Unzer Chooses Fortinet to Protect AWS Workloads and Payment Services

Executive Summary

Unzer, an innovative, modular platform for international payment transactions, debuted in 2020 after a merger of several acquired companies, including Heidelpay. Unzer facilitates the entire spectrum of payment management—from payment processing to customer analytics to risk management—for retail and ecommerce organizations. As such, data security and compliance with regulations like the payment card industry data security standard (PCI DSS) are paramount. Using solutions from Fortinet, the Unzer security team created the Unzer enterprise network with zero-trust network access to protect its workloads on Amazon Web Services (AWS).

A small security team needs a manageable, cloud-based solution

As a new organization made up of recent acquisitions, the Unzer security team saw two paths forward for networking. They could build on existing networks to connect the new branch office, or they could take a cloud approach by establishing an internet connection and use an AWS Virtual Private Network (AWS VPN) to connect to a virtual machine on premises. Unzer determined the cloud approach was the right choice. “As a small security team, I wanted to keep it simple,” said Hooman Ahmadi, network engineering manager at Unzer. “We needed to launch a network in the new branch offices as fast as possible, so I looked for an integrated, cloud-based solution that I could maintain and manage on our own.”

Fortinet solutions secure 28 AWS accounts

Fortinet proved to offer the best solutions for the job. Unzer used FortiManager to centrally manage the branch office network configuration as well as its VPN solutions and perimeter firewalls. Since then, the team has deployed the complete Fortinet Security Fabric to protect 28 AWS accounts and more than 100 evolved packet cores (EPC). Unzer now has two Fortinet FortiGate-VM next-generation firewalls in AWS in two separate Availability Zones. In between them is a Software-Defined Wide Area Network Hub. Also known as SD-WAN, this hub enables Unzer to use a combination of transport services for secure connections. In addition, an Auto Discovery VPN (ADVPN) dynamically establishes direct tunnels that allow more direct connections.

Zero-trust network access protects AWS workloads

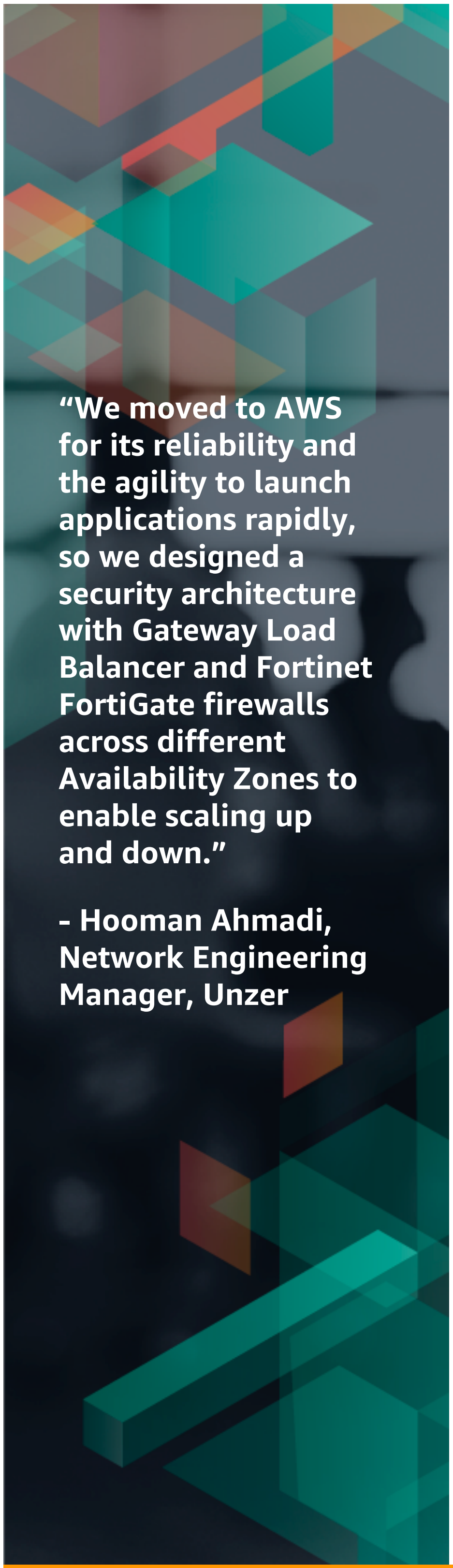
Today, Unzer runs nearly all its workloads—both internal and customer-facing—on AWS. “To provide secure access to our data and services on the AWS Cloud, we adopted the concept of zero-trust network access, which uses a secure SSL VPN into FortiGate firewalls that are connected via

unzer

About Unzer

Based in Germany, Unzer is a fast-growing and innovative FinTech dedicated to revolutionizing transaction management.

> **“To provide secure access to our data and services on the AWS Cloud, we adopted the concept of zero-trust network access, which uses a secure AWS VPN to Fortinet FortiGate firewalls that are connected via AWS Transit Gateway.”**
>
> **- Hooman Ahmadi, Network Engineering Manager, Unzer**



> “We moved to AWS for its reliability and the agility to launch applications rapidly, so we designed a security architecture with Gateway Load Balancer and Fortinet FortiGate firewalls across different Availability Zones to enable scaling up and down.”
>
> **- Hooman Ahmadi, Network Engineering Manager, Unzer**

AWS Transit Gateway and from there, no resources are available until the user is authenticated and authorized,” Ahmadi said. The company’s 800+ employees can work remotely and securely access the company’s SAP system. In addition, external customers can use the Unzer payment platform via publicly available APIs.

Fortinet FortiGate firewalls + AWS = zero cardholder security incidents

Unzer’s payment application is containerized and managed with Amazon Elastic Kubernetes Service (Amazon EKS). Separate FortiGate firewalls protect this cardholder data environment and help ensure compliance with PCI DSS. The FortiGate firewalls have a dedicated Amazon Virtual Private Cloud (Amazon VPC) and use different routing tables to make sure all East-West and North-South traffic passes through them. To ensure users maintain the right level of access to different nodes of the application, the security team uses dynamic objects and tags.

To date, Unzer hasn’t had any security incidents in its cardholder data environment and has consistently passed PCI audits.

Centralized core firewall delivers security without hurting agility

As Unzer grew its footprint in AWS, visibility into and control over its traffic became more challenging. Currently the network engineering team is implementing a centralized solution where every connection goes through an inspection VPC that includes FortiGate firewalls connected to FortiManager and FortiAnalyzer for visibility. Using Gateway Load Balancer (GWLB), the team can also dynamically distribute traffic amongst the firewalls. GWLB works with AWS Auto Scaling groups to deliver elastic scaling to meet on-demand bandwidth needs and eliminate performance bottlenecks.

“We moved to AWS for its reliability and the agility to launch applications rapidly, so we designed a security architecture with GWLB and FortiGate firewalls across different Availability Zones to enable scaling up and down,” Ahmadi said. As Unzer gears up for a centralized core firewall, the team is excited about having a scalable security solution that can be managed from a unified hub.

About Fortinet

Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future.

FORTINET®