

AlgoSec Horizon

Secure application connectivity
across your hybrid environment



Solution brief

 algosec



Clouds and data centers are converging

In hybrid environments, where data centers and multiple clouds coexist, the convergence of network and security introduces several specific challenges. The integration of these separate domains is necessary to manage the complexities of modern IT infrastructure, but it creates various obstacles that organizations must overcome:


Challenges

Many organizations face inconsistent security across multiple domains, which creates vulnerabilities, increases the risk of data breaches, and makes it difficult to enforce policies uniformly. This fragmentation also complicates compliance efforts, leading to potential violations and legal exposure.

Managing and enforcing security policies across diverse environments often requires manual effort. This introduces human error, delays, and misconfigurations that weaken overall security posture. The lack of automation further amplifies these challenges, making it hard for security teams to respond efficiently and consistently to threats.

Limited visibility into network and security configurations creates blind spots that hinder threat detection and response. These visibility gaps, combined with an expanding attack surface—especially in hybrid environments—provide more opportunities for attackers to exploit weaknesses, particularly at the intersections of misaligned network and security controls.

Finally, the growing complexity of regulatory requirements makes it difficult to maintain continuous compliance. Without streamlined policy alignment and orchestration, organizations risk falling short of legal and industry standards.



Addressing convergence challenges

To effectively manage these challenges, organizations need to adopt solutions that:

- **Integrate network and security management** across cloud and on-premise environments
- Provide **unified visibility and control** over the entire infrastructure
- Enable **automation and orchestration** to reduce manual effort and operational risk
- Enforce **consistent security policies** across both data centers and cloud platforms, with a focus on reducing misconfigurations and compliance risks

At AlgoSec we believe organizations can address these common convergence challenges more efficiently by adopting solutions that unify network and security management across cloud and on-premise systems. An application-centric approach is crucial to this process, as it ensures that both the network and security strategies are aligned with business-critical applications.

AlgoSec Horizon Platform

Secure application connectivity across your hybrid environment

AlgoSec Horizon is the industry's first application-centric security management platform for the hybrid network environment. Gain deep visibility, automate security changes, prioritize risk, and ensure continuous compliance in your datacenter and multi-cloud network:

- **Visualize application connectivity**

Horizon delivers an intuitive, unified view of application traffic across hybrid and multi-cloud environments. It maps traffic flows and dependencies between cloud and on-premise infrastructures, improving decision-making and enhancing proactive risk management.

- **Automate connectivity and security policies**

With Horizon, manual processes are reduced, enabling faster application deployment while ensuring security and compliance. The platform automates policy changes seamlessly across hybrid environments, reducing errors and operational disruptions.

