at every layer.
- **Automation you can trust:** Automate policy changes and compliance workflows—firewall policy updates, risk assessments, and audit reporting—saving time while maintaining accuracy.
- **Continuous compliance:** Always audit-ready with continuous monitoring and dynamic policy adjustments, aligned to evolving regulations like PCI DSS, GDPR, and DORA.
- **Resilience through innovation:** Align security with business needs, enabling rapid application deployment while minimizing downtime and security risks.



Key components of the Horizon Platform

- **Application-centric visibility:** AppViz and ObjectFlow uncover hidden dependencies, mapping connectivity across on-premises and hybrid systems.
- **Automation for accuracy:** FireFlow automates policy changes, recertification, and compliance checks, reducing manual errors and audit preparation time.
- **Risk analysis and management:** Firewall Analyzer identifies misconfigurations and policy risks, ensuring proactive compliance alignment.
- **Unmatched network security posture**: Perform over 150 network security policy risk checks and customize risk parameters to enable tailored segmentation or enforce Zero Trust policies.
- **Dynamic cloud security:** AlgoSec Cloud featuring Prevasio technologies provide deep visibility into cloud infrastructure, identifying risks and misconfigurations in real-time.

Thank you!

Secure the applications that run your business

- Streamline operations
- Visualize application connectivity
- Automate application connectivity changes
- Maintain continuous compliance
- Easily discover and manage risk

All while reducing downtime and accelerating application delivery

Request a demo

algosec