REVERSINGLABS

CUSTOMER: Fortune 500 Europe financial institution

HEADQUARTERS: Central Europe

EMPLOYEES: 45,000+

INDUSTRY: Financial Services

F500 Europe Bank uses Spectra Analyze to stop malicious files before they reach the endpoint

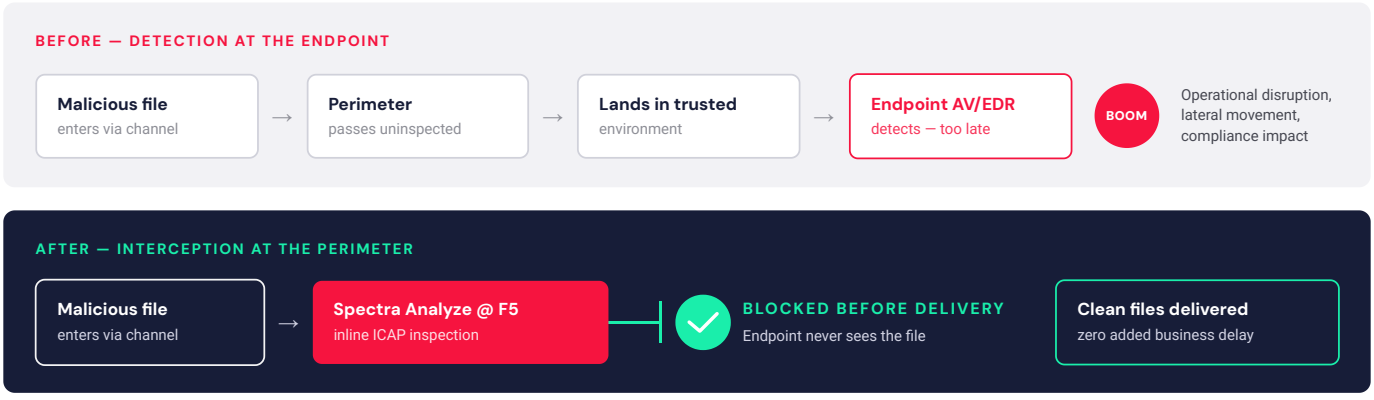
A Fortune 500 Europe banking group needed to control the files uploaded into its internet banking, mobile apps, customer portal, and privileged support channels — entry points where traditional security tools deliver poor efficacy and unacceptable latency.

Uploaded files were reaching trusted environments before inspection was complete, leaving the bank exposed to operational disruption, lateral movement, and potential compliance impact — without an answer that could keep pace with critical banking services.

> **"When our IT Audit team mandated a file scanning solution, we needed something we could trust completely, and that's what ReversingLabs Spectra Analyze delivered."**
>
> Security Engineer,
> F500 European Bank

Moving Detection Left of Boom

Why endpoint detection is too late — and what changes when inspection moves to the perimeter



Like many financial institutions, the bank already operated mature endpoint security controls, including antivirus (AV) and endpoint detection and response (EDR) solutions. However, security leadership recognized that relying solely on downstream detection exposed a critical gap. By the time a malicious or anomalous file reached an endpoint for inspection, the organization was already exposed to operational disruption, lateral movement risk, and potential compliance impact.

Under a strict mandate from IT Audit — reflecting the operational-resilience obligations now facing European financial institutions under regulations such as DORA — the organization required an upstream preventive control capable of intercepting threats at the network layer, with zero tolerance for performance degradation from the business.

The Solution:

The bank selected ReversingLabs Spectra Analyze to introduce advanced file inspection capabilities designed to stop attacks earlier in the kill chain.

Deployed on-premises and integrated directly into the organization's existing F5 BIG-IP infrastructure using ICAP, Spectra Analyze enabled inline inspection and classification of inbound files before delivery to internal systems.

The bank chose Spectra Analyze because it pairs inline ICAP verdicts with a full malware analysis workbench: the same platform that blocks a file at the perimeter lets the security team pivot into deep static analysis, while classification verdicts flow through REST APIs into SIEM and SOC workflows.

By shifting inspection to the network perimeter, the institution strengthened preventive controls while maintaining the speed and reliability required for critical banking operations.

Key capabilities deployed:

- Zero Trust File Structure Controls: Format integrity validation across 4,800+ file types, with full deconstruction of complex multi-layered files and automated anomaly detection prior to delivery
- Zero-Day Detection: Real-time identification of emerging threats beyond the reach of signature-based detection
- Superior Malware Detection: High-fidelity analysis exposing the latest complex and evasive threats
- Auditable Inspection Logs: Comprehensive, exportable reports across all file traffic to support internal policy and regulatory compliance requirements

CHALLENGES:

- No inspection controls at upload entry points — files reached back-end applications unchecked
- Zero-day and evasive threats beyond signature-based AV
- IT Audit mandate for an upstream preventive control
- Zero tolerance for performance degradation

SOLUTION:

- Deploy Spectra Analyze inline at network entry points, integrated with existing F5 BIG-IP infrastructure via ICAP, to inspect and classify every inbound file before delivery.

