Case Study

INAIL Secures Data and Services, with the Integrated Approach from Intel Security

Istituto Nazionale Assicurazione contro gli Infortuni sul Lavoro (Italian National Institute for Insurance against Accidents at Work, or INAIL)

Customer profile

The public agency manages mandatory insurance and protects workers against workplace injuries and occupational diseases.

Industry

Public administration.

IT environment

Supporting all the services offered, it includes two data centers, around 2,000 host servers, and 15,000 clients/endpoints. Physical, virtual, and cloud platforms providing web services.

Challenges

To supply the general public with high-quality services always available, in line with the company's mission.

Intel Security Solutions

- McAfee® ePolicy Orchestrator® (McAfee ePO)
- McAfee VirusScan® Enterprise
- McAfee Host Intrusion Prevention
- McAfee Complete Data Protection Advanced
- McAfee Total Protection for Data Loss Prevention
- McAfee Network Security Platform
- McAfee Global Threat Intelligence
- McAfee Advanced Threat Defense
- McAfee Threat Intelligence Exchange
- McAfee Endpoint Threat Protection
- McAfee Web Gateway
- McAfee Event Reporter

McAfee Professional Services

- McAfee Distribution Services

The wealth of sensitive data and information available to INAIL and the services it provides to citizens, businesses, and the Public Administration requires highly effective strategies and decisions in the IT security context. An advanced, multilayered approach is essential for a modern, mature public organization, along with a far-sighted, global vision, which must include a company culture that promotes awareness of the benefits of the responsible use of personal information technology for everybody.

Solutions that meet the demands of an organization like INAIL are also necessary in order to enable an integrated security model at all network levels, including endpoints, to overcome risks and reduce hacking attempts. What is the goal? To reduce costs overall and increase staff productivity in order to maintain the high quality of services delivered. For over 10 years, INAIL has been working with Intel Security to provide total, flexible safeguarding of IT resources, adopting an integrated approach to security management.

The Public Agency Is Also Changing

Since its foundation in 1933, INAIL has worked with citizens, businesses, and the Public Agency to manage workmen compensation insurance, a compulsory requirement for all employers with employees and contractors in industries and settings legally identified as hazardous. Changes to working practices and the ongoing introduction of more advanced technology have led to the INAIL insurance requirement being extended to almost all production and services operations. INAIL also plays a vital role in planning accident prevention and workplace safety policies and in relevant awareness-raising and knowledge-sharing procedures.

IT is at the heart of INAIL's operation, with two data centers designed with business continuity and disaster recovery systems, presently being upgraded for the introduction of Tier 3, according to ANSI/TIA-942 standards for data processing services. The environment includes approximately 2,000 host servers and more than 15,000 clients/endpoints running 300 applications, with an architecture consisting of physical, virtual, and cloud platforms, which deliver services through the web to employees and external users. These numbers and level of complexity require a fully integrated security system that can take advantage of every kind of information and intelligence to ensure full protection.

Security at the Heart of IT

Stefano Tomasini is central manager of the Digital Organization. "Security is vitally important to INAIL", he says. "Bringing the entire IT security process into a single department gives us a complete overview of both the organizational aspects and the behaviors of our employees, which is critical for the implementation of effective security strategies."

It is no accident that INAIL has formed a local security unit, to which CERT, SOC, and application security teams report, with the task of applying best practices for IT security, as defined by the organization. But all INAIL's offices are involved in event management and incident response processes. The agency's mission is to treat security as a process, so that it can be continually improved as a function of experience in the field and the increasing maturity of the players involved.

Results

- Smart security management.
- Fewer endpoint infections.
- Blocks Internet attacks.
- Proactive identification of vulnerabilities in the IT environment.
- Greater visibility at all levels.
- Establishes a corporate IT Security culture.