- **Prioritize risks based on business context**

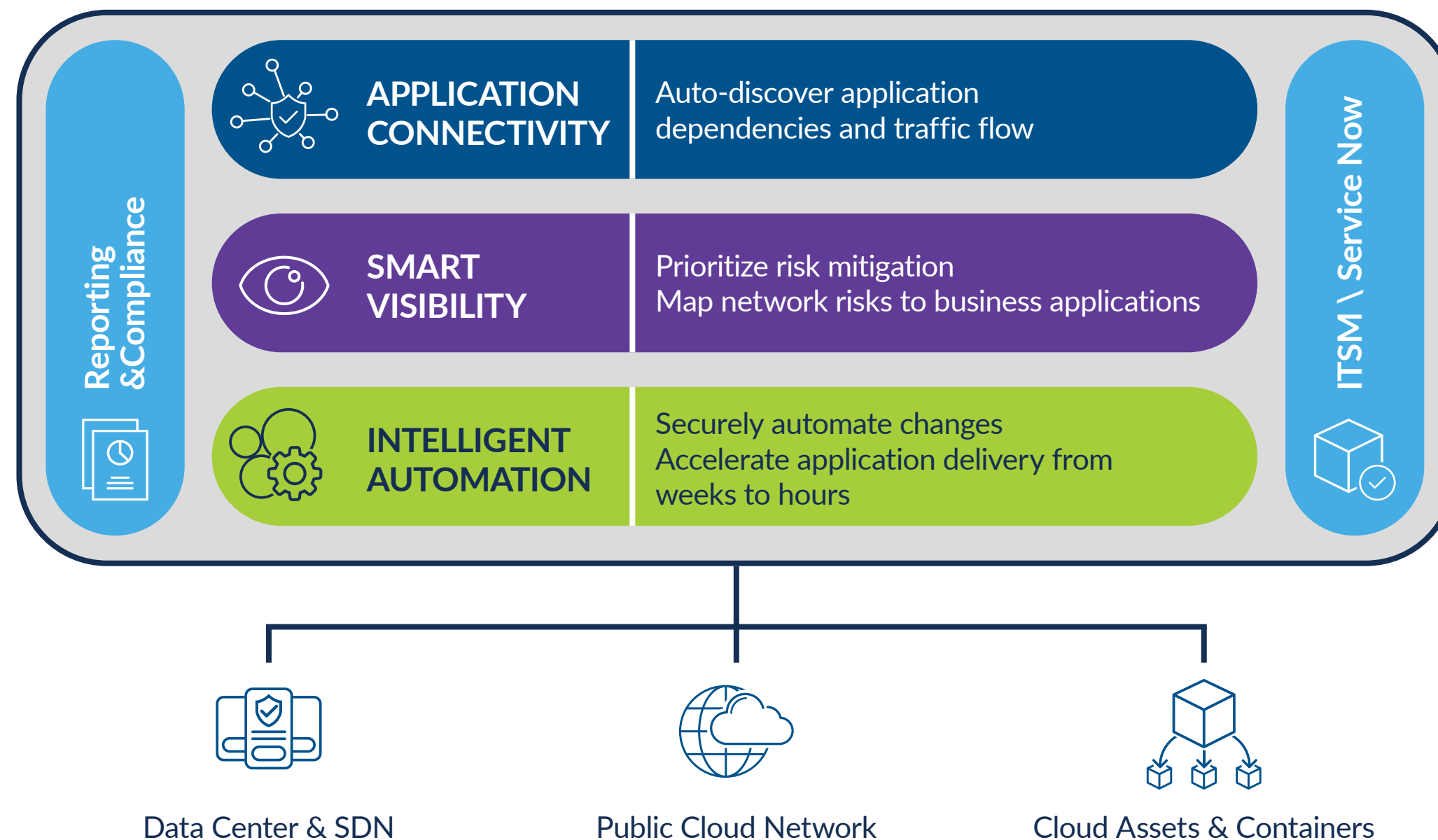
Horizon links security risks directly to business-critical applications. By focusing on the most important risks, organizations avoid alert fatigue and ensure that high-priority issues are addressed first.

- **Maintain application-centric compliance**

Horizon simplifies compliance by automatically identifying policy gaps and streamlining audit preparation, helping security teams efficiently manage compliance requirements across hybrid infrastructures, reducing risk, and saving valuable time.

Key benefits of AlgoSec Horizon

- Secure application connectivity across hybrid environments
- Accelerate security and compliance processes
- Automate security policy enforcement, reducing manual effort
- Gain end-to-end visibility into application traffic and risks
- Prioritize risks and improve security decision-making based on business-critical applications



ALGOSEC HORIZON PLATFORM

Secure application connectivity
across your hybrid environment

Secure your enterprise network

ASMS

AlgoSec Security
Management Suite

Secure your cloud network

ACE

AlgoSec Cloud
Enterprise

Visualize application connectivity
Auto-discover application dependencies
and traffic flows

Prioritize risk mitigation based on
business context
Map network security risks to applications

Securely automate application
connectivity changes
Accelerate application delivery
from weeks to hours

Maintain application-centric
compliance
Identify and resolve compliance gaps
in the cloud and datacenter

