Case Study

Robust Data Loss Prevention for Spain's Leading Occupational Health Not-for-Profit Organization

Umivale

Customer profile
Not-for-profit organization in Spain that collaborates with Social Security to help businesses of all sizes manage occupational health.

Industry
Public health

IT environment
750 Microsoft Windows endpoints running Windows 7 and Windows 10 and 65 Microsoft 2008 Servers, along with multiple browsers, Adobe software, and Microsoft Office 2010 and 2013.

Challenges

- Securing sensitive healthcare and personal data.
- Protecting data at rest, data in use, and data in motion.
- Preventing data exfiltration, achieving compliance, and having better overall control over data.
- Reducing operating costs for IT systems and avoiding other costs associated with regulatory breaches.

Intel Security solutions

- McAfee® VirusScan® Enterprise
- McAfee® Complete Data Protection—Advanced Suite
- McAfee® DLP Endpoint
- McAfee Endpoint Threat Protection
- McAfee ePolicy Orchestrator software

The security analyst at UMIVALE, a not-for-profit organization in Spain that collaborates with Social Security, is confident that the personal information and healthcare records of patients are fully protected, thanks to McAfee® Complete Data Protection—Advanced Suite, McAfee® ePolicy Orchestrator® (McAfee ePO™) software, and other advanced Intel Security endpoint technologies.

Raul Marín, chief IT security analyst at Umivale, firmly believes that he and his team have a social obligation to Umivale's partners and their employees—to serve as a trusted custodian of the healthcare and sensitive personal data of workers in Spain.

Headquartered in Valencia, Spain, Umivale has approximately 700 employees and supports more than 55,000 businesses of all sizes and across all sectors—from multinational enterprises with more than 30,000 employees to national banks to medium-size and small businesses. With its close ties to Spain's Seguridad Social (Social Security) administration, Umivale is required to maintain strict adherence to regulatory mandates relating to occupational healthcare data and worker privacy.

In his role at Umivale, Marín is "constantly keeping an eye out for threats that may put the organization at risk or may potentially cause a data breach. We cannot afford, in any way, to compromise the privacy and well-being of our 600,000 constituents in the Spanish workforce. We are first and foremost concerned about upholding our obligations to our clients and to maintaining the privacy and safety of their healthcare data. Our clients are aware that we hold ourselves to a high standard of information security."

Governed by Rigorous Best Practices

Marín and his team are meticulous about applying the highest possible level of security controls across all components of the organization's primarily Microsoft-based environment, which includes 750 Microsoft Windows endpoints running Windows 7 and Windows 10 and 65 Microsoft 2008 Servers, along with multiple browsers and common applications like Adobe software and Microsoft Office 2010 and 2013.

At Umivale, application deployment is centralized and application usage is carefully monitored. "Our infrastructure does not allow users to operate outside the established parameters. This protects both the organization and the individual user. These operational restrictions help us avoid potential problems. Every change is monitored and inventoried strictly. Everything has been designed with prevention in mind."

In addition to vigilant monitoring of all systems, Marín and his team ensure that all endpoints and workstations have the latest .DAT updates. They also have standardized access protection rules to minimize the probability of compromise by next-generation threats like CrytoLocker ransomware malware.

intel Security

"Intel Security DLP solutions offer a wider array of capabilities and met all our criteria: prevention of data exfiltration, compliance, and better control over sensitive data. Also, we have more control than we've ever had before over confidential data that moves across mobile devices and other channels."

—Raul Marín, Chief Security Analyst at Umivale

Results

- Improved monitoring of input and output flows of sensitive information in the organization.
- Increased protection against attacks and the ability to derive statistics and reports that allow for continuous improvement of safety procedures.
- Improved utilization and enforcement of policy through preconfigured and customizable rule sets.
- Analysis of the volume and contexts of terminology associated with health treatments.
- Faster data protection.

