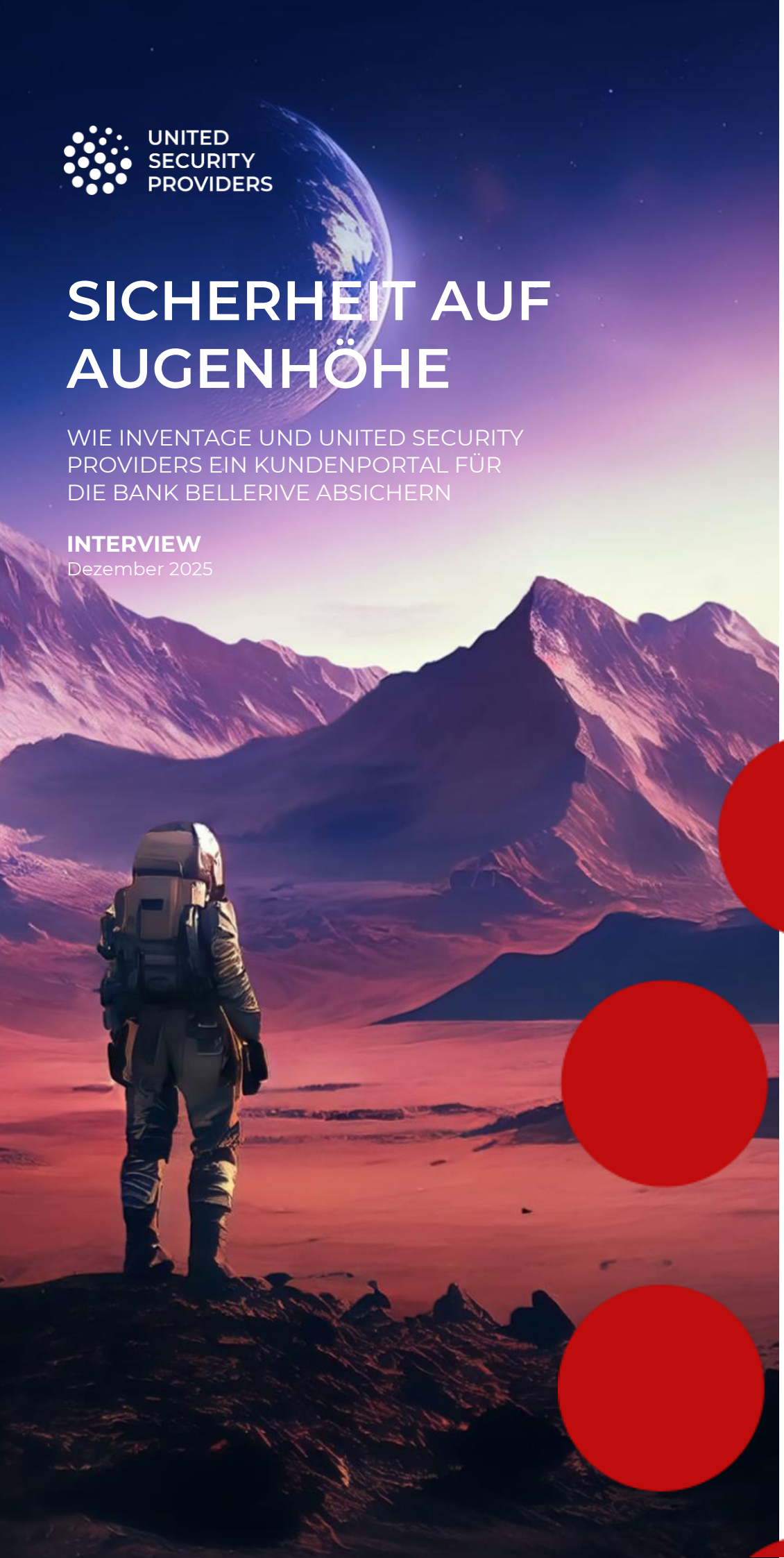
UNITED SECURITY PROVIDERS

SICHERHEIT AUF AUGENHÖHE

WIE INVENTAGE UND UNITED SECURITY PROVIDERS EIN KUNDENPORTAL FÜR DIE BANK BELLERIVE ABSICHERN

INTERVIEW
Dezember 2025



Die Digitalisierung im Bankenumfeld stellt hohe Anforderungen an Sicherheit, Compliance und Flexibilität. Gemeinsam mit Inventage realisierte die Bank Bellerive ein modernes Kundenportal – schlank, stabil und regulatorisch abgesichert. Die Security-Architektur basiert auf Core WAAP von United Security Providers. Im Interview erklärt Stefan Stolz, Mitgründer und Geschäftsführer von Inventage, wie die Lösung entstand – und warum moderne Applikationssicherheit heute nicht mehr am Perimeter beginnt.

STEFAN STOLZ
GESCHÄFTSFÜHRER
INVENTAGE AG

HERR STOLZ, BEGINNEN WIR MIT INVENTAGE: WAS IST EUER KERNGESCHÄFT?