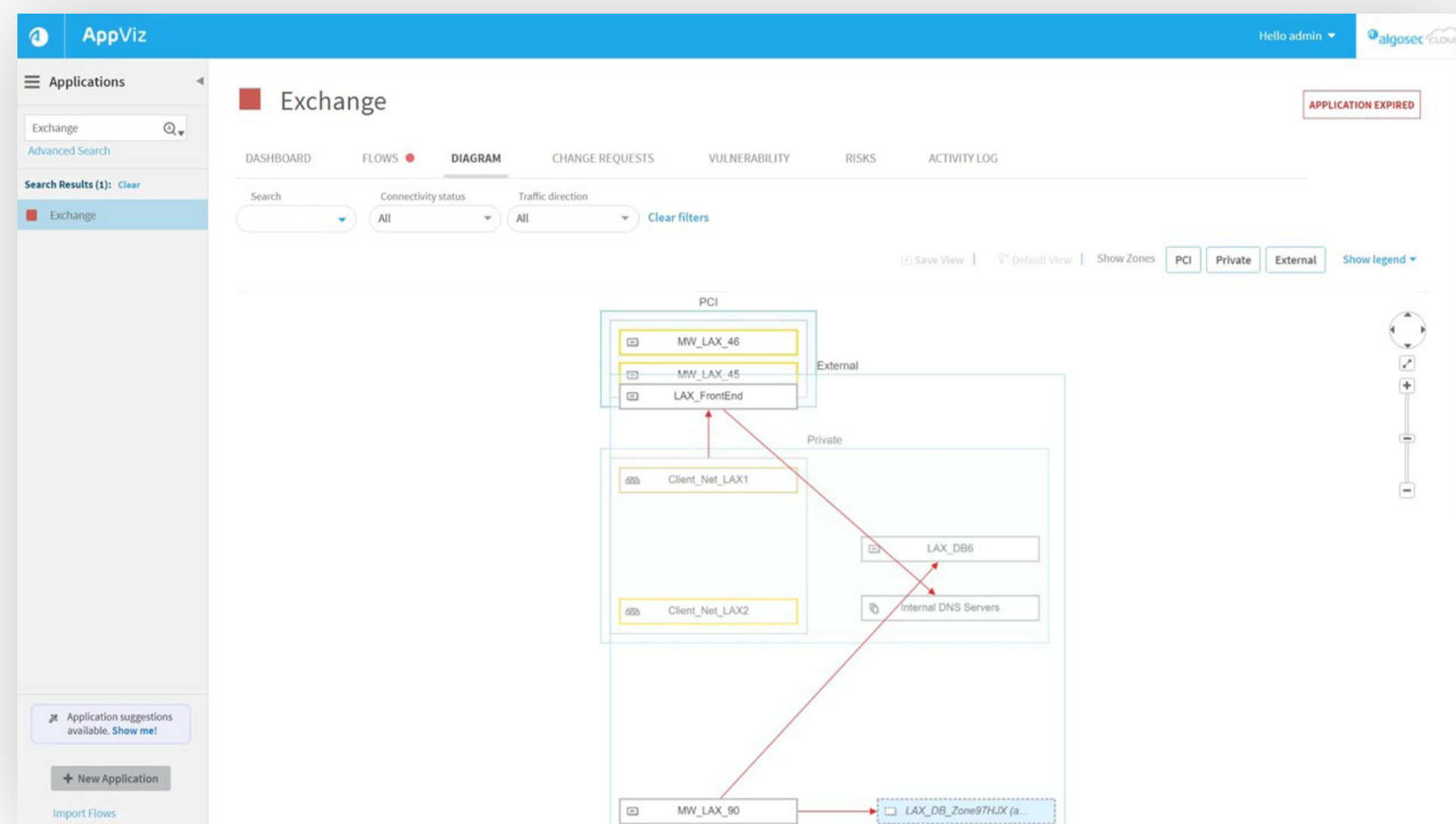
AlgoSec Security Management Suite (ASMS)

Secure your enterprise network

The **AlgoSec Security Management Suite (ASMS)** is a key component of the **AlgoSec Horizon** platform, designed to simplify and automate network security management across hybrid environments. The ASMS solution improves visibility, automates security processes, and enhances the overall security posture of hybrid infrastructures.

Key capabilities:

