



ITALIAN MINISTRY OF THE INTERIOR

Italian Ministry of the Interior Combats Cyber-threats and Enhances Long-Term Security Posture with RSA

AT-A-GLANCE

Challenges

- As a provider of services to citizens and other government departments, the Italian Ministry of the Interior must ensure it remains resistant to cyber-attacks.
- It needed to improve visibility across its network in order to identify and combat threats proactively, and to control access to its services.

Results

- RSA NetWitness® Logs and Packets enables the Ministry to capture data and turn it into actionable information, masking sensitive details when necessary.
- It is now able to better understand attacker behaviour and combat threats more quickly and proactively.
- Combining RSA NetWitness Logs and Packets with RSA NetWitness Endpoint and RSA Web Threat Detection has given the organization a greater level of network visibility.

“RSA NetWitness Logs and Packets is my best colleague because it provides the correct information – not just data...It has completely changed our approach to security.”

STEFANO PLANTEMOLI, SECURITY MANAGER, ITALIAN MINISTRY OF THE INTERIOR

The Italian Ministry of the Interior is responsible for internal security and the protection of constitutional order, for civil protection against disasters and terrorism, for displaced persons and administrative questions. The personal policies department manages the Ministry's human and financial resources, as well as its IT coordination.

Why is security important to you?

Security is mission critical for us. We offer a lot of services to citizens and other government agencies, so it's very important to avoid becoming a cyber-attack target.

How did you go about meeting your security goals?

We focused on technology. We needed something to help us analyze our network and control access to our services. In the future we also want to be able to move to software that can govern our processes and the flow of information through the organization.

We needed a solution to gain better visibility in order to understand and stop the threats we were facing.

Why did you choose to work with RSA?

RSA has a specialist focus on IT security. I invested in RSA NetWitness Logs and Packets three years ago and since then I have seen the platform grow, and it always meets my needs. Another important aspect for me is the contribution made by RSA Professional Services. They're knowledgeable and well trained and I'm very satisfied with the work they've done.

How have you used RSA NetWitness Logs and Packets?

We received a lot of unforeseen traffic during an election day. When we saw the spike of traffic, we began to think it was a DDOS attack. We then had a number of problems with our firewall, in particular with the IPS. We decided to turn off the IPS as we were already using RSA NetWitness Logs and Packets and knew we could use it to analyze the session and stop the attack. It was very useful, because when I turned off the IPS on the firewall, we still had the resource to provide the services our citizens needed during an election day.

What value does RSA NetWitness Logs and Packets offer you?

RSA NetWitness Logs and Packets is my best colleague because it provides the correct information – not just data – so that I see not only the IP but also the IP reputation and behaviour of any possible threat. It's very powerful. The tool enables me to capture this information, and I can mask it on the dashboard if it's sensitive. The tool is very flexible, it's very scalable and I can decide from which DMZ to capture the traffic.

It has completely changed our approach to security, because now we have the control to

capture some traffic and accept some sessions to investigate them and see how an attack has been made. Before RSA NetWitness Logs and Packets we just had a prevention solution. If we knew the threats and the approach they took, we could stop an attack, but if we didn't know the approach or it was a zero-day attack, we wouldn't be able to. Now with RSA NetWitness Logs and Packets we can understand attacker behaviors and then apply the right policy to stop them. When a new vulnerability comes out, RSA is able to develop a new parser and new correlation rules, so we can start analyzing our own ability to combat it very quickly.

Now I know that I can release new services to our citizens and support new access methods for our customers and users.

What other RSA solutions do you use?

I started with RSA NetWitness Logs and Packets but we also deployed RSA Web Threat Detection, which is another powerful tool. We also use RSA NetWitness Endpoint to protect our servers and workstations and it has enabled us to start on a journey to better understanding threats across our whole system. It's helped us gain a lot of information and made us very skilled on malware.

What are the next steps in your journey with RSA?

When we started working with RSA, we were at an initial level. Today we are working to move up to the intermediate level and we're planning to use RSA Archer to extract incident information and build processes and an SOC for incident management.

CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.rsa.com

©2016 EMC Corporation. All rights reserved. EMC, RSA, the RSA logo, RSA NetWitness Logs and Packets, RSA NetWitness Endpoint and RSA Archer are the property of EMC Corporation in the United States and/or other countries. All other trademarks referenced are the property of their respective owners. Italian Ministry of the Interior