Wir sind spezialisiert auf Individualsoftware, Kundenportale und Cloud-Lösungen. Daraus ist auch unser Produkt Uniport entstanden – eine modulare Plattform, die wir bei verschiedenen Kunden einsetzen, darunter auch bei der Bank Bellerive. Daneben bringen wir tiefes Engineering-Know-how im Bereich IAM mit.

WER SIND IHRE KUNDEN?

Unsere Kundschaft kommt mehrheitlich aus dem Finanzsektor – u. a. VP Bank, Julius Bär, Glarner Kantonalbank und Thurgauer Kantonalbank oder Albin Kistler. Besonders relevant im Kontext dieses Interviews: die Bank Bellerive.

WELCHEN FOKUS HAT DIE BANK BELLERIVE?

Die Bank Bellerive ist eine kleinere, exklusive Zürcher Privatbank. Sie gehört der Graubündner Kantonalbank und den grössten Kunden der Bank Bellerive. Sie ist spezialisiert auf individuelle Vermögensverwaltung und zeichnet sich durch Kundennähe, Transparenz und persönliche Betreuung aus. Ihre Kunden sind meist wohlhabende Privatpersonen.

WAS WAR DER AUSLÖSER FÜR DAS PROJEKT DER BANK BELLERIVE?

Die Bank Bellerive hatte den Wunsch, ihren Kunden einen modernen digitalen Zugang zu ihren Vermögenswerten zu bieten – also ein Kundenportal. Dafür wurde eine kompakte, aber hochsichere Lösung mit überschaubaren Betriebs- und Entwicklungskosten gesucht.

WELCHE HERAUSFORDERUNGEN ERGABEN SICH DABEI?

Die Bank Bellerive hat kein eigenes IT-Team. Damit waren wir der zentrale Partner – zuständig für Architektur, Umsetzung und Betrieb. Klar war für uns: Wenn wir ein solches Portal betreiben, braucht es zwingend Schutz auf mehreren Ebenen. Unsere Applikation basiert auf einer Zero-Trust-Architektur, aber das allein reicht nicht. Für den vorgelagerten Schutz – also Traffic aus dem Internet – war eine containerisierte WAAP die richtige Ergänzung.

WARUM FIEL DIE WAHL AUF CORE WAAP?

Sicherheit ist bei uns seit jeher ein integraler Bestandteil der Architektur – kein nachträgliches Add-on. Seit über 25 Jahren entwickeln wir Systeme mit höchsten Anforderungen an Sicherheit und Datenschutz. Für uns war klar: Wir liefern Applikationen nur mit vorgelagerter Security aus – die WAAP ist fester Bestandteil. Core WAAP passt ideal zu dieser Philosophie: containerisiert, schlank und in unsere Pipelines integrierbar.

Unsere Plattform Uniport wurde nicht nur als Zero-Trust-Architektur, sondern von Grund auf auch als Microservice-Architektur entwickelt. Die Lösung wurde also in mehrere dedizierte Microservices aufgebrochen. Das war ein bewusster Schritt in Richtung Flexibilität, Modularisierung und Betriebsstabilität.

Früher wurde die Applikation entwickelt und erst am Ende ergänzte das Security-Team eine vorgelagerte WAF. Und das war dann meistens ein riesiger Aufwand, weil diese WAFs sehr generisch funktionieren mussten. Sie konnten die Applikation gar nicht wirklich kennen.

Das war ein richtiges Bottleneck. Änderungen mussten abgestimmt, getestet und wieder freigegeben werden. Es hat alles verzögert. Die WAF wurde zum Nadelöhr, weil sie zentral verwaltet wurde und nicht agil mitentwickelt werden konnte.

> **Heute, mit Core WAAP, ist das anders. Wir können die Sicherheitslogik zusammen mit dem Code versionieren, testen und ausrollen.**

Das bringt uns eine verbesserte Geschwindigkeit und Qualität sowie eine signifikante Aufwandsreduktion.

Natürlich hätten wir das Portal auch mit einer klassischen vorgelagerten WAF schützen können, aber das hätte schlicht nicht zu unserem Architektur- und Betriebsmodell gepasst. Eine solche Perimeter-WAF wäre viel zu starr gewesen. Wir wollten eine Lösung, die sich service-nah und containerisiert betreiben lässt. Core WAAP war dafür ideal. Jeder Microservice erhält seinen eigenen Schutz durch eine dedizierte WAAP, die Regeln lassen sich präzise und granular definieren, statt ein unübersichtliches Regelset für alles zu pflegen. Mit der Perimeter-WAF hat dies immer einen immensen Aufwand für uns bedeutet, um das Regelset «zurechtzubiegen».

WELCHE WEITEREN VORTEILE HAT DIE LÖSUNG GEBRACHT?

> **Ein zentraler Vorteil von Core WAAP ist die nahtlose Integration in moderne Entwicklungs- und Betriebsprozesse.**

Durch das Prinzip «Shift Left» wird Security bereits in frühen Phasen des Software Development Lifecycles (SDLC) berücksichtigt. Die WAAP-Konfiguration ist als Code verwaltbar, lässt sich versionieren und in CI/CD-Pipelines einbinden. Dadurch können wir Sicherheitsrichtlinien testen, bevor sie in Produktion gehen, was die Qualität erhöht und spätere Korrekturen reduziert.

