semperis

CASE STUDY MAIRE

MAIRE

Isaac Newton famously said, "If I have seen further than others, it is by standing on the shoulders of giants." The spirit of that concept drives the innovations coming from MAIRE group, a global technology and engineering organization focused on advancing the Energy Transition. This visionary Group, which traces its origins back 150 years, applies the past century's advancements to today's challenges—and transforms what comes next.

> The potential loss of Active Directory is a scenario that requires dedicated planning, specialized tools, enhanced monitoring capabilities, and an automated recovery capability. These are areas where Semperis gives us a much higher level of confidence and readiness."

Andrea Licciardi
Senior Cyber Security Manager

IDENTITY SECURITY FOCUS REDUCES RISK AND SOLIDIFIES RESILIENCE FOR MAIRE

Supporting MAIRE's global operations across international engineering hubs, large project sites, advanced collaboration systems, and digital platforms requires an extensive, distributed, and dynamic IT environment. Even a relatively minor cyber incident has the potential to disrupt routine operations.

Ensuring the security and resilience of MAIRE's powerful digital engine is the responsibility of Senior Cyber Security Manager Andrea Licciardi and his team in the Cyber Risk Operation Center (CROC). Because Active Directory is the heart of that engine, they turned to Semperis for the specialized identity security expertise they require.

"In an organization like MAIRE group," says Licciardi, "security is no longer a purely technical matter. It is fundamentally about business continuity, risk management, and protecting the value the Group delivers every day across its global projects."

THE CHALLENGE: MAKING SECURITY A STRATEGIC ADVANTAGE

For MAIRE, cyber resilience is business resilience.

With operations across 50 countries and nearly 10,500 people (supported by 50,000 global professionals), the CROC team oversees a hybrid architecture spanning distributed cloud, integrated legacy systems, and a digital identity infrastructure that's the entry point for activity across the company.

The mandate: keep security, performance, and reliability consistent as the ecosystem grows.

"In this context, technology is not just an enabler—it is a core component of the Group's industrial mission," says Licciardi. "It allows us to make data-driven decisions, ensures the continuity of global operations, and provides the digital backbone needed to deliver complex projects safely, transparently, and efficiently."

The environment is complex not just because of its scale but also because of the work it enables: high-end engineering, global supplier management, execution of critical industrial projects, and an ecosystem of partners that requires interoperability, security, and speed. The CROC is more than a security operations center (SOC); it is a centralized resource for risk assessment and management, aligning cybersecurity activities with business goals.

"Inside the CROC, we don't simply react to alerts. We interpret them, we connect them to the business, and we assess their real impact," Licciardi explains. For example, "a vulnerability in a domain controller is not just a technical concern; it may represent a risk for a project site, a contractual deadline, or a strategic partnership."

"Our responsibility is not purely technical—it's strategic," says Licciardi. "Security has become a competitive advantage, directly influencing the Group's ability to deliver complex projects."

PUTTING IDENTITY SECURITY AT THE HEART OF CYBER RISK MANAGEMENT

As the company's access gateway, AD supports the entire identity ecosystem—and must be treated as a strategic asset. The MAIRE team centers its activities in four key areas:

- Protect global operational continuity under pressure from advanced threats or unexpected events
- Strengthen digital identity and access security by protecting identity assets, reducing attack surfaces, and eliminating hidden risks
- Reduce cyber risk across the Group's complex supply chain ecosystem
- Enable innovation through security, automation, and AI

> "Identity is one of the most sensitive elements of any digital environment. If an attacker compromises Active Directory, the entire company is at risk."
>
> **Andrea Licciardi**

The team recognizes AD as both an advantage and a potential source of vulnerability. Cyber attackers increasingly target digital identities and critical infrastructure, relying on:

- Identity compromise as the primary entry point
- The difficulty of detecting anomalies in complex environments
- The opportunity to deliver operational impact at global scale

In hybrid and distributed environments, distinguishing legitimate activity from suspicious behavior is not straightforward. Over time, the attack surface grows, identities multiply, and systems interconnect in new ways—enabling an attacker to move silently within the noise of daily operations.

MAIRE's team has diligently structured the AD environment to minimize risk. Even so, Licciardi acknowledges they must be ready for incidents from any angle—especially across the on-premises/cloud boundary with Entra ID.

"Being prepared and trained is essential to ensuring continuity and reliability even in the most challenging situations," he emphasizes. "The potential loss of Active Directory is a scenario that requires dedicated planning, specialized tools, enhanced monitoring capabilities, and an automated recovery capability. These are areas where Semperis gives us a much higher level of confidence and readiness."

CHOOSING SEMPERIS: AD-SPECIFIC SOLUTIONS FOR FULL-LIFECYCLE IDENTITY SECURITY

Before Semperis, MAIRE had advanced backup platforms, mature cybersecurity tools, and a modern SIEM. What was missing? A solution specifically designed to protect, monitor, and recover Active Directory.