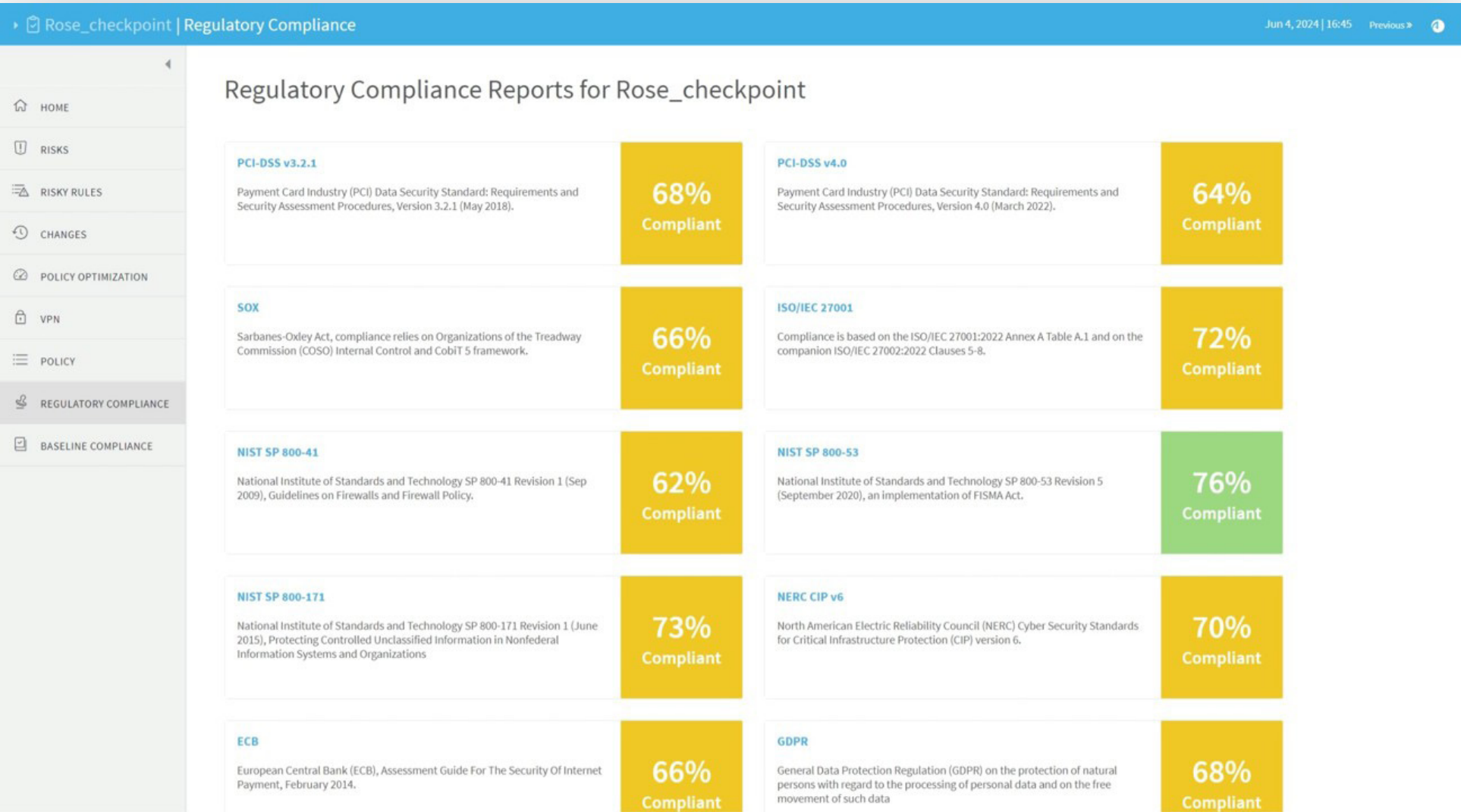
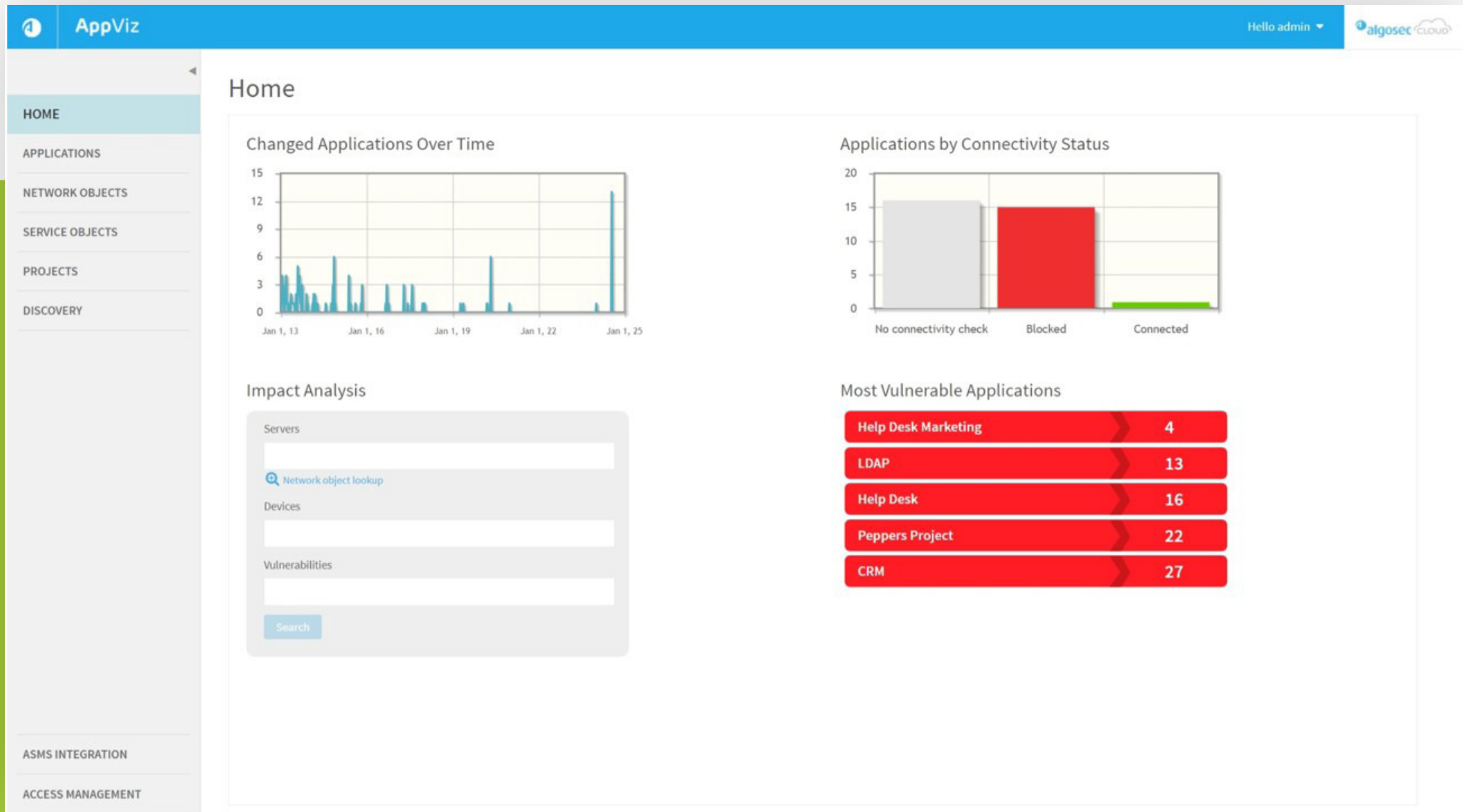
- **Unified visibility:** ASMS offers full visibility into application connectivity and network security policies across hybrid environments, including cloud and on-premise infrastructure. This provides a comprehensive, single-pane-of-glass view of all application traffic, helping organizations make faster, data-driven security decisions.



