LINK11

CASE STUDY

Quipu
Part of the ProCredit Group

www.link11.com

Security That Adapts to the Application: How Quipu Found a Unique Solution with Link11

In the high-stakes world of financial technology, the standard approach to security is often insufficient. For Quipu GmbH, the IT backbone of the ProCredit Group, relying on off-the-shelf cloud protection measures left critical gaps in their defense. Faced with sophisticated web attacks and a market of vendors offering rigid, standardized solutions, Quipu sought a partner who could adapt to their complex infrastructure, not the other way around.

The Digital Engine of ProCredit Group

Founded in 2004, Quipu GmbH serves as the dedicated IT service provider for the ProCredit Group, a development-oriented commercial banking group operating primarily in Eastern Europe and Germany. Headquartered in Frankfurt, Quipu has evolved from a support unit into an advanced technology company responsible for the entire digital lifecycle of the group's operations: from Banking Software and Card Payment Services to cloud and infrastructure.

Quipu's philosophy centers on "made-to-fit solutions". The company designs IT architectures that respect local market requirements while leveraging global expertise. This internal mission to build tailored solutions makes them particularly sensitive to the quality of their own vendor relationships - they expect the same level of adaptability they provide for their clients.

With a strategy centered on providing a fully digital banking experience, high availability is not negotiable. Almost all client interactions occur via the internet, making their front-end services the lifeline of the bank's daily business. In this environment, downtime translates immediately to lost revenue and eroded customer trust.

When Cloud-Native Protection Falls Short

Initially, Quipu's front-end services were hosted in the cloud, protected by the provider's native security features, including WAF and rate-limiting. The team operated under the assumption that this standard layer of defense was sufficient to repel common threats.

However, reality struck when attackers managed to bypass these defenses with relatively small-scale bot attacks, bringing critical services down. The native tools proved too blunt for the precision required. To mitigate ongoing attacks, Quipu's security team was forced into a reactive corner: they had to manually decrease rate limits or block traffic from entire countries. While this stopped the bots, it also blocked legitimate customers, effectively achieving the attacker's goal of service denial.

When Quipu turned to their cloud provider for a permanent fix, the response was alarming. "The answer was that there is no silver bullet," stated Borut Lape, Senior Cybersecurity Officer at Quipu. Consequently, the team had to secure every component of the infrastructure separately instead of relying on a comprehensive solution. It was an enormous manual effort without any security guarantee.

Escaping the „Cookie-Cutter" Trap

As Quipu defined the requirements for a new security architecture, certain criteria emerged as essential; they were factors that would ultimately determine which vendors could realistically serve their needs.

1 **The Need for a Fully Managed Service**

Quipu had previously experimented with on-premises WAF appliances but found the operational overhead unsustainable. Maintaining complex rule sets required specialized knowledge that was easily lost when key staff members left the company. „We didn't have dedicated team members to manage it. If they're trained but do not work daily with the solution, the knowledge is rarely at the level that it should be," explained Borut Lape. They needed a partner to take over this complex task.

2 **Custom Ports as Key Differentiator**

A critical technical requirement was the support for custom ports. Quipu's environment utilized specific ports beyond the standard 80 and 443. While Quipu's IT architecture was valid and functional, many major hyperscale vendors simply could not support it, offering only rigid, standardized configurations.

3 **Compliance & Trust**

As a financial service provider, strict adherence to PCI DSS, GDPR, and DORA regulations was mandatory. The ideal partner needed to offer an authentic and high-quality approach to data privacy and regulatory compliance.

A Unique Fit in a Rigid Market

Quipu evaluated several top market vendors but encountered a landscape of rigidity. Faced with complex pricing structures and providers who preferred selling their standard solutions rather than addressing customer wishes, Quipu felt not taken seriously.

