Secure Digital Communications Platform, Zivver, Boosts Network Security While Reducing TCO

INDUSTRY
Information Technology & Services

HEADQUARTERS
Amsterdam, Noord-Holland

COMPANY SIZE
51-200 employees

OVERVIEW

Zivver offers a secure digital communications platform, which adds a security and privacy layer on top of an organization's existing email and communication systems. Their innovative solution has earned them recognition by Gartner in the Email Data Protection (EDP) category.

OUR SOLUTION

Harmony
Secure the Workspace

Zivver serves over 6,000 organizations globally, helping to protect their sensitive information, avoid data leaks, and improve compliance.

Zivver, a fast-growing company in the red-hot digital security field, epitomizes the modern work environment. Most of their resources are in the cloud, and their nearly 150-strong workforce is primarily remote and widespread, with a "working from anywhere" policy where employees can work from anywhere around the globe.

> With limited authentication options and role-based access managed capabilities, we were at risk of bad actors exposing internal resources. We needed better segmentation, and better security at the front door.
>
> *Frank Horenberg, Head of IT at Zivver*

CHALLENGE

Zivver's previous network access solution was falling short in two critical areas: security and performance.

From the security perspective, Zivver was looking for a solution that would further enhance protection against potential breaches. They wanted to put in place stronger user authentication and tighter role-based access controls to sensitive internal assets.

From the performance aspect, as Zivver was expanding outside of the Netherlands market, there was a need to speed up connectivity and reduce latency for their global workforce.

"The solution we were using had one gateway in the Netherlands – which made connectivity for workers outside Europe, or on the edges of it, slow to impossible."

Additional challenges Zivver was looking to address were the overhead in manual user provisioning efforts and the cumbersome user authentication process of the previous product they used.

SOLUTION

Zivver set out to find the best secure network access solution for their dynamic and faced-paced work environment: "As our needs grew, we put together a very clear set of requirements."

The IT and security team researched some of the leading solutions in the market and realized that most of them were not fully meeting their needs.

"We looked at some of the popular solutions, but the functionalities that the traditional solutions offered weren't relevant for us."

When they researched Harmony SASE, Frank found that it answered their security and business needs. "We liked the strong product vision and strategy. We were happy to find that this solution fit our needs very nicely."

> For me a good secure networking solution, as boring as it seems, is one I don't have to hear about. As long as I don't have system administrators or users coming to me with questions, problems, and issues – it works.
>
> *Frank Horenberg, Head of IT at Zivver*

OUTCOME

When it came to secure network access for their global workforce, automatic account provisioning System for Cross-domain Identity Management (SCIM), and easy integration with Single Sign-On (SSO) were critical. These would allow remote employee authentication without having to use a certificate, which could potentially be exploited if malicious players got their hands on a stolen device.

It was also extremely important that the secure network connection was stable and continuous. "Having the ability to actually deploy and anticipate growth, especially overseas, and then deploy networks on a global level was important to us." Frank adds "Uptime is also very very important. 50 minutes of downtime means 50 minutes when no one can work. Our developers are dependent on virtual private cloud (VPC) resources. We needed a solution that always works."

Harmony SASE enabled Zivver to automate the onboarding and offboarding of users – processes that were previously manual, cost the company valuable man hours, and were prone to error. Frank can now ensure that new employees have access to the resources they need only, based on their role – per Zero Trust least privileges best practice. Later, when users are offboarded, automated rules ensure access is immediately revoked. "In the case of an incident, access can be cut off immediately, without user intervention. This minimizes risks and saves time."

The single pane of glass dashboard allows Frank to easily produce logs and get insights about all activities on a network level. Frank explains: "If there was a malware infection on a laptop – having the ability to see whether a user was connected at that point to internal resources helps us minimize risk". He adds: "We can quickly detect suspicious behavior, and revoke access automatically while temporarily deactivating the account."

The implementation process went smoothly. As soon as Zivver were happy with the results of their beta testing, implementing across the entire organization was easy. "When we went live, it was simply a matter of expanding the user group from 10 to 150. No additional configuration was needed"

Frank also has peace of mind knowing that when the company's growth and priorities change, it will be easy to address those challenges since scaling up for additional employees and expanding with additional capabilities is easy.

Zivver's security requirements are of the highest level as a cyber security company.

We enabled Zivver to achieve the level of security they need and their customers expect. "Using this solution not only drives value by supporting staff in creating secure network access to work but also by adhering to compliance such as SOC 2 Type II and local legislation. This solution proves to our stakeholders that not only is our digital communications solution secure, but also that we lead the way in network security, following our own security by design and Zero Trust principles."

Another important business enabler is a fast and stable connection enabled by the global private backbone. "It's a necessity for our organization, allowing us to prevent network security from becoming a blocker both to productivity and commercial business."

With us, Frank can address the many network security challenges that today's modern enterprise faces. He can ensure the company has a secure and stable network that workers can rely on, no matter where they connect from–or when.

Frank is now confident that if a malicious attack attempt is made, he can quickly detect and address it, keeping his users and network safe.

Frank knows that as the company grows, we will enable him to grow the network and meet any future demands.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Platform Services for collaborative security operations and services.

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

www.checkpoint.com

September 2024 – RB