- **Automated security policy management:** ASMS automates security policy management, reducing manual tasks and minimizing errors. By ensuring security policies are consistently applied across all environments, ASMS helps accelerate security changes while maintaining compliance with regulatory standards.

AlgoSec Security Management Suite (ASMS) - Key capabilities:

- **Risk-based prioritization:** ASMS integrates risk analysis into its security policy management, enabling security teams to prioritize the most critical vulnerabilities affecting business applications. This linking of risks to application criticality, allows organizations to identify and address high-priority issues first.



- **Continuous compliance management:** ASMS helps security teams maintain compliance by automating policy audits and reporting across the hybrid network. With this feature, ASMS helps to streamline the compliance processes, ensuring that organizations stay ahead of evolving regulations.

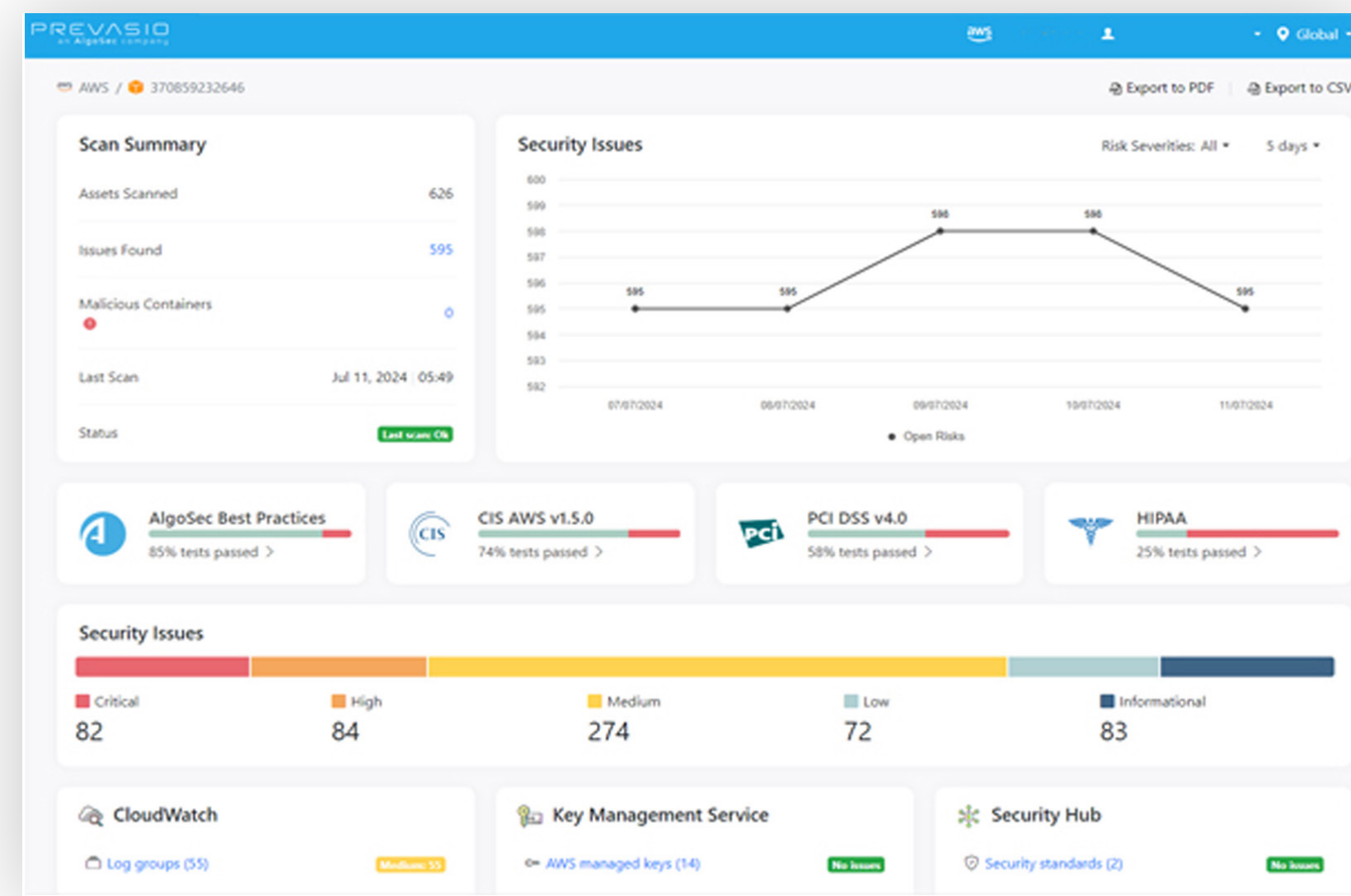
AlgoSec Cloud Enterprise (ACE)

