Security Scorecard

CASE STUDY

MAX for Global Technology Provider

Fortune 500 company increases capacity for strategic risk management projects

SecurityScorecard MAX streamlines assessments and continuous monitoring

The Challenge: Time consuming requirements

A global technology company faced challenges in managing high risk suppliers that required comprehensive cybersecurity assessments every two years and continuous monitoring. This process included on-site, SIG Lite, or other types of vendor risk assessments that are time-consuming, resource-intensive, and often yield limited new insights, particularly for major cloud and telecom providers. The need to maintain compliance with industry best practices, such as SOC 2 and ISO 27001, while optimizing internal resources, also became a critical imperative.

Key Benefits

- Optimized resource allocation
- Enhanced audit and compliance support
- Direct and expert vendor engagement

About the Customer

The customer's engagement with SecurityScorecard is primarily driven by two key internal teams focused on risk management. One team specializes in supply chain security and privacy, ensuring that external vendors and suppliers adequately protect critical data. The other team focuses broadly on IT risk management, encompassing both internal IT risks and third-party cybersecurity risks related to the supply chain. Together, these teams are responsible for maintaining a robust security posture across the organization's extensive vendor ecosystem.

> “
> Our focus shifted to higher-visibility projects, dedicating resources to critical business areas.
>
> Cybersecurity Risk Management Lead

Customer Info

Industry

Technology, Manufacturing

Headquarters

United States

Products

MAX Managed Services

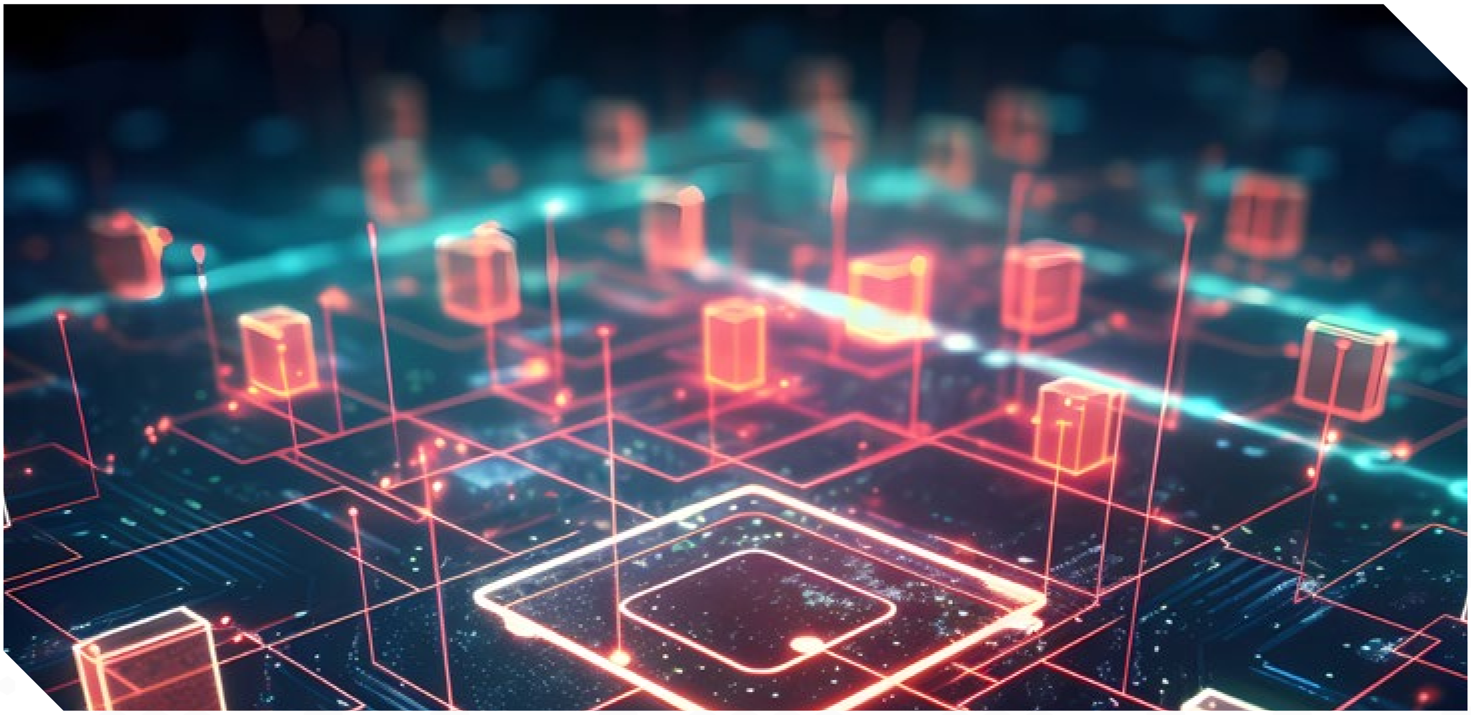
SecurityScorecard.com
info@securityscorecard.com