"The issue wasn't only technical," says Licciardi. "It was also about time, prioritization, and our ability to react effectively. Without a platform specifically designed to analyze, protect, and recover Active Directory, the team had to rely on manual checks, iterative analyses, and processes that couldn't meet the required level of granularity or confidence."

Those AD-specific requirements made Semperis an easy choice. They selected three solutions that cover the full identity threat detection and response (ITDR) lifecycle:

- Directory Services Protector (DSP)
- Disaster Recovery for Entra Tenant (DRET)
- Active Directory Forest Recovery (ADFR)

These solutions addressed specific operational pain points.

DEEPER VISIBILITY WHERE IT MATTERS MOST

The SIEM generated extensive logs and events, but could not provide native, context-aware understanding of Active Directory's internal logic. The CROC team needed to correlate identity risks, detect subtle misconfigurations, and surface behaviors that generic platforms miss.

"We needed a platform to transform this workflow from 'manual and reactive' to 'automated, monitored, and recovery-ready,'" says Licciardi.

DSP and DRET provide clear visibility into drift, anomalous changes, exposures, and configuration deviations. Inside the CROC, these signals are linked immediately to operational impact:

- Which project could be affected?
- Which accounts matter most?
- Which services could stop?

This visibility enables faster, informed decisions.

RECOVERY IS A CERTAINTY, NOT A HYPOTHESIS

For the CROC team, the most critical element was recovery speed after a compromise.

"Our backup tools were excellent for data, workloads, and applications, but they were not built to orchestrate a secure and reliable restoration of the entire Active Directory forest," Licciardi explains.

With ADFR, identity recovery becomes automated, testable, and repeatable—no longer a manual effort or best-case assumption.

"Now, we can face the worst-case scenario without losing the ability to operate," says Licciardi.

COMPLIANCE: DATA-DRIVEN, CONTINUOUS, AUTHORITATIVE

Semperis solutions reshaped the team's approach to compliance audits—and the tone of those conversations.

"When you bring clean, verifiable data to the table, an audit becomes a professional dialogue, not a debate over interpretations," says Licciardi.

Previously, audit preparation depended on manual evidence gathering and cross-checks. Today, auditors demand:

Clear, immediate evidence: DSP and DRET provide rapid views of AD state, critical changes, and exposures.

"We no longer 'explain' our security posture," Licciardi says, "we show it."

- **A measurable, standards-aligned identity posture:** Every aspect—domain hardening, access governance, privilege oversight, drift detection, recovery—is tracked, contextualized, and easily validated.
- **Demonstrable resilience, not just compliance:** Auditors don't ask only "What controls do you have?" but "How quickly can you get back up?" With ADFR, MAIRE demonstrates an automated, documented, repeatable recovery model.

"This isn't theory; it's a process we can execute, test, and validate," Licciardi says.

A MORE MATURE OPERATIONAL CULTURE

Clear visibility, precise alerts, and native recovery capabilities have fostered closer collaboration among IT, cybersecurity, and operations. Conversations are more data-driven, decisions faster, and awareness of identity-risk awareness higher.

Semperis supports the CROC team's mission—not as another tool, but as the platform to monitor, protect, and, when necessary, restore the identity infrastructure at the most critical moments.

With AD-focused tools, people work with more clarity, speed, and alignment. The CROC becomes a place for aware decisions. The result: reduced risk, reinforced continuity, and sustained industrial value.

OPERATIONAL RESILIENCE THAT'S MEASURABLE, NOT THEORETICAL

Before Semperis, Licciardi's team had theoretical trust they could recover from a full AD compromise. Today, with a purpose-built platform for forest-wide recovery, they have concrete confidence grounded in specialized tools, automation, clear procedures, and worst-case-ready design.

With DSP, DRET, and ADFR, they have an industrial-grade AD recovery platform that enables:

- Operation with certainty, not assumptions
- Reduction of manual effort with automated, tracked, and verifiable actions
- Deeper, clearer understanding of the digital identity landscape

> "Semperis has given us the ability to observe our identity environment with uncommon depth. Today, we don't simply 'manage' Active Directory, we govern it, monitor it continuously, protect it as a strategic asset, and consider it part of how we deliver value as a business."
>
> **Andrea Licciardi**

ABOUT SEMPERIS

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid Active Directory environments, Semperis' patented technology protects over 100+ million identities from cyberattacks, data breaches, and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, New Jersey, and operates internationally, with its research and development team distributed throughout the United States, Canada, and Israel.

Semperis hosts the award-winning Hybrid Identity Protection conference and podcast series (www.hipconf.com) and built the community hybrid Active Directory cyber defender tools, Purple Knight (www.purple-knight.com) and Forest Druid. The company has received the highest level of industry accolades, recently named to Inc. Magazine's list of best workplaces for 2023 and ranked the fastest-growing cybersecurity company in America by the Financial Times. Semperis is a Microsoft Enterprise Cloud Alliance and Co-Sell partner and a member of the Microsoft Intelligent Security Association (MISA).

semperis