Edenred Protects Its Prepaid Card Services with Check Point SandBlast

Check Point SandBlast Stops Threats Attached to Emails and Protects Digital Operations for Edenred

"SandBlast blocks malware attached to emails. No matter whether suspicious activity is occurring—SandBlast prevents it from getting in."

— Romain Dayan, IT Security and Telecommunications Director, Edenred

Customer Profile

Edenred is a world leader in prepaid corporate services.

Challenge

- Stop malicious files attached to emails from entering the network or users' inboxes
- Manage consistent, end-to-end security across four continents
- Ensure compliance is maintained according to multiple security regulations
- Increase operational efficiency

Solution

- Check Point SandBlast Zero-Day Protection

Results

- Eliminated malicious content embedded in emails from affecting users and protects against previously unknown threats
- Established consistent security policy across any environment and location
- Validated all compliance requirement and best practices to meet regulatory standards without affecting workflows
- Increased operational efficiency with automated forensics, saving security staff valuable time on incident response

Overview

Edenred

Edenred introduced the Ticket Restaurant meal voucher to the French market in 1962—one of the first employee benefits adopted by organizations across the country. Today, Edenred connects 43 million users with 1.4 million merchants and manages trusted transactions for 750,000 companies.

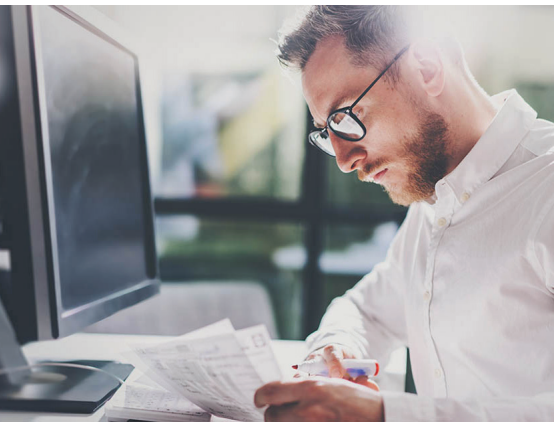
Edenred provides digital solutions by giving companies and employees the ability to perform a variety of everyday transactions worldwide. Corporate employees use Edenred payment cards or their mobiles to buy lunch or groceries. Fleet drivers fuel up, pay parking fees, and get their trucks serviced with Edenred cards. Merchants use Edenred to accelerate customer checkout and reimbursement. Companies use Edenred services to improve expense management, reduce operations costs, and minimize risks involved in complex transactions. With more than 2 billion transactions managed every year, Edenred has to meet the highest security and compliance standard to protect its customers' privacy and data.

Business Challenge

Protecting Client Security and Privacy

"We know our corporate clients and their employees," said Romain Dayan, IT Security and Telecommunications Director at Edenred. "Because we process personal and financial data, security and privacy are our topmost concerns."

Edenred has been a Check Point customer for many years, using Check Point solutions to protect its corporate networks and data centers worldwide. As the company continues to evolve, so do its data transport, storage, and security needs. As a financial organization, it is also subject to the Payment Card Industry Data Security Standard (PCI DSS), banking regulations, transaction authorization requirements, and General Data Protection Regulation (GDPR) laws. One of the most important requirements for Edenred was to create security and compliance standards that encompass its operations in North America, Europe, Brazil, and Singapore. In order to achieve it, Edenred needed a solution that provides not only the best protection but also can meet the most demanding compliance standards.



Solution

Zero-Day Protection

Edenred was seeing a growing amount of malware arriving with email. Its anti-spam solution wasn't enough to protect against advanced threats, so the security team chose SandBlast Zero-Day Protection for complete protection against zero-day and targeted attacks. Unlike other sandbox solutions, SandBlast's Threat Emulation technology with CPU-level inspection can stop the most sophisticated threats. Using evasion-resistant malware detection techniques, SandBlast can look into exploits that try to bypass OS security controls and stop the attack even before it tries to launch and evade detection. In addition to that, SandBlast's Threat Extraction component removes malicious active content and embedded objects and delivers a clean file to end users.

Results

Prevention for Greater Security

With SandBlast, users receive safe files quickly—without the delays of traditional sandboxes. This gives the IT team greater assurance that cyber threats are kept out without disrupting productivity.

"SandBlast blocks malware attached to emails," said Dayan. "No matter whether suspicious activity is occurring—such as attempts to modify a registry, in network connections, or by new file creation—SandBlast prevents it from getting in."

> "Even with 60 Check Point clusters, SandBlast is simple to manage. That's important, because it's hard to find technically skilled staff to manage complex systems."
>
> — Romain Dayan, IT Security and Telecommunications Director, Edenred

Unified Management for Comprehensive, End-to-End Coverage

SandBlast allows Dayan and his team to easily extend Check Point protection wherever it's needed—on premises or in the cloud—quickly and easily. Using single-pane-of-glass security management, Edenred gains consistent security policy and enhanced visibility for all networks and threats. The unified management controls everything from the firewall, to threat prevention and endpoints, regardless of where they are, bringing enterprise-level security to the entire organization.

"Even with 60 Check Point clusters, SandBlast is simple to manage," said Dayan. "That's important, because it's hard to find technically skilled staff to manage complex systems. We have one person managing the solution in each location, and we hope to centralize management globally to one place."

Automatic Response Saves Time

At first, the security team used manual forensics, comparing documents to known threats to see if they matched. When they saw that SandBlast automatically stripped out suspicious content and delivered a safe file, they were amazed at how much effort it saved them. SandBlast delivers detailed reports, including screenshots, to document anomalous activity. It also shares newly discovered threats with Check Point's ThreatCloud™ intelligence database, where they are distributed to protect other connected Check Point gateways.

To learn more about SandBlast, visit: https://www.checkpoint.com/products-solutions/zero-day-protection/