GFT

Pioneering Secure Digital Banking with GFT and Palo Alto Networks

DIGITAL REPORT 2024

IN ASSOCIATION WITH:

paloalto® NETWORKS

PIONEERING SECURE DIGITAL BANKING WITH GFT AND PALO ALTO NETWORKS

WRITTEN BY:
LOUIS THOMPSETT

PRODUCED BY:
MATT ANSELL

Dean Clark, Chief Technology Officer for GFT, provides a unique insight into the creation of Salt Bank and GFT's work with Palo Alto Networks Prisma Cloud

With a history spanning over 35 years, GFT has distinguished itself in the crowded field of technology providers by focusing on key platforms and services that support critical activities within banks and insurers.

Dean Clark, Chief Technology Officer for GFT UK, has been at the forefront of the company's transformation over the past five years.

During this time, GFT has evolved from its German roots into a global data and modern platform engineering services provider, specialising in the financial services sector.

"At GFT, we typically focus on hiring and training engineers with core domain expertise, not just technology expertise," says Dean.

This strategy has paid dividends. Despite global market challenges, GFT has outpaced many of its competitors.

Its strength lies in its ability to bridge the gap between legacy systems and cutting-edge technology. Today, it works with banks to support their cloud transformation strategies, as more organisations see the value of shifting away from their centralised mainframes.

While, in the past few years, some legacy institutions have been resistant to change, market pressures are forcing even the most conservative institutions to reconsider their technological strategies.

Dean notes: “Consumers want mobile-first banking. The new wealthy don’t want to pick up and speak to a wealth manager. They want an app on their phone. This consumer trend is forcing more legacy players to think about their new technology strategy and push for change.”

The security challenge of forming new digital banks

Indeed, while shifting core operations to the cloud represents an exciting prospect, it brings security concerns to the forefront. While many banks are adopting a gradual approach to cloud adoption by operating multi-cloud hybrid models, new digital banks are being formed fully on the cloud.

GFT has a partnership with Engine by Starling, the technology arm of digital bank Starling Bank, which provides a cloud-native and flexible SaaS banking platform to not only enable cloud transformation, but one where security is assured by design.

When creating next-gen digital banking platforms, one of the pivotal security challenges is securing the cloud infrastructure, built predominantly using Infrastructure as Code (IaC). It’s about ensuring it embodies coding best practices and is devoid of vulnerabilities and misconfigurations.

This security must also reach consumer portals – and be meticulously embedded into digital banking mobile apps that ensure compatibility and security across iOS and Android platforms.

This approach, inherent in the design of Engine, focuses on pre-empting security vulnerabilities and establishing a robust defence against potential breaches, all whilst providing an engaging and reliable user experience.

> **“We typically focus on hiring and training engineers with core domain expertise, not just technology expertise”**
>
> **DEAN CLARK**
> CHIEF TECHNOLOGY OFFICER, GFT

Salt Bank: A secure digital banking success story

GFT has already leveraged Engine by Starling in the creation of Salt Bank, a next-gen digital bank operating in Romania. Built and debuted in under 12 months, the founding of Salt Bank represents more digital banking opportunities for consumers in emerging markets while highlighting the reality that new digital offering can go to market at a rapid pace.

For Salt Bank, security was a cornerstone in its creation, not an add-on. From inception, GFT and its partner Palo Alto Networks Networks incorporated leading security features, such as zero trust architecture, threat modelling, cloud security posture

DEAN CLARK

TITLE: **CHIEF TECHNOLOGY OFFICER**

INDUSTRY: **IT SERVICES AND IT CONSULTING**

LOCATION: **UNITED KINGDOM**

Dean is responsible for the technology strategy for GFT, with a heavy focus on cloud and new innovative technologies. His focus is on identifying areas of customer business that can be improved via transformation or rationalisation.

Dean’s experience has seen him work on complete cloud migrations for a UK retail bank, Head of Web Engineering for an investment bank, and Head of Technology for a managed hosting provider. This varied experience brought him to GFT where his combination of banking, insurance and IT leadership have been perfectly placed.

management and security operations automation by design.

This anticipatory strategy involved the weaving of advanced security measures into the fabric of the bank's cloud infrastructure, providing robust defence against the developing landscape of digital threats.

The results speak for themselves. Launched in 2023, Salt Bank has exceeded its annual target of onboarding 230,000 customer by the end of 2024.

The bank offers a current account paying 3% interest (for transactors above a certain limit), digital wallet compatibility, mixed-term deposits, a multicurrency card (supportin 17 different currencies) and a savings account.

"Customers appreciate the simplicity and speed of onboarding, with an average time of less than seven minutes to create a live account," says Dean.

