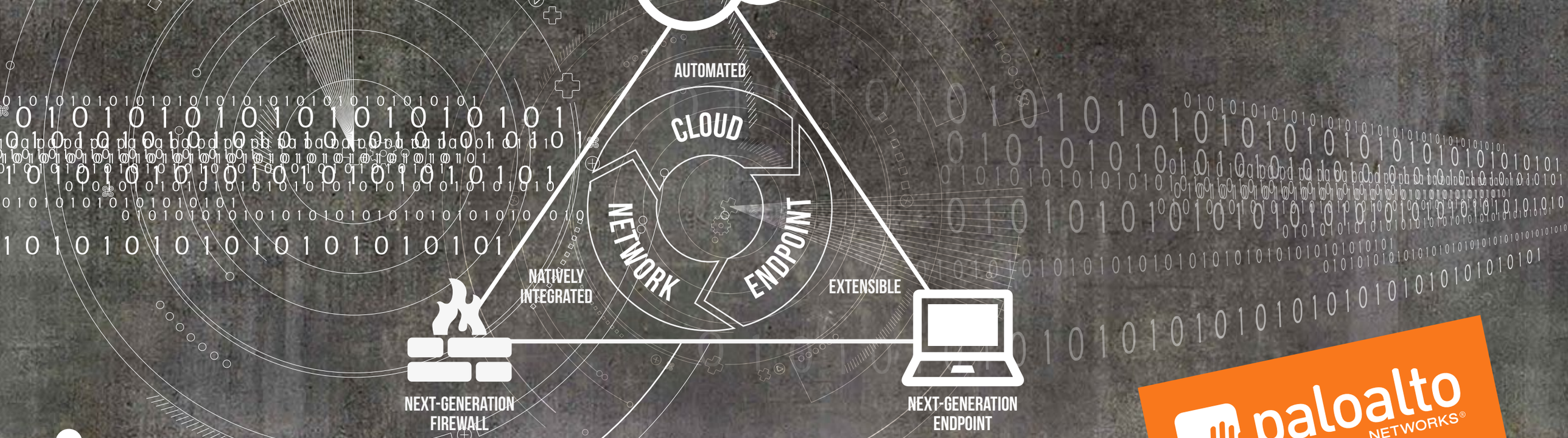


paloalto NETWORKS®

THE WORLD HAS CHANGED

PREVENTION

INTRODUCTION>
PLATFORM>
CASE STUDY>
LEARN MORE>

the fault is our own >

consistently disrupt advanced attacks >

WE NEED TO ARCHITECT SECURITY FOR BREACH PREVENTION.

paloalto NETWORKS®

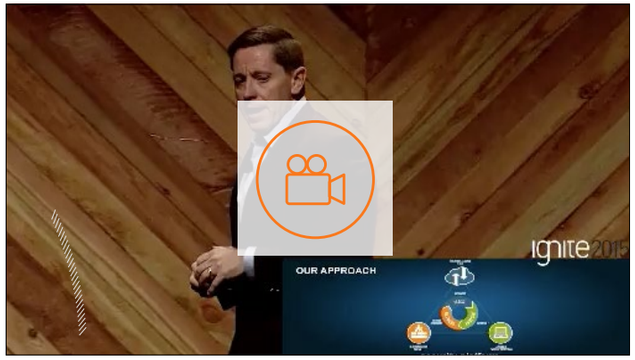
Reading the headlines today, we see breach after breach of our most sensitive personal information, our most innovative intellectual property, and our most vital daily services.

The fault is our own;
a reactionary mindset to cybersecurity is not sustainable and will inevitably erode the trust all users place in the Internet as a global commerce and social networking tool.

Palo Alto Networks CEO Mark McLaughlin: Change the dynamics of attacks.

Cyberattacks don't happen by magic; just like any operation, they follow a chain of logic — an attack lifecycle — that requires each step to be successful. Attackers can change their tools and techniques, but they still have basic rules they must follow to get at our data.

Security to date has focused on identifying weaknesses in these attack cycles and addressing them at individual points. But an attacker only has to be right once about a weak spot to cause millions of dollars in damage and cleanup costs.



To consistently disrupt advanced attacks, *we need to focus, not just on points of the attack, but on the entire attack lifecycle – and use that knowledge to prevent attacks before they happen.*

It's time for all Internet-connected businesses to architect for prevention, placing preventative capabilities in every single place where an attack needs to be successful and ensuring those capabilities integrate tightly together in an automated platform.