Ein weiterer Vorteil von Core WAAP ist, dass die Lösung problemlos mitwachsen kann. Es funktioniert für kleine Kunden mit schlanker Infrastruktur genauso wie für grössere Setups mit komplexen Anforderungen. Diese Skalierbarkeit ohne Architekturbruch ist für uns ein echter Pluspunkt.

Das Preismodell ist flexibel und passt auch zu kleineren Kunden. Wir konnten die Hosting-Kosten gegenüber einer Perimeter-WAF mit Core WAAP um Faktoren reduzieren.

Zudem: Das gesamte Portal – inklusive WAAP – läuft containerisiert auf einem Kubernetes-Cluster. Das Setup ist schlank, unabhängig von Hyperscalern und jederzeit portierbar. Sollte die Bank oder Inventage entscheiden, den Provider zu wechseln, wäre dies in Rekordzeit möglich. Diese Unabhängigkeit von Hyperscalern ist heute Gold wert – gerade für Banken. Das muss die WAAP mitmachen, sonst wäre dies nicht möglich.

GAB ES KONKRETE FUNKTIONALITÄTEN, DIE EUCH POSITIV ÜBERRASCHT HABEN?

Ja, insbesondere die automatische Regelgenerierung mit dem hybriden Security-Model. Das System erkennt, welche Requests legitim sind, und schlägt daraus ein initiales Regelset vor. Damit sparen wir enorm Zeit in der Konfiguration. Auch die Möglichkeit, die WAF komplett via Code zu konfigurieren, ist für uns essenziell. UI-only-Lösungen wie bei anderen Anbietern sind für uns schlicht nicht mehr zeitgemäss.

WIE WAR DIE INTEGRATION IN EURE UMGEBUNG?

Reibungslos. Core WAAP liess sich als Containerlösung direkt in unsere Infrastruktur integrieren. Wir betreiben das gesamte Portal auf Kubernetes. Auch die vier eingesetzten WAAP-Instanzen fügen sich nahtlos ein.

WELCHE ROLLE SPIELTE USP DABEI?

> **Die Zusammenarbeit mit USP war offen, lösungsorientiert und partnerschaftlich.**

Wir konnten Herausforderungen rasch adressieren und hatten das Gefühl, wirklich mitgestalten zu können. Wenn wir unseren Partner auf Augenhöhe und nah angehen können, ist das für uns Gold wert.

WIE HAT DIE BANK BELLERIVE AUF DIE LÖSUNG REAGIERT?

Die Bank Bellerive hat ein tolles Kundenportal mit hervorragendem Schutz. Sie hat uns in puncto Security komplett vertraut. Sie wusste: Die Lösung ist professionell und nach höchsten modernen Standards geschützt. Sie mussten sich nicht darum kümmern.

WÜRDET IHR EUCH IM RÜCKBLICK WIEDER FÜR CORE WAAP ENTSCHEIDEN?

Unbestritten! Es hat genau gepasst – architektonisch, technisch, kulturell.

GIBT ES TECHNOLOGIEN ODER KONZEPTE, DIE SIE FÜR KÜNFTIGE PROJEKTE IM ZUSAMMENSPIEL MIT CORE WAAP BESONDERS SPANNEND FINDEN?

Inventage setzt bei seiner Plattform bereits auf GraphQL – unter anderem, um Daten präzise und effizient bereitzustellen. Mit dem Release 1.4 unterstützt Core WAAP nun auch GraphQL nativ. Für Inventage eröffnet sich damit die Möglichkeit, ihre bestehenden API-Strukturen noch gezielter abzusichern – ein klarer Vorteil bei wachsender Komplexität. In Kombination mit feinjustierter API-Absicherung durch Core WAAP verspricht GraphQL nicht nur bessere Performance, sondern auch mehr Kontrolle, weniger Overhead und eine optimierte User Experience.

WAS WÜRDEN SIE EINEM ANDEREN SOFTWAREANBIETER MIT ÄHNLICHEN HERAUSFORDERUNGEN RATEN?

> **Die Kombination aus container-nativer WAAP, Zero-Trust-Architektur und Microservices bietet enorme Vorteile**

– insbesondere im Finanz- und Compliance-Bereich. Wer heute noch auf klassische Appliances setzt, macht sich unnötig abhängig und unflexibel.

Für uns ist Core WAAP integraler Bestandteil unserer Lösung geworden. Gerade bei sensiblen Daten – ob im Banking, in der Vorsorge oder im Gesundheitswesen – sollte diese Art von Schutz keine Option, sondern Standard sein.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

swiss made software

UNITED SECURITY PROVIDERS

ZERO TRUST UNIVERSE

Besuchsadressen
Bern | Stauffacherstrasse 65/15, 3014 Bern
Zürich | Baslerpark, Baslerstrasse 60, 8048 Zürich

+41 31 959 02 02
info@united-security-providers.ch
united-security-providers.ch