CUSTOMER CASE STUDY

State Transport Leasing Company (STLC) Chooses Check Point to Create a New Standard for Cyber Security

Check Point's Next-Generation Threat Prevention Solutions Deliver All-round Security and Maintain a Reliable and Flexible Network Infrastructure

STLC State Transport Leasing Company

Customer Profile

State Transport Leasing Company (STLC) is a leading Russian leasing company specializing in transport.

Challenge

- Consolidate multiple security solutions to simplify management and improve security
- Protect the corporate network from external and internal threats
- Protect against Advanced and Zero-day threats
- Enhance endpoint security without interrupting the business flow
- Increase security effectiveness and ease security admin workload

Solution

- Check Point SandBlast Zero-Day Protection
- Check Point Security Management R77.30
- Next-Generation SmartEvent

Results

- Consolidated security architecture with real time prevention
- Centralized and optimized security management via a single, customizable console
- Enhanced visibility with SmartEvent including detailed logs, customized reports and forensic analysis for simple incident investigations

> "Check Point solutions prevent threats of all kinds when users unknowingly access malicious resources, completely eliminating the very possibility of damage or data breach."
>
> — Sergey Rysin, Security Advisor to STLC Director

Overview

STLC — Russia's Premier Leasing Company

State Transport Leasing Company (STLC) is a leading Russian leasing company specializing in the leasing of air transport, sea and river vessels, railway vehicles, trucks and special equipment such as energy-efficient passenger transport. STLC's customers and partners include flagship Russian and international banks, manufacturers of air, rail and road transport and carrier companies. STLC was established in 2001 as ZAO Civilian Aviation Leasing Company. It expanded its portfolio in 2005 to include road transport and infrastructure. STLC has evolved into the largest Russian leasing company entrusted with the financing of high-profile civilian aviation and transport projects, such as deliveries of the Sukhoi Superjet 100 passenger plane.

Business Challenge

Bolstering Corporate Network Security and Easing the Workload of System Administrators

"Our employees handle all sorts of commercial and sensitive information," says Sergey Rysin, Security Advisor to the STLC Director, adding: "The IT department is tasked with keeping it secure. In the face of increasingly sophisticated security threats and data breach mechanisms, it is vital that we are able to respond quickly to all intrusions and develop systems that can ward off external threats. Since a person is incapable of processing such a vast array of information single-handedly, we have come to rely on a robust solution that can respond to our corporate needs. Check Point gives us the highest level of security."

Check Point SOFTWARE TECHNOLOGIES LTD

February 20, 2018

In recent years the company has repeatedly faced all kinds of issues concerned with data protection, from unauthorized access to corporate resources and threats posed by ransomware. While the IT team promptly prevented all issues as they came to light, STLC management realized the need for proactive threat prevention in order to avoid damage to the business.

“Prior to Check Point, the IT infrastructure of STLC relied on a solution by another well-known vendor, which failed to solve the task of blacklisting of resources and real-time prevention of cyber attacks. When we decided to take critical action and search for a new solution, we considered offerings by Palo Alto and a number of Russian vendors. Check Point products stood out among the competitors for their ease of configuration, a user-friendly interface and the ability to prevent threats from entering the network more effectively than the competition. Last but not least, they did a good job achieving the requirements identified during the pilot project stage,” Mr Rysin continues.

> “Check Point products stood out among the competitors for their ease of configuration, a user-friendly interface and the ability to prevent threats from entering the network. Last but not least, they did a good job achieving the requirements identified during the pilot project stage."
>
> — Sergey Rysin,
> Security Advisor to STLC Director

Solutions

Effective Integrated Security

The STLC corporate network has a multi- layered architecture. Check Point Next Generation Threat Prevention protects the corporate network perimeter from external threats and prevents user access to potentially malicious websites and services while preserving access privileges essential to performing the user’s duties. When a user attempts to access a potentially malicious external resource, the system automatically blocks the request and notifies the administrator. “Check Point solutions prevent threats of all kinds when users unknowingly access malicious or unknown resources, completely eliminating the very possibility of damage or data theft, and preventing any potential damage,” says Rysin. All network traffic is continuously monitored by SmartEvent, the Check Point SIEM system, which allows to track all network activity and generate reports on demand.

The SandBlast solution is used to protect endpoints on the STLC corporate network. “The SandBlast solution provides quality endpoint protection against any type of malware and other security threats, which makes it all the more easier for the IT department to provide support to users,” Mr Rysin adds.

All major companies face the same common problems associated with the use of removable drives, internet access and external mail services used by employees. The Check Point SandBlast Endpoint Security enables administrators to flexibly configure access privileges, prohibit downloads and transmission of specific file types, and protect users against both common threats and zero-day attacks such as ransomware. The intuitive interface and ease of administration enables the company to respond to changing conditions and requirements promptly while maintaining the much-needed flexibility with a high level of security.

Results

Deep Integration and Full Visibility

Check Point R77.30 security policy stands out for its high flexibility. Permission to access applications, services and external resources can be granted easily on a user basis, ensuring the optimal level of security while allowing all the features that users truly need, without interrupting the business flow. Flexible yet efficient rules encourage employees to adopt a more responsible attitude toward good information security practices.

"As they say, the best defence is prevention," Mr Rysin continues, adding: "Check Point solutions effectively block unauthorized attempts to access restricted resources, which helps us avoid the majority of potentially dangerous situations without affecting the quality of communication with external services and networks. Mindful of the system warnings, users have adopted a more responsible approach toward using information and services from external networks. The logs and alerts received on each security incident are also very intuitive, which has enabled us to generate high-quality reports on the threats prevented. We use them in forensics and subsequent analysis without having to waste any extra time."

"The system proved flexible at the deployment stage, while quality support helped us roll out the system efficiently and quickly," Mr Rysin concludes, adding: "Cross-platform and centralize administration capabilities have made it much easier for us to keep our perimeter secure without jeopardizing the quality or reliability of protection. We are happy to recommend Check Point solutions to colleagues at other companies."

For more information, visit:
checkpoint.com/products-solutions/
zero-day-protection/

Check Point
SOFTWARE TECHNOLOGIES LTD