No one's going to prevent every attack and that's not a reasonable promise to make to businesses, governments or consumers. But if our only answer is to clean up after an attack, we'll all continue to suffer the consequences and the very trust our digital world relies on will be jeopardized. Breach prevention is the way forward, and we're ready to lead the way.

INTRODUCTION>

PLATFORM>

CASE STUDY>

LEARN MORE>

paloalto NETWORKS®

- Next-Generation Security Platform >
- Automatic and Awesome >
- Integration Means Security >
- The Ultimate Breach Prevention >

NEXT-GENERATION SECURITY PLATFORM.

Palo Alto Networks is partnering with some of the most demanding industries to ensure their data and critical infrastructure remain safe from targeted attacks, whether adapting traditional, cloud-based, or hybrid infrastructure, these organizations have learned firsthand the power of a next-generation security platform when it comes to safely enabling the use of all applications, maintaining complete visibility and control, and confidently pursuing new business ventures, while protecting the organization from the latest cyberthreat. We invite you to explore the details of this platform.

"The joint Palo Alto Networks-VMware network security and network virtualization solution enables rapid provisioning of next-generation network security with our applications and a single pane of glass management interface for all our security policies across our nearly 100 percent virtualized data center environment."

***John Spiegel**, Global IT Communications Manager, Columbia Sportswear*

John Spiegel, Columbia Sportswear

play audio quote

Melvin Benevides, Systemmetrics Corporation: Proactive security means stopping them at the door

STOP AUDIO

INTEGRATION MEANS SECURITY.

paloalto NETWORKS®

tennis

GOLDCORP

Our natively integrated platform brings network, cloud and endpoint security into a common architecture, with complete visibility and control, ensuring your organization can detect and prevent attacks. This next-generation security platform streamlines day-to-day operations and boosts security efficacy, and the one-of-a-kind, multi-layered defense model prevents threats at each stage of the attack life cycle.

"We now have visibility. We can now see any potential attacks in real time and prevent them, and this is very refreshing to say the least. We couldn't do that with our previous firewall so I believe we are now in the best possible position with regards to network protection."

***Steve Wood**,*

CEO, Tennis Australia

play audio quote

Steve Wong, Goldcorp: "Breaches happen" is not an excuse

STOP AUDIO

AUTOMATIC AND AWESOME.

Focus your team on only the high-priority security events and let the Palo Alto Networks platform take care of the lower-priority congestion. An automated platform eliminates the need for expensive, manual processes and improves your organization's ability to quickly respond to new global threats. New threats are quickly detected and attacks are prevented — all without your best people spending hours manually monitoring endless pools of alerts.

"There has to be more of a focus on stopping the bad guys, not merely responding to attacks after the fact. The industry has been caught in a mode of believing that it's only a matter of "when" they will be hacked, he contends, as opposed to "if" they will be hacked. That's defeatist."

Golan Ben-Oni,
VP Network Architecture, IDT Corporation

play audio quote

Ashtosh Kapse, IOOF: In financial services detection is a little bit too late

STOP AUDIO

THE ULTIMATE BREACH PREVENTION.

paloalto NETWORKS

Stadt Zürich
Entsorgung + Recycling

MOTOROLA SOLUTIONS

Our Next-Generation Security Platform protects every corner of your organization — safely enabling all applications and users — from their mobile devices to the very core of your hybrid cloud computing environment.

Integration and automation mean security. Palo Alto Networks natively integrated platform brings network security, cloud-based threat intelligence and advanced endpoint protection into a common architecture, providing complete visibility and control and ensuring enterprises, governments and service providers can not only detect, but also prevent advanced attacks.

"We didn't even need to consider testing another endpoint security product. Palo Alto Networks Traps Advanced Endpoint Protection 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."

Julio Lorenzo,
Leader, Group Field Infrastructure for Entsorgung Recycling Zurich (ERZ)