The Solution: Cyber risk staff augmentation

To run a scalable and efficient third-party risk management program, the customer adopted MAX, SecurityScorecard's managed service. While already leveraging SecurityScorecard's SecurityRatings for continuous monitoring of a broader set of suppliers, the customer gained an extension to its risk management team to act as an outsourced arm for direct vendor engagement and remediation support.

The cornerstone of MAX are its incident likelihood assessments, which focus on controls that are known to be root causes of security policy violations. These assessments can be performed instantly and are updated on a quarterly basis. MAX also operates a 24x7 Vendor Risk Operations Center (VROC) which continuously analyses thousands of signals, findings, and indicators, using its expert insight to alert the customer to the most significant breach indicators and advise on trends across all vendors. When signs of escalating risk like exposure to known exploited vulnerabilities (KEVs), leaked credentials, and ransomware infections are detected, the MAX team will personally meet impacted vendors, explain the findings, and deliver remediation advice. This supply chain incident response capability ensures issue resolution, usually within 48 hours, and shields the customer from fire drills that are disruptive to the risk management team.

> “
>
> Having the ability to have vendors be automatically alerted to issues and having the MAX team engage with the vendors directly to advise them is really beneficial.
>
> Cybersecurity Risk Management Lead



The Result: Optimized resource allocation

The adoption of SecurityScorecard's MAX Services has optimized resource allocation and enhanced compliance. By having SecurityScorecard handle important but less valuable vendor assessment work, the customer's third-party risk management team gained significant capacity to pivot its focus to more complex vendor risk analysis and critical IT risk management projects. This strategic reallocation of resources has improved the overall security posture and operational efficiency of the organization

> “
>
> **MAX gets the people that should be talking about supply chain risk together to resolve the issues.**
>
> Supply Chain Security Lead

Increased capacity for strategic projects

Outsourcing risk management tasks increased the internal team's ability to dedicate more resources to mission-critical initiatives and innovative projects directly tied to core business goals. They could prioritize strategic IT risk management efforts, develop new security frameworks, and proactively address emerging threats, rather than being bogged down by routine vendor oversight. This shift enabled a more impactful and forward-looking approach to security across the enterprise.

Enhanced Audit and Compliance Support

The documentation provided by SecurityScorecard supported SOC 2 compliance certification, satisfying auditors' requirements for continuous monitoring. The audit-ready format was easy to review and auditors did not have any follow-up questions. This has simplified the compliance process, ensuring the company adheres to industry best practices without overburdening internal staff. Adherence to standards like SOC 2 allows the company to maintain its strong security posture and demonstrates that they can be trusted by customers.

Direct and Expert Vendor Engagement

The customer bypassed the need for internal project or commodity managers, who own supplier relationships but may lack deep cybersecurity expertise, to mediate security discussions with suppliers. The MAX team, which has expertise in risk management, incident response, and threat hunting, directly alerts vendors to identified issues, provides detailed explanations, and offers actionable recommendations for remediation. This expert-to-expert communication ensures that security gaps are understood and addressed more effectively, accelerating the overall risk mitigation process.