Secure your cloud network

AlgoSec Cloud Enterprise (ACE) is another core component of the **AlgoSec Horizon** platform, extending its application-centric security capabilities into cloud environments. As businesses expand their operations into multi-cloud and hybrid infrastructures, ACE ensures that security policies, visibility, and compliance are maintained across all cloud-native applications.

Key capabilities:

- **Comprehensive cloud visibility:** ACE provides deep visibility into cloud-native application traffic, identifying application dependencies, vulnerabilities, and data flows across cloud and on-premise environments. This complements Horizon's holistic view of application connectivity, ensuring that security teams have complete visibility across the entire hybrid network.



The screenshot displays the PCI DSS v4.0 non-compliance risks table. The table lists 896 non-compliance risks, with the first 5 entries shown. The table columns are: Severity, Non-Compliance, Region, Resource, Issue, Remediation, Read more, and Action.

| Severity | Non-Compliance | Region | Resource | Issue | Remediation | Read more | Action |
|----------|--|-----------|-----------------------|--------------------------|--|---------------------------|-------------------|
| Medium | CIS 2.2.1 PCI DSS 3.5 HIPAA (Encryption) | us-east-1 | vol-0a20a865a60058137 | No EBS encryption found. | Enable EBS encryption, either using encryption by default or by enabling encryption when you create a volume that you want to encrypt. | More info | P |
| Medium | CIS 2.2.1 PCI DSS 3.5 HIPAA (Encryption) | us-east-1 | vol-0cd9a6cc64a65af84 | No EBS encryption found. | Enable EBS encryption, either using encryption by default or by enabling encryption when you create a volume that you want to encrypt. | More info | P |
| Medium | CIS 2.2.1 PCI DSS 3.5 HIPAA (Encryption) | us-east-1 | vol-0a739301daeb70319 | No EBS encryption found. | Enable EBS encryption, either using encryption by default or by enabling encryption when you create a volume that you want to encrypt. | More info | P |
| Medium | CIS 2.2.1 PCI DSS 3.5 HIPAA (Encryption) | us-east-1 | vol-0693222a0d50301b4 | No EBS encryption found. | Enable EBS encryption, either using encryption by default or by enabling encryption when you create a volume that you want to encrypt. | More info | P |
| Medium | CIS 2.2.1 PCI DSS 3.5 HIPAA (Encryption) | us-east-1 | vol-0bd63ae76d896d073 | No EBS encryption found. | Enable EBS encryption, either using encryption by default or by enabling encryption when you create a volume that you want to encrypt. | More info | P |