The Outcomes

The institution initially deployed Spectra Analyze to protect three core business services: Internet banking, mobile banking, and customer support.

Following deployment, the institution achieved:

- Real-time inspection of inbound files — 1000s of files/day with sub-second processing for typical documents
- Earlier detection of zero-day and evasive threats
- Improved alignment with Zero Trust security principles
- Enhanced auditability and compliance visibility, supporting DORA-aligned preventive controls
- High-availability protection across critical services
- Minimal operational overhead and tuning requirements

Following a successful rollout, adoption expanded organically across the organization. Service owners within the bank observed what the solution is capable of and actively requested to be onboarded. Today, the platform protects 10 services — more than tripling the original deployment scope.

Why It Matters

For financial institutions, detecting threats after delivery is no longer sufficient. This deployment demonstrated that advanced inline file inspection can operate at enterprise scale without compromising performance or user experience.

By integrating advanced file analysis directly into existing infrastructure, the bank improved protection against modern threats while enabling the business to operate securely at speed.

RESULTS:

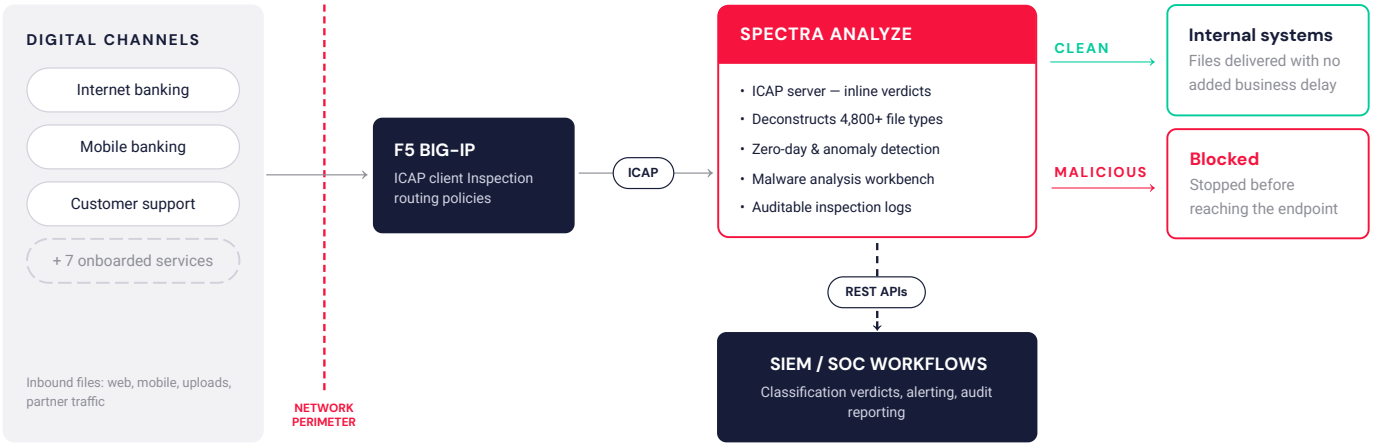
- 100% of files entering through the bank's protected digital channels are inspected and classified inline before delivery - 1000s files/day
- Zero delivery delays reported by the business - sub-second processing on typical documents
- Satisfied the IT Audit mandate with a demonstrable, DORA-aligned preventive control
- Scaled from 3 to 10 protected services in 3 months

RL PRODUCTS:

- Spectra Analyze

Inline Zero Trust File Inspection — Reference Architecture

Every inbound file is inspected and classified before delivery to internal systems



Does this story apply to you?

- You operate in a regulated industry with zero tolerance for downtime or delays
- Files enter your environment through web, mobile, and partner channels
- You already run F5 BIG-IP or other ICAP-capable infrastructure
- Audit or regulatory pressure (DORA, NIS2) is driving demand for preventive, demonstrable controls

IF TWO OR MORE APPLY, THIS DEPLOYMENT MODEL IS DIRECTLY TRANSFERABLE TO YOUR ENVIRONMENT.

Download the full case study for deeper technical insights and implementation details.

Deployment Journey

IT Audit mandate	Evaluation & selection	3 core services live	Organic expansion	Today: 10 services
Upstream preventive control required— zero performance impact tolerated	Spectra Analyze chosen for inline verdicts + analysis workbench + REST APIs	Internet banking, mobile banking, customer support via F5 BIG-IP + ICAP	Service owners actively requested onboarding	More than tripling the original deployment scope

Learn More About RL Solutions

CONTACT US TODAY

ABOUT REVERSINGLABS

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, the ReversingLabs Spectra Core powers the software supply chain and file security insights, tracking over 40 billion searchable files daily with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

CS-Rev-13.08.26

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com