Magic Stone helps Protecting Innovation in the Semiconductor Sector

Client Overview

A leading manufacturer of plasma-based semiconductor equipment, with over 300 systems deployed globally. The company serves critical roles in the integrated circuit fabrication process through advanced plasma technologies.

Importance

Cyber security is critical in the semiconductor industry due to the highly sensitive intellectual property (IP), proprietary manufacturing processes, and the role of semiconductors in national infrastructure and defense systems. A breach can result in severe financial loss, operational disruption, reputational damage, and potential national security implications.

Priority

Cybersecurity is a strategic priority. With rising threats and geopolitical risks, protecting design data, processes, and partners is essential. Cyber resilience isn't optional—it's vital for business continuity and trust.

Key Challenges

The semiconductor industry faces a unique set of cybersecurity challenges driven by its complex operations, high-value, intellectual property, and global footprint. Securing such an environment means navigating:

- **Complex supply chains**, with diverse and international vendors that are difficult to secure and monitor end-to-end
- **Legacy OT systems** integrated with modern IT networks, creating visibility and control gaps
- **IP protection demands**, as proprietary chip designs and process data are prime targets for cyber espionage
- **High-velocity R&D environments**, where rapid innovation can easily outpace security controls
- **Insider threats**, with employees and contractors having privileged access to critical systems and data

Addressing these challenges requires a security strategy that goes beyond traditional IT defense—one that is built for the realities of high-tech manufacturing and intellectual property protection.

Compliance Standards

Companies in the semiconductor industry must meet some of the world's most demanding cybersecurity and data protection standards. The client aimed to align with leading cybersecurity standards such as **ISO/IEC 27001** and **IEC 62443**, while also preparing for evolving regulatory demands like **GDPR** and **NIS2**. With many overlapping frameworks in play, they needed a security strategy that was both technically robust and audit-ready—capable of supporting compliance across global markets without slowing innovation.

How did Magic Stone addressed the challenges

Stage one – deploying ITsMine

Magic Stone began by deploying ITsMine to secure the client's most valuable assets—chip designs, engineering files, and proprietary process data. The solution ensured full control over sensitive information, even beyond company boundaries, helping prevent data leakage and insider threats.

In addition, it added a vital layer of ransomware protection. If a breach were to occur, the platform's "red button" feature could instantly destroy compromised data—ensuring attackers walk away empty-handed. Combined with early detection of abnormal behavior, this gave the client both peace of mind and practical defense—without disrupting their agile R&D operations.

Stage Two – TPRM with Rescana

In the second stage, Magic Stone implemented Rescana to provide autonomous visibility into the client's third-party ecosystem. With an international network of vendors, managing external cyber risk manually was no longer scalable.

Rescana continuously assessed supplier security posture without requiring questionnaires or direct system access. Its automated risk scoring identified vulnerabilities, exposed assets, and compliance gaps—mapped to key standards like ISO 27001 and NIS2.

This allowed the client's team to replace time-consuming manual reviews with real-time, actionable insights, saving valuable time while improving control over supply chain security.

Results

By combining data-centric protection with autonomous third-party risk management, Magic Stone delivered a focused, high-impact improvement to the client's cybersecurity posture.

- Sensitive data remained protected, even beyond the organization's perimeter—without disrupting agile R&D workflows
- Insider and ransomware threats were neutralized proactively, backed by the option to destroy compromised data instantly
- Third-party risk visibility shifted from static to real-time, allowing the client to make faster, smarter decisions across its global vendor network
- Compliance readiness improved significantly, with continuous alignment to frameworks like ISO 27001, GDPR, and NIS2

- The client gained stronger control with less complexity, saving time and reducing operational burden on internal security teams

Together, these steps provided not just protection—but resilience, autonomy, and peace of mind in one of the most targeted industries in the world.

Conclusion

In a threat landscape where ransomware, data leakage, and supply chain risks are escalating, Magic Stone delivered exactly what the client needed: focused, expert-led protection without added complexity.

By addressing both internal and external risk vectors—starting with sensitive data and extending through third-party ecosystems, we helped the client move from reactive defences to proactive resilience. All without adding noise, complexity, or slowing innovation.

This case reinforces what we believe: you don’t need a dozen disconnected tools—you need specialists who know where to look, how to act, and what actually works.