SNAP SHOT

ENTSORGUNG + RECYCLING ZÜRICH
Progressive Swiss City Bolsters Security
with Palo Alto Networks

paloalto
NETWORKS®

Stadt Zürich
Entsorgung + Recycling

Entsorgung Recycling Zurich (ERZ) recycles waste for the city of Zurich, Switzerland. Every day, ERZ collects over 30,000 bags of waste, cleans the streets, sidewalks and parks, and cleans the waste water of the City of Zurich. With approximately 900 employees, ERZ Disposal and Recycling is the largest service department in the Civil Engineering and Waste Department of Zurich.

INDUSTRY // Waste Management

CHALLENGE // Improve security to prevent advanced attacks on endpoints, reduce IT management burdens, and lower CPU utilization.

SOLUTION // Traps Advanced Endpoint Protection and WildFire added to Palo Alto Networks Enterprise Security Platform

SUBSCRIPTIONS // Traps Advanced Endpoint Protection and WildFire

APPLIANCES // PA-4020

PA-4020 (1)

RESULTS

• Reduced administrative expenses with a more automated, easy-to-use endpoint security tool

• Improved allocation of internal resources

• Provides new level of protection and prevention from tight integration of security platform

No Time to Waste

ERZ provides critical basic infrastructure services to the people of Zurich 24/7, so it recognizes the importance of protecting its network. The changing nature of threats, and the limitations of its incumbent endpoint security products, led ERZ to look for a new solution. "Risks like Advanced Persistent Threats and others emerged," says Julio Lorenzo, Leader, Group Field Infrastructure for ERZ. "Our legacy anti-virus solutions weren't equipped to protect us from these sophisticated attacks. We didn't have any reliably functioning endpoint security. We needed more than just protection on the Internet gateway to fend off threats from outside and inside."

ERZ has been using the Palo Alto Networks PA-4020 next-generation firewall for several years for perimeter network security, application and bandwidth control, and IPS. "It is stable, reliable, performs excellently and provides outstanding IPS and true application control," says Lorenzo. "Palo Alto Networks isn't limited to only providing point-to-point security, but application layer security as well."

For anti-virus and endpoint protection, over the years ERZ deployed multiple products from McAfee, Symantec, Hewlett-Packard, and most recently, Kaspersky. Kaspersky put excessive administrative burdens on ERZ's three-person IT staff, and left ERZ vulnerable. "It was a constant challenge to apply security patches on time to address new vulnerabilities or Zero-Day attacks," says Lorenzo. ERZ wanted a modern endpoint security solution that wouldn't require additional resources. "We're always looking for new solutions that can automate work and threat prevention, which were taking us a half day of work to manage," says Lorenzo.

Redefining Endpoint Security

Omicron AG is a security solutions provider for numerous organizations in Switzerland, and ERZ's longtime IT advisor. Omicron AG recommended Palo Alto Networks Traps™ Advanced Endpoint Protection. Traps is part of the Palo Alto Networks Enterprise Security Platform, which also consists of a Next-Generation Firewall and Threat Intelligence Cloud. It delivers application, user, and content visibility and control, as well as protection against known and unknown cyber threats. The Threat Intelligence Cloud provides central intelligence capabilities, as well as automation of the delivery of preventative measures against cyber attacks.

Traps prevents sophisticated vulnerability exploits and unknown malware-driven attacks. It is a highly scalable, lightweight agent that uses an innovative new approach for defeating attacks without requiring any prior knowledge of the threat itself. Traps provides organizations with a powerful tool for protecting endpoints from virtually every targeted attack.

ERZ tested Traps in its lab. "We didn't even need to consider testing another endpoint security product," says Lorenzo. "Traps offers a highly reliable, strong level of protection in the cyber attack lifecycle – much better than legacy anti-virus, and takes a different, prevention-oriented approach to achieving endpoint security." Another big selling point was its ease of use. "We don't have to babysit and update Traps constantly, and it would still prevent unknown attacks," says Lorenzo.

No Recycled Solutions

ERZ replaced Kaspersky with Traps. "Patching is no longer time-consuming or urgent because Traps keeps us safe even before patches are deployed," says Lorenzo. "Traps also requires almost no housekeeping and doesn't absorb resources. Before, our solutions were always running and using resources unnecessarily. Traps only kicks in when needed."

Lorenzo appreciates the scalability and lightweight nature of Traps. "It has no impact on performance," says Lorenzo. "You can use Traps in various places and easily cover different networks, and jump right in and work with it with minimal training."

At the same time ERZ rolled out Traps, it deployed Palo Alto Networks WildFire™. A WildFire subscription protects against advanced malware and threats by proactively identifying and blocking unknown malware, Zero-Day exploits, and Advanced Persistent Threats. WildFire extends the Palo Alto Networks Enterprise Security Platform and uniquely applies its behavioral analysis regardless of ports or encryption. When an unknown threat is discovered, WildFire automatically generates protections to block the threat across the cyber attack lifecycle in near real-time.

"WildFire provides another layer of protection," says Lorenzo. "Native integration between Traps and WildFire means that unknown executables attempting to run on our endpoints are automatically checked. If the file is malicious, Traps will prevent it from running. Furthermore, even unknown malware can be prevented because Traps can submit unknown executable files to WildFire for analysis."

Progressive Swiss Department Gets Progressive Security

ERZ is glad it entrusted its security to Palo Alto Networks. "I like the simplicity of Traps, that it uses an innovative, completely new approach compared to typical anti-virus products, and that it uses less resources," says Lorenzo. "Our savings mostly relate to using fewer personnel resources. Now we also have far less administrative expenses due to non-functioning anti-virus agents and other IT products."

ERZ has improved endpoint and overall security, and reduced IT administrative burdens. "There is no silver single bullet in IT security," says Lorenzo. "From perimeter security to the endpoint, everything needs to be tightly integrated because you don't know where threats may come from. Traps endpoint security, integrated into the Palo Alto Networks Enterprise Security Platform, shows you what is happening, where it's happening, and it stops threats. It provides a new level of protection and prevention against known and unknown threats before they can cause damage."

4401 Great America Parkway
Santa Clara, CA 95054

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

www.paloaltonetworks.com