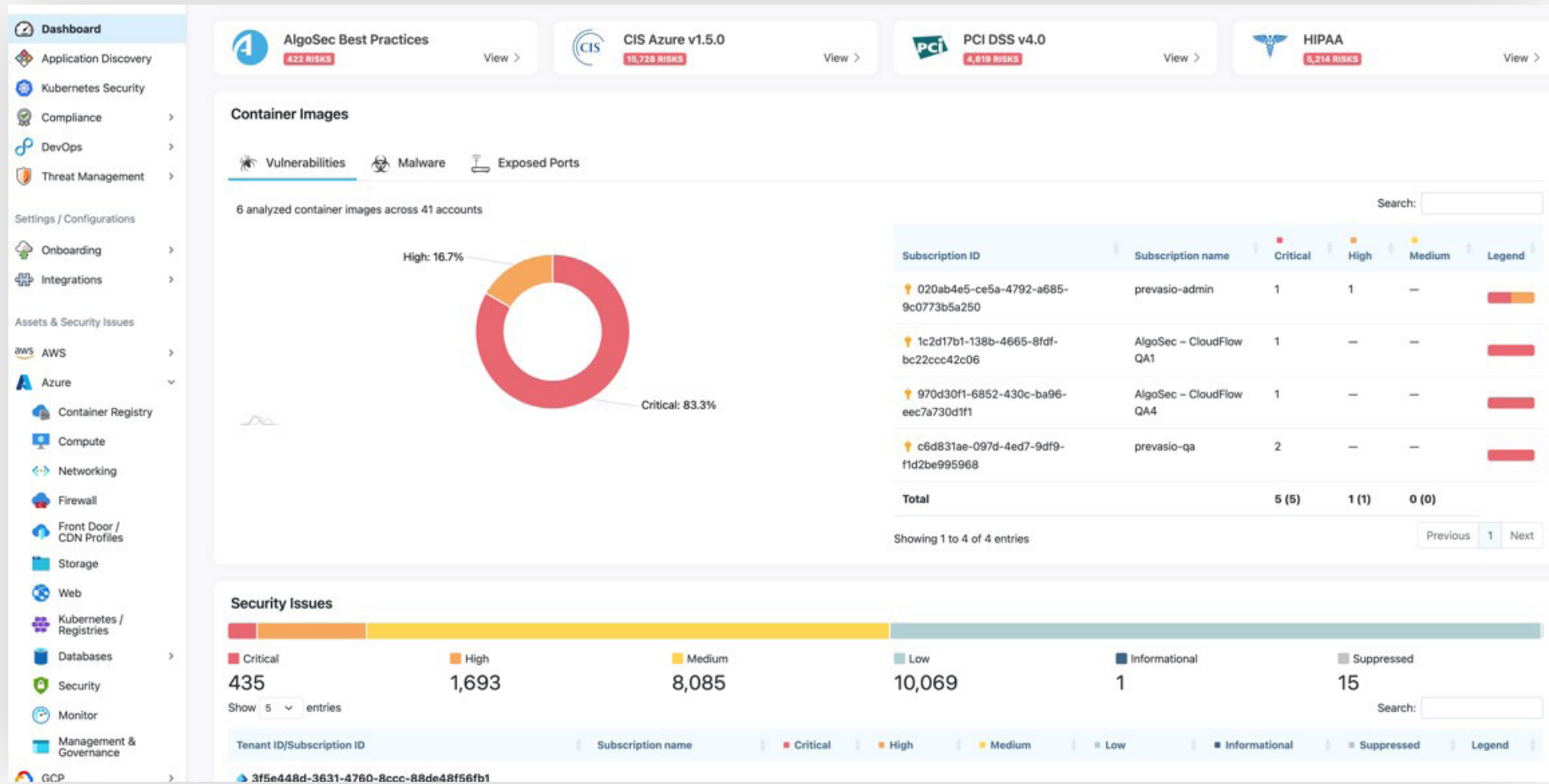
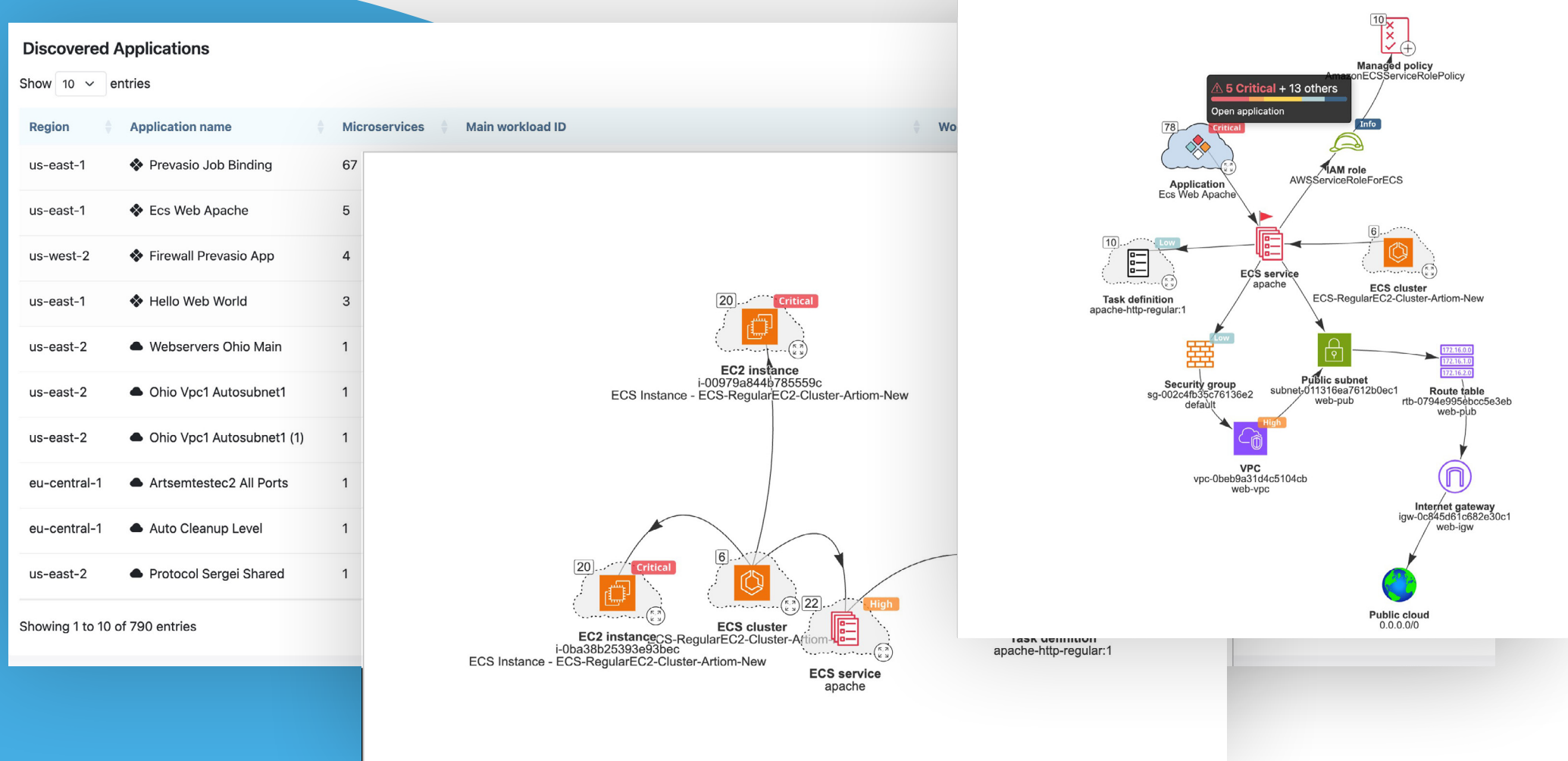
Showing 1 to 5 of 896 entries