He adds: "To achieve this level of customer satisfaction, GFT harnessed its global delivery model across 18 nationalities to maintain momentum on a highly complex and diverse build and deployment, demonstrating the deep expertise required to create a truly integrated and innovative new bank."

SALT BANK: A TRIUMPH OF COLLABORATION

Salt Bank was launched just a year after the project began. The new retail bank debuted with a current account paying 3% interest (for transactors above a certain limit), digital wallet compatibility, mixed-term deposits, a multicurrency card (supporting 17 different currencies), and a savings account.

By all measures, Salt Bank's launch has been an outstanding success. The objective to onboard 230,000 new customers by the end of 2024 was almost achieved within just a month of launch, with 200,000 new customers joining within a month. Customers appreciate the simplicity and speed of onboarding, with an average time of less than seven minutes to create a live account.

Following the launch, there was an unprecedented number of customers signing up each day, and the systems managed the process faultlessly. Salt Bank has stated its objective to onboard 1 million customers within three years of operation; early signs are that they are likely to reach this business case milestone far sooner.

Salt Bank's success is a triumph of collaboration in the digital age, demonstrating the accretion potential of successfully integrating many leading industry platform solutions.

GFT harnessed its global delivery model across 18 nationalities to maintain momentum on a highly complex and diverse build and deployment, demonstrating the deep expertise necessary to create a truly integrated and innovative new bank.

For Salt Bank, security was a cornerstone, not an add-on. The goal was to set a new benchmark for security and scalability and to build customer-centric, cloud-first solutions where speed and responsiveness were imperative.

“Consumers want mobile-first banking. The new wealthy don’t want to speak to a wealth manager. They want an app on their phone”

DEAN CLARK
CHIEF TECHNOLOGY OFFICER, GFT

Building banks securely by design with Palo Alto Networks Networks Prisma Cloud

While Engine by Starling provides the SaaS platform for digital banks, the question remains how GFT ensures its cloud platform is secure by design?

Step in Palo Alto Networks Networks Prisma Cloud platform, which is central to GFT’s success in building secure digital banks.

A single-vendor, cloud-native application protection platform CNAPP), Prisma Cloud is designed to protect applications from code to cloud across any public, private, hybrid or multi-cloud environment.

Dean recounts his initial encounter with Prisma Cloud at AWS re:Invent: “When I was looking at it at the time, it just seemed to offer a product that was more mature than a lot of the others in the market.”

For Salt Bank, GFT implemented Palo Alto Networks Networks Prisma Cloud to provide a ‘single pane of glass’ view of the entire IT estate as it was built.

This approach enabled GFT to continuously monitor cloud resources and workloads for misconfigurations and vulnerabilities, quickly scaling security to match the cloud infrastructure.

What's more, Prisma Cloud's Cloud Security Posture Management (CSPM) feature allows GFT to not only monitor posture, but also detect and remediate risks, and maintain compliance across the cloud environment.

The Cloud Infrastructure Entitlement Management (CIEM) from Prisma Cloud provides control over permissions across multi-cloud environments, essential for maintaining a secure access model.

Furthermore, Prisma Cloud's agentless workload scanning enables the scanning of hosts, containers, Kubernetes and serverless environments for vulnerabilities and threats. Its API visibility helps discover, profile and protect APIs across cloud-native applications, a crucial aspect of modern digital banking platforms.

PALO ALTO NETWORKS PRISMA CLOUD OFFERS A UNIFIED APPROACH

Prisma Cloud is a comprehensive cloud-native application protection platform (CNAPP) designed to secure applications from code to cloud across various cloud environments. It offers a unified approach to security, integrating multiple capabilities into a single platform to provide best-in-class protection. The platform focuses on three main areas:

1. Risk Prevention: It shifts security left by integrating with engineering ecosystems to prevent risks and misconfigurations before they reach production. This includes IaC security, secrets security, CI / CD security and software composition analysis and more.

2. Visibility and Control: Prisma Cloud provides continuous monitoring and control over cloud assets, including Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), agentless workload scanning, API visibility, cloud discovery and Data Security Posture Management (DSPM).

3. Runtime Protection: It offers real-time protection for cloud workloads, web applications and APIs. This includes cloud threat detection, host security, container security, serverless security, web application and API security.

Prisma Cloud is powered by Code to Cloud intelligence, which connects insights from the development environment through to application runtime. This helps in contextualising alerts, prioritising critical risks and offering remediation guidance. The platform aims to reduce risk, prevent breaches, improve DevSec collaboration, increase efficiency and enhance compliance and security posture across multi-cloud environments.

