CASE STUDY

Linking Europe and Asia with a Complete, Connected Security Strategy

Avrasya Tüneli (Eurasia Tunnel), which links Europe with Asia under the Bosphorus strait in Turkey, uses a comprehensive, connected Palo Alto Networks platform to deliver powerful, agile, and automated security at a lower cost.

paloalto® NETWORKS

IN BRIEF

Customer

Avrasya Tüneli

Industry

Transportation

Organization Size

150 people

Services

Connected security platform comprising best-in-class, integrated network, endpoint, and IoT security.

Country

Istanbul, Turkey

Challenges

Implement a forward-thinking, efficient IT security strategy to protect end-to-end IT infrastructure and ensure a fast, uninterrupted journey for 50,000+ drivers every day.

Requirements

+ Secure protection of end-to-end tunnel IT infrastructure.
+ Simplify and automate everyday security tasks using ML and AI.
+ Create a single, unified view of security operations.
+ Deploy quickly with minimal configuration.

Solution

Palo Alto Networks platform, comprising Strata™ Next-Generation Firewall (NGFW) with Threat Protection, URL Filtering, DNS, WildFire®, GlobalProtect™, DLP and IoT Services. Palo Alto Networks Cortex XDR

CHALLENGE

Building a bridge to the future

As the Director of IT and Toll Collection Systems for Avrasya Tüneli, Murat Çalişirişçi was staring into a big hole. Building work was progressing quickly on the five-kilometer tunnel in Istanbul, linking the two continents of Europe and Asia, and the team needed a modern, adaptive security solution to support safe, continuous tunnel operation. The security infrastructure spans the network, endpoints, and more than 2,000 Internet of Things (IoT) devices.

“With no legacy infrastructure, we could start with a blank piece of paper,” says Murat Çalişirişçi. “However, we realized that separate point security systems would be inadequate to prevent the rising volume and sophistication of cyberattacks. They would also demand manual intervention, delaying our actions.”

The challenges didn’t stop there. Manual detection and remediation would do little to reduce risk, as it would mainly be executed after the event, with limited visibility and manual correlation of the different attack elements. The tunnel’s unregulated IoT devices, for example, would pose immense cybersecurity risks, leaving the security team blind to unknown devices and unable to scale their operations or prioritize efforts.

And then there were the resources constraints. Emrah Dündar, IT and Security Manager at Avrasya Tüneli, explains, “Our security operations team comprises three people. We needed a partner that we could trust to manage everyday security processes and proactively eliminate vulnerabilities without demanding an increase in headcount.”

REQUIREMENTS

All-in-one network, IoT, and endpoint security

Emrah Dündar and his team acted quickly. Initially concentrating on network security, they quickly broadened the scope of their target security operating model to incorporate endpoint and IoT security. The requirements were:

- Implement simple, integrated, and automated controls to detect and prevent threats, at every stage of the attack lifecycle, across all digital operations.
- Use an intelligent, automated security platform that could be administered by a lean team.
- Safeguard more than 2,000 SCADA operational technology (OT) devices from threats and minimize the attack surface.
- Gain visibility and reduce risks from the weak points and blind spots across the tunnel organization.
- Stop attacks by applying analytics to the endpoint, network, and cloud data.
- Secure the network with proven next-generation antivirus, detection, and response.

SOLUTION

Palo Alto Networks shows there's light at the end of the tunnel

Avrasya Tüneli selected Palo Alto Networks following a rigorous evaluation of vendors. "Palo Alto Networks scored highly on every aspect of the proof of concept," says Emrah Dündar. "We worked closely with the local Palo Alto Networks team and channel support on a proof of concept. By evaluating all the features on the PA-3200 Series ML-Powered NGFW, we subsequently deployed the entire Palo Alto Networks platform."

This platform comprises a complete, end-to-end suite of integrated security technologies. "It's integrated, automated, and simple," Emrah Dündar explains. "Their integrated platform offers holistic protection, connecting all key security data through a single pane of glass. Every component of the platform is best-in-class, and their future product roadmap demonstrated them to be a visionary partner."

This intelligent Palo Alto Networks PA-3200 Series ML-Powered NGFW is the cornerstone of the network security strategy. It combines the complete suite of NGFW cloud-based security services—Threat Prevention, Advanced URL filtering, WildFire® malware analysis, and enterprise DLP—to detect and prevent advanced threats. "The platform is cleverly designed with a prevention-focused architecture," says Murat Çalişirişçi. "We rely on it every day to prevent attacks. The ML-powered automation and analytics ensure we are continually learning and improving our network security strategy."

> Palo Alto Networks scored highly on every aspect of the proof of concept. We worked closely with the local Palo Alto Networks team and channel support on a proof of concept. By evaluating all the features on the PA-3200 Series ML-Powered NGFW, we subsequently deployed the entire Palo Alto Networks platform.