- **Automated security policy enforcement:** ACE automates the management of security policies across multi-cloud environments, ensuring consistent enforcement of security policies, even in complex cloud infrastructures. This reduces manual intervention, supporting Horizon's goal of automating security and connectivity changes across hybrid environments.

AlgoSec Cloud Enterprise (ACE) - Key capabilities:

- **Micro-segmentation for enhanced security:** ACE isolates cloud applications using micro-segmentation, reducing the blast radius of potential attacks and containing threats. This aligns with Horizon’s risk prioritization, ensuring that applications are secured based on their business-critical value.
- **Compliance monitoring:** ACE provides automated compliance monitoring for cloud applications, ensuring adherence to industry regulations such as PCI DSS and HIPAA. It complements Horizon’s compliance management capabilities, offering audit trails and reports that make it easier for organizations to maintain compliance across hybrid and cloud environments.

- **Proactive risk management:** ACE detects vulnerabilities within cloud supply chains and CI/CD pipelines, preventing malicious workloads from compromising critical applications. This supports Horizon’s proactive risk mitigation approach, protecting cloud-based business operations from emerging threats.



The **AlgoSec Horizon** platform delivers a unified, application-centric approach that spans both on-premise and cloud infrastructures, providing businesses with the tools needed to confidently navigate the complexities of modern network security.

Results with AlgoSec Horizon

Comprehensive visibility

A single-pane-of-glass view across hybrid environments enhances proactive risk management and accelerates troubleshooting

Reduced manual effort and errors

Automation minimizes human error, improves efficiency, and lowers operational costs, freeing teams to focus on high-priority tasks

Risk-based prioritization

Focus on critical risks tied to business applications reduces alert fatigue and improves incident response times

Continuous compliance

Automated compliance management ensures adherence to evolving regulations, reducing audit failures and the manual compliance burden

Faster application delivery

Intelligent automation accelerates deployments, reduces downtime, and helps businesses stay agile and competitive

Horizon enhances visibility, automates processes, strengthens security, and accelerates compliance and application delivery, **leading to greater agility and reduced risk**

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.