INAIL's services must never be susceptible to breakdown as a result of computer hacking, in line with the company mission. Escalating threats, more focused and more effective than ever before, mean that INAIL needs to adopt the next-generation of security strategies. "The spread of advanced malware, DDoS attacks, cybercrime, and the IT risks associated with our activities has grown to worrisome levels", explains Tomasini. New trends in technology and attack opportunities associated with the use of mobile devices, virtualization, the cloud, social media, and collaborative working tools also figure into the picture. "It was vital to plan appropriate policies and security solutions to guarantee reliable operation of our IT environment."

In addition to the protection of sensitive data, businesses like INAIL have to comply with current regulations and Public Administration security standards, which require an ongoing commitment to improved management processes and protection from ransomware and DDoS attacks.

Intel Security: An Integrated Approach

For more than 10 years, Intel Security has been playing an important role in INAIL IT Security. The unified, adaptive Intel Security ecosystem enables full integration between all products and services, even from third parties, encouraging real-time intelligence sharing on threats and their context. The Integrated Intel Security model works at all levels of security (endpoint, server, network), and can, therefore, help reduce risk, cutting the volume of events and response times, as well as lowering overall costs and the involvement of operational staff.

Intel Security solutions used by the institute protect hosts, monitor data movement, shield the network perimeter from attacks, normalize internet navigation web content and flag administrators about possible vulnerabilities of managed IT assets.

Together with antivirus and traditional intrusion detection technologies, INAIL can rely on sandboxing capabilities and advanced dynamic analysis of malicious code. INAIL also benefits from real-time sharing of information on possible attacks or harmful files not yet classified, thanks to integration of Intel Security solutions with the cloud.

Protection Safeguards Business

The first and most obvious benefit of Intel Security for endpoints and network perimeter was stopping new threats.

In terms of strategy, INAIL is able to correlate IT-related data more easily, creating an information asset pool that further reduces risk of infection and internet attacks. It is possible to identify vulnerabilities, classify them according to severity, and implement targeted actions to increase overall visibility on the network. This allows INAIL to verify and evaluate the ROI used by the institute to build a reference model in order to evaluate the quantitative value of a security measure before and after.

In day-to-day practice, the local security unit can enjoy the benefits of automatic management and correlation of events, in operational as well as reporting terms. The collected data is not just delivered in the form of reports; it enables INAIL to avoid dangerous situations, quickly activating the correct countermeasures against detected threats.

Intel Security solutions have also enabled INAIL to optimize IT security and respond to the main compliance requirements imposed by the current regulations and by international security standards. These solutions also improve the organization's reputation through more efficient processes, time savings, and lowered operational costs, in line with the needs of a modern business. "Our work is evaluated based on the speed of delivery and quality of execution of a project, with the aim of satisfying those who use our services" says Tomasini.

"The integrated model of Intel Security supports us in reducing risks and response times, as well as cutting overall costs and the involvement of operational staff."

— Stefano Tomasini, CIO

Scalable Technology with Smart Management

The integrated approach offered by Intel Security solutions makes several technologies available with a single management system, positively impacting efficiency and maximizing the benefits of synergy between solutions and event correlation in a secure environment, leading to an overall lowering of management costs.

"The connected Intel Security philosophy enables us to use a consistent, flexible, and centralized system of products that speak the same language and are manageable in an intuitive, integrated way," adds Tomasini.

Thanks to these features, in the future, INAIL will be able to add new modules to the platform with minimal effort and immediate results.

This also applies to add-ons for new technology supplied by Intel Security. "Tools such as McAfee Data Center Security Suite and the connectors for the cloud, both fully integrated with McAfee ePO software, provide a positive response to new security requirements resulting from major technological changes to our IT assets and from international standards. In April 2016, the EU Parliament ratified the European Regulation on Data Protection, that will go into effect throughout the European Union in 2018. The regulation should help Europe deal with the changing digital era and strengthen the rights of European citizens, offering them a powerful tool to control their own personal data and defining a unified and simplified framework of rules and procedures provided for those who, like us, handle personal data," concludes Tomasini.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com