

e x e o n

Smart Cyber Security.

Planzer – an ExeonTrace NDR Case Study

ExeonTrace secures

Planzer's distributed network





Planzer Management: Nils Planzer, Nicolas Baer and Severin Baer, fltr



— Project overview

Industry: Logistics & Transportation

Benefits provided by ExeonTrace:

- Visibility of the highly distributed IT infrastructure
- Pure software-based – deployed within just a few days and no additional hardware needed
- Ongoing incident monitoring – deployed within just a few days
- Legacy systems highly protected

Challenges faced by ExeonTrace:

- Distributed network across 70 different locations globally
- Outages would have far-reaching operational and financial consequences
- Historic log data needed to localise possible incidents
- Legacy systems that need to be secured

— Planzer Business Background


With more than 5'000 employees worldwide and a revenue of almost 1 Bio. CHF, Planzer is a leading Swiss logistics company.

Planzer operates 1'900 vehicles at 70 locations in Switzerland, Italy, France, Germany and Hongkong amongst others.

The family owned Planzer group transports goods and parcels by road and rail nationally and internationally. In addition, Planzer also offers warehouse logistics services to domestic and global clients.

An abstract graphic in the bottom-left corner consisting of a dense, overlapping mass of thin, wavy lines in various colors including red, pink, purple, blue, and green. The lines appear to flow and swirl together, creating a complex, organic shape.

PLANZER

An abstract graphic on the left side of the slide, consisting of a dense, tangled mass of thin, wavy lines in various colors including red, orange, yellow, and green. The lines appear to flow and curve, creating a sense of movement and complexity. The graphic is positioned on the left side of the slide, partially overlapping the white background.

“As CEO and owner of a fast-moving logistics company, I cannot afford any system interruptions due to cyber incidents. With ExeonTrace, we have found a solution to monitor our network and quickly detect cyber threats.”

Nils Planzer

CEO & Owner Planzer

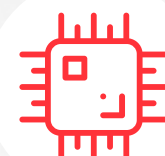
Challenges



Planzer's day-to-day operations highly rely on digital systems, downtime simply isn't an option. Also, the Maersk cyber attack in 2017 demonstrated the industry need for cyber defenses that take alert before the damage arise



The Planzer security team sought a solution easily allowing them to navigate through the log data to go back in time in case a security incident or problem happens



As Planzer operates across 70 sites, the low set-up effort without additional hardware at every location was a requirement.



In addition, Planzer aimed at securing critical legacy systems which are essential for the daily business operations but are especially vulnerable to attacks since they can no longer be updated

Solutions



Total visibility:

Through the integration of ExonTrace, all Planzer sites and networks can be monitored. With the Algorithm-driven threat scoring, the network is constantly monitored and advanced attacks are immediately reported by an alert



Software-based:

ExeonTrace software deployed as a VM in the customer's Azure cloud



Clever data handling:

Flow data collection (NetFlow) from 70 locations distributed all over the world. Data exported by customer's existing firewalls. Using NetFlow data makes the solution very lightweight, reducing the bandwidth needed for the analysis



Rapid deployment:

Setting up the solution and establishing visibility over 70 locations took a single day only. After that, configuration and fine-tuning the solution with the customer took all-in-all about one week

— Benefits



Unique value: ExeonTrace allows the customer to centrally monitor and navigate through the network activities of all 70 sites without any hardware. This hardware-free solution makes it cost- and time-efficient both in set-up and in operations.



ExeonTrace provides visibility into Planzer's highly distributed IT infrastructure.



Planzer's security team regularly checks ExeonTrace's UI and investigates the anomalies triggered by ExeonTrace. Anomalies consider historic data and make them visual in order to find root causes efficiently.




ExeonTrace is not only used by the security but also by the operations team in order to monitor the usage of the systems across all locations, to plan as well as to verify network changes (e.g. migration of services to the cloud).



ExeonTrace provides additional security for the whole company network and especially for the business-critical legacy systems, as monitoring rules are even more restricted.



ExeonTrace allows the recording and long-term storage of relevant security log data. A graph database achieves data reduction and enables easy navigation through the log data in the interface.

An abstract graphic in the bottom-left corner consisting of a dense, tangled mass of thin, wavy lines in various colors including red, orange, yellow, and green. The lines appear to flow and curve upwards and to the right, creating a sense of movement and complexity.

“I’m highly impressed by the technical abilities
of this Network Detection & Response solution.
I can definitely sleep better knowing that we
have ExeonTrace in our network.”

Peter Hagen

CIO Planzer

— Get in touch with us

e x e o n

Smart Cyber Security.



Gregor Erismann
CCO
+41 78 797 05 09
gregor.erismann@exeon.com

Exeon Analytics AG
Grubenstrasse 12
8045 Zurich
Switzerland
contact@exeon.com

exeon.com