SentinelOne™

Sant'Anna
Scuola Universitaria Superiore Pisa

Scuola Superiore Sant'Anna Maintains Openness Without Compromise

SentinelOne protects every endpoint against every type of attack and automates remediation

The Challenge: Balancing Openness with Ransomware Protection

Scuola Superiore Sant'Anna is committed to driving innovation and research in disciplinary fields ranging from applied sciences to social sciences. As an independent public university, the school provides students with a diverse range of experiences that integrate closely with their studies. Programs emphasize applied research in biorobotics; life sciences; communication, information and perception technologies; law, politics and development; and economy and management.

Faculty, students, and research groups collaborate with many external organizations, which demands an open, flexible network infrastructure. Users are also highly mobile, often conducting research and storing sensitive or confidential data on their devices in field situations with unsecured connectivity. These factors make it impossible to apply stringent corporate security models and data controls to the school's environment. At the same time, it is essential to protect devices and data against malware and other advanced threats while meeting European privacy and regulatory requirements.

CHALLENGES

- Defend mobile systems and valuable research data against attackers
- Secure highly mobile users and the use of cloud-based analysis services
- Minimize total cost of ownership while achieving advanced protection

SOLUTION

- SentinelOne Endpoint Protection Platform

BENEFITS

- Extended protection to every endpoint—desktop, mobile, and in the cloud
- Prevented ransomware infection and automated remediation
- Reduced risk and lowered security cost of ownership

Balancing security with openness had become a significant challenge. Higher education institutions have become profitable targets for attackers seeking Personally Identifiable Information (PII), which can sell on the dark web for $200 per record. Hundreds of cyber attacks were launched against higher education institutions in 2017, resulting in leaks of valuable scientific, engineering, medical, and defense research. The Sant'Anna School's antivirus solution was not catching advanced threats effectively. Cloud-based research analysis services were difficult to secure, and available advanced threat protection products relied heavily on signatures or whitelisting applications, which simply does not work in this environment.

Dr. Italo Lisi
Chief Information Officer, Scuola Superiore Sant'Anna

"SentinelOne completely automates our response to ransomware. It reverses changes to registry and system settings, instantly rolls compromised files back to their previous condition, and prevents other network systems from being infected. It is impressive to see it work."

"Our existing threat prevention measures help secure the school's network perimeter and internal networks," said Dr. Italo Lisi, Chief Information Officer of Scuola Superiore Sant'Anna. "However, the same measures are not easily extended in our environment with highly mobile users and cloud-based research."

For example, if a researcher is studying migration flows in Libya, personal and sensitive data should be protected with the same level of defense enjoyed by researchers locally or in Europe. However, the school could not rely on full connectivity to analyze possible threats using cloud-based services. Managing whitelist-based security solutions presented similar difficulties. Because researchers require access to a diverse range of applications, domains, and Internet resources, the school could not use a "block-by-default" policy and restricted the installation of new applications.

"To preserve openness without compromising security, we focused our attention on behavior-based security protection products," said Dr. Lisi. "Our unique needs demanded an innovative, advanced type of endpoint protection."

An Effective, Flexible Protection Solution

During Dr. Lisi's team's searched for a new solution, they learned about SentinelOne from the Gartner Magic Quadrant for endpoint security solutions. They also reviewed numerous independent reports and sought the opinions of similar universities.

"A study from NSS Labs particularly impressed us," said Dr. Lisi. "NSS Labs assigned SentinelOne a very high score for its effectiveness, a well as a cost per single endpoint significantly lower than that of major competitors. We tested all major solutions, and we chose SentinelOne based on our results."

Vista Technology, a SentinelOne partner, worked with Scuola Superiore Sant'Anna to deploy SentinelOne across its laboratories, research centers, and administrative desktop computers. Dr. Lisi's team included SentinelOne in the school's automated software provisioning system for fast, easy deployment.

Any User, Any Environment

SentinelOne delivered the endpoint protection that the school needed for both Windows and MacOS systems. The same protection that defends desktop systems now protects mobile users as well, whether they are online or offline. The school expects SentinelOne to protect every endpoint against every type of attack, at every stage of the threat lifecycle with no impact to users.

Nothing Escapes Detection—or Remediation

Behavior-based detection enables Scuola Superiore Sant'Anna to prevent ransomware and other infections from advanced attacks. Because it doesn't rely on signatures or application whitelists, SentinelOne protects the school against the latest and unknown malware, exploits, and live and insider attacks. Threats are detected and stopped at machine speed, preventing them from establishing a foothold in the school's network or spreading to other systems.

"SentinelOne completely automates our response to ransomware for Windows endpoints supporting Microsoft Volume Shadow Copy Service," said Dr. Lisi. "It reverses changes to registry and system settings, instantly rolls compromised files back to their previous condition, and prevents other network systems from being infected. It is impressive to see it work."

High Expectations

The school is performing an extended testing process to collect specific data on SentinelOne's effectiveness. With unprecedented visibility into the actual threats targeting the school, the team can now use threat data to drive overall risk reduction effectively and enhance existing security measures.

"We expect SentinelOne to help us achieve significant reduction in risk," said Dr. Lisi. "We also expect it to simplify security infrastructure management and lower the cost of security operations. We're confident that it will meet our expectations."

SentinelOne™

For more information about SentinelOne Endpoint Protection Platform and the future of endpoint protection, please visit: sentinelone.com.