



Italian Supermarket Leader Gruppo Finiper Uses TippingPoint to Block Malicious Attacks

The Challenge: While Gruppo Finiper has always placed a priority on carefully managing upgrades and access for individual workstations, store officials recognized that those measures were simply not enough to protect the network against outside intrusions. With such a vast and diverse network to manage, Gruppo Finiper needed a way to analyze incoming network traffic and block malware attacks.

“Our network is large, so it is very difficult to constantly monitor all traffic and update the operating system on all machines,” says Giovanni Oteri, head of information technology at Gruppo Finiper. “But without this ability, we were leaving ourselves open to malicious attacks.”

Why TippingPoint

Gruppo Finiper was determined to weigh their options carefully, so they conducted extensive trials, pitting TippingPoint’s Intrusion Protection Systems (IPS) against other leading offerings. By far, TippingPoint tipped the scale—by delivering the IPS that responded best to Gruppo Finiper’s exacting requirements. The solution includes continuous data packet checks, frequent filter updates and a leading-edge intrusion prevention platform.

Gruppo Finiper’s IPS is based on the TippingPoint Threat Suppression Engine (TSE), a dedicated hardware platform that employs state-of-the-art technology capable of running thousands of checks on each data packet without blocking network traffic. This parallel processing approach ensures a continuous flow of packets inside the IPS with a latency lower

than 84 microseconds, regardless of the number of filters applied.

Another critical advantage is the filters themselves, known as TippingPoint Digital Vaccine®. Developed at DV Labs, TippingPoint’s world-renowned research organization, Digital Vaccines are designed to pinpoint the source of an attack—from the simplest one to the most complex—without compromising network performance. Depending on the need, Digital Vaccines are updated twice a week, or immediately after critical threats and vulnerabilities are discovered.

In addition, DV Labs teams document attack characteristics, enabling Gruppo Finiper IT staff to get frequent updates on problems caused by worms or viruses.

TippingPoint simultaneously applies filter types to detect protocol anomalies, statistical traffic anomalies, prevent distributed denial of service attacks, and block or rate-limit traffic from unauthorized applications such as peer-to-peer file sharing.

“As we saw with the Conficker outbreak, it is easy to block a company’s entire network. In our case, nothing has happened because TippingPoint IPS has blocked all the attacks, and we have been warned in real time of their development, so we have had enough time to develop a defense strategy, even in the unfortunate event that the malware—despite the IPS—entered the network.”

Giovanni Oteri
Head of Information
Technology
Gruppo Finiper

In all, Gruppo Finiper uses more than 30 TippingPoint IPS, installed in conjunction with the firewall, to analyze inbound data center traffic.

- Data center—two TippingPoint 1200E systems with an aggregate throughput of 1.2 Gbps, capable of handling more 750,000 connections per second.
- Data rooms at store locations—30 TippingPoint 210E systems, with an aggregate throughput of 200 Mbps, capable of handling more than 8,000 connections per second.

“Undoubtedly,” Gruppo Finiper’s Oteri says, “this form of protection is the most effective way to defend networks from attack.”

In the future, Gruppo Finiper plans to implement a TippingPoint solution for Network Access Control (NAC), to help implement consistent network security policies for users and IT equipment. The company plans to extend the IPS already in place to solidify network access control and firmly establish uniform security policies.

Benefits_Summary

Today, Gruppo Finiper credits TippingPoint IPS with providing excellent network protection from all types of attack, particularly worms and viruses. Installed transparently within the Gruppo Finiper network, TippingPoint analyzes packet contents in real time to guard against malicious network intrusions.

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS
European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450
Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999