Link11 stood out by offering what Sean Power, Solution Engineer at Link11, describes as a "bespoke" solution: "Quipu needed a solution that could adapt and complement their needs." Beyond this technical flexibility, Link11 demonstrated a welcoming, customer-first attitude that made Quipu feel understood and prioritized from the start. Rather than forcing the IT service provider to redesign their application to fit the security tool, Link11 customized its protection to fit the client's reality.

This flexibility allowed Quipu to secure their custom port environments without re-engineering their entire infrastructure. Link11's solution comprised a solid 75% standard product base, with the remaining 25% being customized or built from scratch to meet Quipu's exact needs.

A Partnership Built on Deep-Rooted Trust

The decision for Link11 also went beyond technical specifications; it was about leveraging a foundation of proven reliability. Link11 was already a trusted partner for Quipu, successfully providing ISP and DDoS protection services. Expanding this relationship to cover critical Web Application Security was a logical evolution, grounded in years of transparent communication and stability.

This pre-existing trust was solidified during the implementation of the new WAAP solution. In an industry often characterized by anonymous support queues, Link11 provided a

"With Link11 we received a very personal approach, a very human relation."

Borut Lape, Sr. Cybersecurity Officer Quipu

dedicated engineer who effectively became an extension of Quipu's internal team. This went beyond simple support - it ensured that the specific nuances of Quipu's infrastructure were understood deeply, rather than just learned superficially for a single ticket.

Borut Lape highlights this contrast between transactional vendors and a true partner: "With Link11 we received a very personal approach, a very human relation." For Quipu, this translated directly into operational confidence: knowing that the people protecting their infrastructure are as invested in its stability as they are.

From Reactive Firefighting to Proactive Resilience

The transition to Link11's managed service has fundamentally shifted Quipu's security posture from reactive to resilient.

Operational Freedom:
Instead of having to spend resources on manual configurations and acute threat defense, the internal team is effectively freed from this operational burden by Link11's experts.

Collateral Damage Avoidance:
The solution ensures that attacks are mitigated in the cloud, never reaching Quipu's data center. This prevents bandwidth saturation and collateral damage to other systems that typically occur with on-premises appliances.

Strategic Peace of Mind:
Moving away from the perceived security of the past, Quipu now operates with a protection layer that is actively managed and guaranteed, allowing them to focus on their core mission: digital innovation for the banking sector.

Partnership in Practice: Ensuring Long-Term Stability

The implementation is currently in a prolonged onboarding phase. This is a deliberate strategy to ensure safety and precision over speed. This careful rollout, supported by Link11, underscores the nature of the partnership: it is not about a quick fix but about long-term stability.

For other organizations facing similar challenges, Borut Lape offers clear advice: "Analyze your infrastructure in detail and dedicate time to testing the human side of the provider collaboration, not just the paper specs."

With Link11, Quipu found more than just a vendor; they found a partner capable of building a security shield that adapts to their unique digital footprint. Their journey marks a decisive transition from reactive damage control to a proactive, fully managed security posture, proving that in the world of critical infrastructure, personal support and bespoke engineering are the ultimate defense. This comprehensive approach ensures that ProCredit's banking services remain open for business, no matter the threat.

"Analyze your infrastructure in detail and dedicate time to testing the human side of the provider collaboration, not just the paper specs."

Borut Lape, Sr. Cybersecurity Officer Quipu

Quipu is a German IT service provider that has been developing custom-tailored solutions for banking software, card payment systems, and digital financial infrastructure. The company operates a global network of secure IT systems for banks and financial institutions, including the ProCredit banking network. Quipu is PCI-DSS certified and provides payment solutions as well as cloud infrastructure "Made in Germany" that meet the highest security and compliance standards.

Link11 is a German IT security provider specializing in DDoS protection and cyber resilience. The company operates a high-performance, AI-poweredprotection system that detects and automatically defends against attacks in real time. Link11 is BSI-certified, ISO 27001-compliant, and offers security solutions "Made in Germany" that are used worldwide.

Link11 GmbH | +49 69 5800492677 | sales@link11.com | www.link11.com