OPSWAT.

Financial Services Sector Case Study

Critical Infrastructure Protection



Swiss Re makes security a focal point of their digital transformation, partnering with OPSWAT MetaDefender® to secure their web applications.

Financial reinsurance company Swiss Reinsurance Company Ltd is one of the world's leading providers of reinsurance, insurance and other forms of insurance-based risk transfer.

Cybersecurity is of paramount importance to safeguard the enormous amount of client personal data that Swiss Re manages. Swiss Re also needs to ensure compliance with existing and emerging Financial Services regulations and cybersecurity standards, including the Swiss Financial Market Supervisory Authority (FINMA) for financial crime prevention and the General Data Protection Regulation (EU GDPR) to ensure data privacy.

Swiss Re is heavily focused on container deployments and automation to maximize their security posture and system uptimes. Beyond that, they are committed to sharing their experience and expertise back to the open-source and broader financial communities. This innovative approach also creates some security challenges as new technologies can lead to new attack vectors. Swiss Re felt it was imperative that they create solutions that protect against malware threats by adopting leading-edge technologies and the capabilities to support secure micro-services platforms.

> *"Swiss Re is committed to the open-source community and raising the security profile of the entire sector. We are embracing the future, and OPSWAT's commitment to broad cloud-native support for their products is very complementary to our security vision. The MetaDefender Platform provides Swiss Re with a comprehensive, easy to deploy and maintain solution that meets regulatory compliance requirements and eliminates the risk of malware entering the organization."*
>
> Raymond Bucher
> Director/Cloud Architect at Swiss Re

To secure their customer data and other business document traffic, Swiss Re uses MetaDefender ICAP Server deployed in Azure Container Instances (ACI). The solution is integrated with an API Gateway which manages and secures the APIs residing in those containers. When the need arises, the solution can easily scale or be deployed to other platforms.

01

Protect the network—scan any file uploaded by partners or customers at the network edge, before it reaches their web applications

02

Ensure the security of client personal data to meet FINMA and GDPR requirements

03

Automation and ease of integration-configure, set up, and manage the deployment with minimal effort

CHALLENGES

Securing Customer File Uploads on a Global Scale

To enable their customers, partners and employees to conveniently submit and transfer electronic files, Swiss Re created web portals and applications where files could be easily uploaded. This introduced the risk of infected files entering their secure network via one of their web applications. To mitigate the security and compliance risks, Swiss Re needed to ensure that the uploaded files did not contain any malicious content. The primary requirement was to allow incoming files from any outside source and render them 100% safe to consume without adding latency or impacting the workflow or availability of files. Additionally, the solution needed to meet regulatory requirements, be cost-effective and rapidly scalable across the enterprise.

> *"The majority of documents we handle contain client personal data. These must all be scanned before reaching the internal network to protect our web applications from malicious file uploads. OPSWAT provides a high quality, easy-to-use, effective solution to secure this traffic."*
>
> Raymond Bucher
> Director/Cloud Architect at Swiss Re

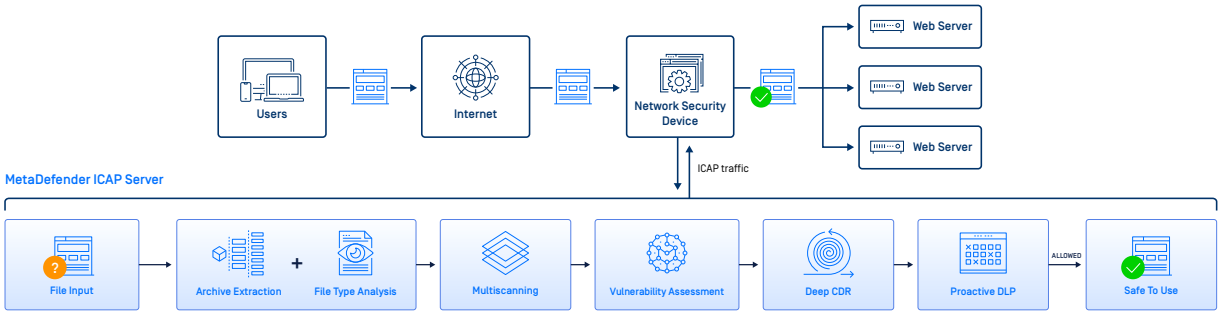
SELECTION CRITERIA

Compatibility with their micro-services architecture played a major role in the selection process–they needed a solution that could easily be deployed in their Azure/Kubernetes environment. The OPSWAT MetaDefender + ICAP Server platform offers seamless support for containerized deployments, providing robust and comprehensive protection capabilities to secure Swiss Re's critical data traffic.

Along with support for their current architecture, they also needed the solution to fit their future roadmap. With the addition of native support for NGINX/NGINX Plus ingress controllers, customers like Swiss Re will have the ability to extend this protection capability to multiple integration points. The end result is a flexible, easy-to-use and unified security experience.

To safeguard their highly sensitive client data, Swiss Re needed advanced capabilities not available in legacy solutions.

Multiscanning technology scans files (including multi-level nested archives) for malware with multiple antivirus engines to achieve the highest detection rates. Processing happens without delays (within milliseconds) and admins are alerted to potential threats in real-time.



SOLUTION

MetaDefender Protects Swiss Re's Network from Malicious File Uploads

Swiss Re deployed OPSWAT MetaDefender Core ICAP Server on top of their Azure Container Instances (ACI) and integrated it with an API Gateway. In conjunction with MetaDefender Core, they can validate all incoming files and scan for malware to protect their infrastructure from malicious payloads and sensitive data loss. This combination of technologies provides Swiss Re scalable and effective protection against malicious traffic at the edge-before it reaches their web applications.

With MetaDefender, Swiss Re gains:

- **Reduced Response Times via a Single Pane of Glass –** The unified platform between "MetaDefender Core and MetaDefender ICAP Server" enables them to seamlessly monitor and respond to threats. Information is readily available allowing quick triage of any potential threats.
- **Advanced Malware Detection and Protection –** OPSWAT's proprietary Multiscanning technology scans every file for malware simultaneously with multiple antivirus engines (using signatures, heuristics, NGAV, and machine learning) to achieve detection rates over 99%. Malware Analysis solutions
- **A Plug-and-Play Toolkit that can be Deployed in Minutes –** OPSWAT's MetaDefender ICAP Server can quickly integrate with the top ADCs, WAFs, load balancers, proxies, etc.

RESULTS

Fast Deployment, High Performance, and Scalability Resulting in Significant Overall Savings

The resulting benefits for Swiss Re include:

- **Scalable Web Application Security –** As they expand their footprint and add new applications to their environment, they can confidently implement OPSWAT technologies to secure those applications as well.
- **Enterprise-Class Performance –** With OPSWAT, they are able to comprehensively scan millions of files and deliver them well within their internal SLAs. More
- **Superior Service –** With OPSWAT, they received the help and professional insight to create a secure method to efficiently handle their vast web application traffic.

Contact OPSWAT

To learn more about how OPSWAT can help improve your critical infrastructure protection, contact us today.

©2022 OPSWAT, Inc. All rights reserved. OPSWAT, MetaDefender, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file.
Trust no device. are trademarks of OPSWAT, Inc.

2022.03.08