—Emrah Dündar, IT and Security Manager, Avrasya Tüneli

A Palo Alto Networks IoT Security subscription combines with this NGFW platform to protect the network of 2,000+ IoT devices operating across the tunnel infrastructure. This includes cameras to monitor traffic flows throughout the tunnel and entry/exit, IP phones, office equipment, and motion sensors. The IoT Security team identified all the devices—even ones that were previously unknown to the security teams—almost immediately following go-live, preventing threats, assessing IoT risks, blocking vulnerabilities, and automatically enforcing least-privilege security policies to keep the devices safe at all times.

The Palo Alto Networks Cortex® XDR™ threat detection and response solution completes this unified platform strategy. Blending ML-based network traffic analysis, detection from more than 200 endpoints, and user behavior analytics in a single, powerful platform safeguards Avrasya Tüneli against even the most sophisticated attacks. When Avrasya Tüneli evaluated different EDR vendors, for example, they created a custom lab environment to evaluate each alternative. Cortex XDR blocked every type of threat the team challenged the system with.

"The difference between Cortex XDR and Palo Alto Networks Traps endpoint security we relied on previously is transformational," says Emrah Dündar. "Intelligent automation makes all the difference. We gain a clear picture of every attack, allowing us to drive response actions across the entire infrastructure."

> "Tunnel safety is our number one priority. IoT Security gives us complete visibility, prevention, and enforcement for every IoT device—and that helps keep the traffic flowing.
>
> **—Murat Çalişirişçi, Director IT and Toll Collection Systems, Avrasya Tüneli**

BENEFITS

Ensuring an uninterrupted shortcut between continents

This modern, end-to-end security platform protects every aspect of the driver's journey and the tunnel's infrastructure: from the website customers use to plan their journey and the automated toll payment system to the network of almost 400 cameras that monitor every corner of the five-km tunnel along with its approach roads. Effective protection against security threats ensures a fast, reliable, and rewarding travel experience—more than 50,000 drivers a day can complete the intercontinental journey with confidence in about five minutes, versus the one to two hours it used to take using the old route through Istanbul.

The integrated IoT Security component is a great example of this 24/7 operation. Murat Çalişirişçi explains, "Tunnel safety is our No. 1 priority. IoT Security gives us complete visibility, prevention, and enforcement for every IoT device—and that helps keep the traffic flowing."

A single platform to see and secure the tunnel's infrastructure

Seamless integration provides Avrasya Tüneli with consistent security, closing gaps in network visibility. Everything from threat prevention and URL filtering to DNS, IoT, and endpoint protection is contained within one platform. Automated threat identification and prevention, coupled with data-driven analytics, ensure Avrasya Tüneli's infrastructure and people are secured and protected.

Emrah Dündar explains, "Palo Alto Networks platform approach gives Avrasya Tüneli the most comprehensive cybersecurity portfolio in one tightly connected system. Features like machine learning and automation transform our security operations, enabling us to quickly and simply detect and respond to threats."

Less complexity means less effort

Avrasya Tüneli is using the platform's powerful automation to increase the speed, consistency, quality, and reliability of tasks. It takes less than a minute, for example, for the Avrasya Tüneli team to implement IoT Security through the NGFW without the need to deploy any new network infrastructure or changes to existing processes before acting. Meanwhile, Cortex XDR automatically collects data from Avrasya Tüneli's endpoints, network, and third-party logs to accurately detect attacks—there's no manual integration.

"The platform gives us the 'power of one,'" says Murat Çalişirişçi. "One best-in-class security platform to automate and protect our critical infrastructure, and one management console to monitor and control security. Three people currently manage our security operations, and I do not anticipate needing to add more people as the organization grows."

Time to value and low total cost of ownership

Examples abound of how this coordinated platform is reducing cost and accelerating time to value. They include:

- The NGFW stops common file and web-based unknown threats instantly.
- 100% of IoT devices are detected within 48 hours.
- C2 activity stopped with DNS Security.
- Cortex XDR led to an almost 100% reduction in alert volume and a significant increase in investigation speed.
- Rapid integration of Cortex XDR and other technologies into the infrastructure enables the team to focus on other high-priority tasks.

CONCLUSION

A trusted partnership for the future

The success doesn't stop there. Avrasya Tüneli is now exploring additional Palo Alto Networks innovations, such as Panorama™ network security management, to further enhance the cybersecurity strategy and stay ahead of threats.

Murat Çalişirişçi concludes, "As we scale and digitize more of our operations, we trust Palo Alto Networks to be beside us. Their unified platform makes it significantly easier to manage our operations, they are continually innovating the product suite, and the support and expertise we receive here in Turkey are second to none."

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com