Dean highlights the importance of this comprehensive approach: “Our goal was to set a new benchmark for security and scalability and to build customer-centric, cloud-first solutions where speed and responsiveness were imperative.”

Integrating security throughout the development process

GFT’s security-first approach is integrated into every stage of its work with clients. As Dean explains: “We start having those security conversations as part of the design of the neobank. What are the customer’s requirements? We’ll drill down into their business rationale, their technology requirements but we’ll also ask them about their security risk posture.”

To fortify the codebase for application code and backend microservices, GFT leverages GitHub’s advanced security capabilities.

These are embedded into the build and deploy pipelines for static code analysis and secrets scanning, alongside Prisma Cloud’s Cloud Code Security for scanning and hardening IaC templates against misconfigurations.

Dean elaborates on the use of GitHub: “Even if you use some of the Atlassian products like Bitbucket, it’s GitHub under the hood. So it made sense to focus our engineers’ expertise and training on and around how to get the most out of GitHub.

“We make sure that our engineers can use all of the functionality. We make sure they understand the full scope of the feature set.”

Enhancing security with NIST Framework and Palo Alto Networks Networks Cortex XSOAR

GFT has also embraced the National Institute of Standards and Technology (NIST) framework to bolster its security design processes, something Dean describes as a "sensible approach to securing a business' design and infrastructure".

He outlines the five core activities of NIST: Identify, Protect, Detect, Respond and Recover. Incorporating these principles into its design process, GFT applies them both to overall systems and individual components.

Dean expands: "As part of our design process, we've adopted a similar approach for both the overall systems design when looking at it holistically and for each of the individual components that go into the design

"We regularly run through NIST's compliance tools with some of our designs to make sure we've not missed anything."

To enhance its security framework, GFT leverages Palo Alto Networks Networks Cortex XSOAR alongside native AWS security tools.

AWS WAF and Shield are primarily used as a defence against web attacks and DDoS assaults, while the AWS Security Hub provides a centralised perspective on security and compliance across AWS accounts. AWS GuardDuty plays a critical role in the overall threat detection strategy, monitoring for malicious or unauthorised activities on the AWS environment.

For incident management, Cortex XSOAR is integrated to automate responses and orchestrate security processes.

"Our goal was to set a new benchmark for security and scalability and to build customer-centric, cloud-first solutions where speed and responsiveness were imperative"

DEAN CLARK
CHIEF TECHNOLOGY OFFICER, GFT

This integration enables the consolidation of alerts, analysis acceleration and the ability to swiftly respond to security incidents, thereby minimising the time to remediation and optimising the efficacy of the overall security operation.

Implementing a 'Zero trust' philosophy

These measures are capped off by Salt Bank's 'Zero trust' philosophy, which GFT has implemented within the bank's ecosystem as cloud components are developed and begin interacting with others in-cloud components and services, and with other third parties.

Proper demarcation is established between applications and the users interacting with the cloud resources, while the principle of 'no access being permitted without identification' is rigorously enforced. Once access is established, monitoring and logging setup are implemented to inspect the traffic interacting with the system.

To enhance security further, mutual transport layer security (TLS) is used as a key design principle when authenticating with any third party over the internet.

To implement least privilege access, GFT builds in segmentation, not only on the network layer but also with the cloud resources that are accessed, by leveraging AWS resource-based policy restrictions.

The future of secure digital banking

The integration of advanced security measures, as demonstrated in GFT's work with Salt Bank, points to a near future where digital banks are built and deployed securely and at scale.

GFT's partnership with Palo Alto Networks Networks and its utilisation of Prisma Cloud represents a successful approach to addressing the complex security challenges in digital banking.

"Our collaboration with Palo Alto Networks Networks allows us to offer a level of security that's not just reactive, but proactive and deeply integrated into every aspect of a digital bank's infrastructure," Dean notes.

The Prisma Cloud solution aims to provide comprehensive security coverage for the entire lifecycle of digital banking applications. This approach is particularly relevant as the financial sector faces increasingly sophisticated cyber threats.

As consumer demands for mobile-first banking solutions grow, and regulatory requirements become more stringent, the ability to build secure, scalable digital banking platforms will likely be a key differentiator in the market.

While meeting customer demands is key for digital banks, Dean warns that "the increasing importance of cybersecurity in digital banking is clear".

"The challenge for the industry will be to balance robust security measures with user experience and innovation. It's a complex task, but one that's crucial for the future of digital banking," he concludes.

GFT

6th Floor
7 Bishopsgate
London
EC2N 3AR

+44 (0)20 3372 9200

gft.com/uk/en

POWERED BY:

BizClik