How Insurance Giant Athora Enhanced Hybrid Cloud Security

INDUSTRY
Financial Services

HEADQUARTERS
Dublin, Ireland

COMPANY SIZE:
1,500 employees

OVERVIEW

Athora is a leading European savings and retirement services group. Athora concentrates on the large and attractive traditional life and pensions market, with an ambition to become a leading provider of guaranteed savings and pensions products in Europe. Athora serves the needs of individual and corporate customers who continue to demand products offering safety of returns and provide innovative M&A and risk transfer solutions to other insurers seeking to enhance their capital position or enact strategic change. Athora's principal subsidiaries are Athora Belgium N.V./S.A. (Brussels, Belgium), Athora Lebensversicherung AG (Wiesbaden, Germany), Athora Italia S.p.A (Genoa and Milan, Italy) and Athora Life Re Ltd. (Bermuda). On December 31, 2023, Athora had AuMA of €73.3 billion, c.1,500 employees and approx. 2.8 million policyholders

OUR SOLUTION

Hybrid Mesh Network Security

"The security capabilities provided by Check Point Cloud Firewall for Azure Virtual WAN have worked just as hoped and expected since installation."

Donal Clissmann, director of infrastructure at Athora

© 2026 Check Point Software Technologies Ltd. All rights reserved.

CHALLENGE

The infrastructure and security teams at insurance and financial services provider Athora understand the complexities in securing cloud native and hybrid-cloud environments. After all, Athora is a cloud-first organization that operates within Ireland, Italy, Belgium. Bermuda, Germany, and the UK. However, as the company grows through acquisition, the security and operations teams must contend with the legacy and diverse IT environments within the companies they acquire. "As much as we are constantly innovating, there are certain systems that we just can't migrate to the cloud," explained Donal Clissmann, director of infrastructure at Athora.

Securing a complex hybrid cloud environment is challenging. To meet that challenge, the Athora team built a layered security architecture that focuses on a zero-trust architecture and is designed to scale. "That's the model in everything we do," said Clissmann.

That approach is essential, as Clissmann detailed, because the pace of change in cloud environments is significantly faster than traditional on-premises infrastructure. This increases the risk of misconfigurations, software vulnerabilities, data breaches, and performance and reliability challenges in cloud environments.

Eoin O'Neill, network lead at Athora, emphasized how relying on user-defined routes to force traffic through firewalls grew complex and error-prone. The team faced challenges scaling their infrastructure as reviewing and updating routing for each necessary change grew more time-consuming and error prone. "Onboarding and managing the Check Point Cloud Firewall for Azure Virtual WAN services, gives the impression the solution is custom-tailored and seamlessly integrated with the service," said O'Neill.

These challenges, among others, underscored the importance of the Athora team finding effective threat prevention and centrally managed secure access control across their virtual LAN and hybrid cloud environment, therefore, we turned to Check Point's cloud firewall.

> I look forward to working with Check Point into the future and leveraging more innovations they will bring our way inside and outside Azure virtual WAN.
>
> Donal Clissmann, director of infrastructure at Athora

© 2026 Check Point Software Technologies Ltd. All rights reserved.

SOLUTION

Clissmann explained that Athora has long depended upon Check Point Software's firewalls to protect its environments, so selecting Check Point Cloud Firewall for Azure Virtual WAN made sense for them to consider. After carefully evaluating its capabilities, the team decided Check Point Cloud Firewall for Azure Virtual WAN would fit their needs.

Check Point Cloud Firewall for Azure Virtual WAN provides enhanced security capabilities for Azure customers using Virtual WAN. It can be deployed directly inside the Virtual WAN hub from Azure Marketplace as a Network Virtual Appliance. This is achieved using an Azure Managed Application, allowing for automated provisioning of cloud security gateways. Check Point Cloud Firewall supplements for Azure Virtual WAN native security capabilities with threat prevention, East-West/North-South network traffic security, secured site-to-site connectivity, and comprehensive management and reporting.

"We've always put security front and center," added Clissmann. "And while we already used Check Point firewalls, we acquired locations around Europe and needed something that would protect our traffic while also helping us manage our increasingly complex environment," he said.