Solution: Integrated Intel Security Solutions Support Umivale's Security Best Practices

Marín and his team have been able to adhere to their rigorous methodologies through the deployment of multiple Intel Security technologies for more than 18 years. "The best proof of the effectiveness of Intel Security solutions is that we've had very few incidents over the years." Currently, user workstations and servers are protected by McAfee VirusScan Enterprise and McAfee Endpoint Threat Protection. Integration with McAfee ePO software provides the security group with centralized, single-pane-of-glass visibility to both user behavior and potential threats.

"With the McAfee ePO console, we can quickly detect and respond to malware that may enter via archives and see how many times antivirus has been activated over time for a historical perspective," says Marín. "In addition, we appreciate rules-based access protection, which doesn't permit an executable archive to reside in the temp folder, nor does it permit installation of unauthorized screensavers by users, for example. Intel Security products have also protected us from encryption-based ransomware attacks. We've had multiple instances of these and have been able to successfully mitigate all of them."

Marín also notes that deployment of Intel Security products has been economical, reducing Umivale's IT operational costs and resulting in avoidance of costs associated with breaches. "We've been able to thwart hundreds of attacks with these solutions," he says. "This would not have been possible without the comprehensive and detailed reports and statistics generated by McAfee ePO software."

McAfee Data Loss Prevention Extends Control Over Sensitive Healthcare Data

Over time, Marín and his team have made sure that all the bases are covered—with antivirus, antispyware, firewall, demilitarized zones (DMZ), network traffic analysis, access protection, and encryption for email. However, maintaining control over sensitive data has been a significant challenge for the organization, which handles hundreds of thousands of client healthcare records on a daily basis.

As Marín puts it, "As users create documents and share documents, there has always been a percentage of data over which we've lacked control. Webmail, the use of smartphones, and other popular technology trends have opened up new threat vectors. And it's impossible for us to restrict the flow of data because data creation and exchange is essential to the services we provide—which is why we decided to investigate Intel Security's data loss prevention solutions."

Marín undertook a thorough evaluation of data loss prevention (DLP) solutions from a variety of vendors. He discovered that most vendors have a management console for their antivirus products, but not for DLP. In addition, he found that the rule sets offered by some vendors were limited and generally did not include applications. "Intel Security DLP solutions offer a wider array of capabilities and meet all our criteria: prevention of data exfiltration, simplified compliance, and better control over sensitive data. Also, we have more control than we've ever had before over confidential data that moves across mobile devices and other channels," affirms Marín.

After doing its due diligence, the Umivale security staff deployed McAfee Complete Data Protection—Advanced Suite and McAfee DLP Endpoint company-wide. Now Marín and his team are assured that all endpoints at Umivale are secured. Additionally, they have the ability to quickly identify and classify sensitive data that is important to Umivale's operation based on document location, author, and other characteristics.

Another benefit is that Marín and his team can get a clear understanding of the data that moves in and out of the organization and then can swiftly establish and enforce policies based on this knowledge. Integration with McAfee ePO software simplifies DLP management and provides Marín's teams with a unified view of the entire Umivale environment and the organization's overall security posture.

"With Intel Security DLP products, we can establish rules for proper management of unstructured data. It's fantastic that we can now ensure that email with confidential healthcare data is encrypted," says Marín.

Building on a Strong Foundation of Data Protection

After spending some time getting to know Intel Security DLP solutions, Marín and his team took it upon themselves to develop their own proprietary tool that integrates with McAfee ePO software and that extends its capabilities to identify sensitive information even more accurately.

They began by aggregating healthcare terminology that would apply to at least 80% of the documents that flow through Umivale and then established lookup dictionaries. Now, Marín and his team can use the McAfee ePO console to quantify how many times a healthcare-related word or phrase appears in files and run all the contexts where the word appears and then separate those occurrences from false positive instances of terms that are unrelated to healthcare. This facilitates the identification of previous and subsequent actions taken on those files. This is made possible only through the integration capabilities of Intel Security's open and connected architecture.

"Taken together, Intel Security products—and especially the DLP solutions—have provided us with distinct advantages in so many areas. On an organizational level, these technologies have helped us make better, more informed decisions, and they have helped us refine our standardized processes," says Marín. "Most importantly, we can gain a better understanding of what goes on in the organization, we can respond more rapidly when incidents occur, and we can fine-tune our policies with greater precision."

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com