play audio quote

Paul Carugati at
Motorola Solutions

STOP AUDIO

INTRODUCTION>
SOLUTIONS>

CASE STUDY>

LEARN MORE>

paloalto NETWORKS®

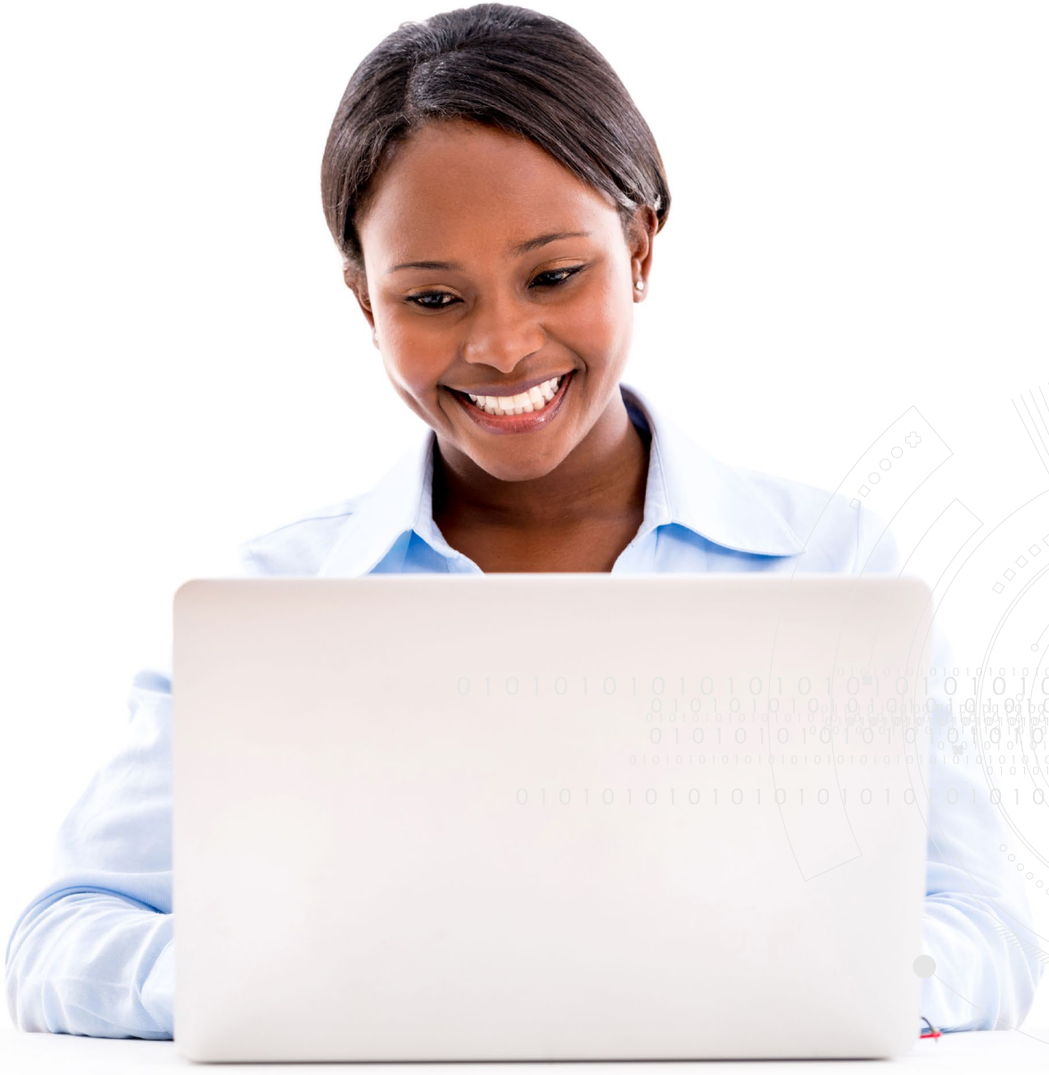
Entsorgung Recycling Zurich (ERZ) >

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.

Stadt Zürich
Entsorgung + Recycling



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 Next-Generation Security Platform

Subscriptions //
Traps Advanced Endpoint Protection and WildFire

Appliances //
PA-4020

With approximately 900 employees, ERZ Disposal and Recycling is the largest service department in the Civil Engineering and Waste Department of Zurich.

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.

"Our legacy anti-virus solutions weren't equipped to protect us from these sophisticated attacks," says Julio Lorenzo, Leader, Group Field Infrastructure for ERZ. "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."

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*

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 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."

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. 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™.*

"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."

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 behavioural 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.

INTRODUCTION>
SOLUTIONS>
CASE STUDY>

LEARN MORE>

paloalto NETWORKS®

Breaking the Cyber Attack Lifecycle >

How Prepared Are You? >

More information >

BREAKING THE CYBER ATTACK LIFECYCLE

A new approach to prevention and resilience.

HOW PREPARED ARE YOU?

Our Next-Generation Security Platform protects every corner of your organization — from your mobile workers to the core of your cloud-enabled data center.

Read the White Paper

Watch the video