Check Point Cloud Firewall for Azure Virtual WAN helps companies like Athora simplify their network security for Azure Virtual WAN deployments and eases network security challenges. Because Check Point Cloud Firewall for Azure Virtual WAN, cloud security gateways can automatically be provisioned directly from Azure Marketplace using an Azure Managed Application. "By using Check Point Cloud Firewall for Azure Virtual WAN, we hoped to enhance our cloud security while taking full advantage of Azure's scalability and connectivity benefits," he said.

OUTCOME

Check Point Cloud Firewall for Azure Virtual WAN did not disappoint and markedly improved Athora's agility and deployment speed. O'Neill noted how quickly the team can spin up new Azure workloads and make those workloads available to business units within a day — something that previously took weeks.

This choice to deploy Check Point Cloud Firewall for Azure Virtual WAN has also yielded impressive security and reliability results, dramatically simplifying routing processes and enhancing dependability. Clissmann emphasized that Check Point Cloud Firewall provides a "secure by default" posture and that posture substantially reduces the risk of misconfigurations and streamlining network management in their rapidly evolving cloud environment.

Joe McGlynn, senior manager of IT shared services at Athora, highlighted how Check Point Firewall for Azure Virtual WAN has eliminated potential conflicts between the firewall platform and underlying Azure infrastructure – especially in the case of Check Point Cloud Firewall for Azure Virtual WAN. "Previously, we just couldn't route external traffic through Azure securely, not without building some inelegant solutions and then trying to shoe them in. Now, we can securely route traffic through Azure," McGlynn explained.

The team added that because Check Point provides a single platform for managing security policies across cloud and on-premises environments, including identity-based rules, security management is now significantly streamlined. "In comparison to what we had previously, from testing to upgrading our infrastructure-as-a-service, management has become significantly easier," O'Neill said.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

Additionally, Check Point Cloud Firewall for Azure Virtual WAN provides robust threat prevention, protecting against malware, ransomware, and other types of attacks across all network traffic flows, as well as secured site-to-site security and comprehensive analytics. "The security capabilities provided by Check Point have worked just as hoped and expected since installation," Clissmann said.

Check Point Cloud Firewall for Azure Virtual WAN is also critical to Athora's zero-trust security architecture. "Athora is heavily invested in a zerotrust strategy, and because Check Point Cloud Firewall for Azure Virtual WAN is integrated into our identity platform, it assists with this effort," said Clissmann. Check Point Cloud Firewall for Azure Virtual WAN supports zero trust by explicitly verifying all connections, regardless of source or destination, enabling least privilege access, network segmentation, and consistent enforcement of zero trust policies throughout an environment.

By deploying Check Point Cloud Firewall for Azure Virtual WAN hubs, Athora can implement a robust zerotrust architecture that verifies all traffic, limits access, assumes breach, and provides consistent security across their Azure and hybrid cloud environments. This seamless integration enhances Athora's current operations and positions it well for future growth by supporting its cloud-first strategy while accommodating legacy systems from acquisitions.

In conclusion, the Athora team also greatly appreciated how Check Point support rapidly resolved any issues brought to their attention, often within hours or days. "I look forward to working with Check Point into the future and leveraging some more innovations they will bring our way," said Clissmann.

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. is a global cyber security leader protecting more than 100,000 organizations worldwide. Its mission is to secure enterprises' AI transformation. With a prevention-first approach and an open ecosystem architecture, Check Point helps organizations block advanced threats, prioritize exposures, and automate security operations across complex digital environments. The unified architecture simplifies protection across hybrid networks, multi-cloud environments, digital workspaces, and AI systems. Structured around four strategic pillars, Hybrid Mesh Network Security, Workspace Security, Exposure Management, and AI Security, Check Point delivers consistent protection and visibility across multivendor environments, enabling organizations to reduce risk, improve efficiency, and accelerate innovation without increasing complexity.

LEARN MORE

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599
U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391
www.checkpoint.com

© 2026 Check Point Software Technologies Ltd. All rights reserved.
RB August, 2026