SOLUTION BRIEF

# SecurityScorecard MAX

## Managed Services for Supply Chain Detection and Response

## Challenge

### Your Vendors' Security Issues Become Your Problems

Your organization likely depends on hundreds or thousands of third-party vendors. When these vendors have security vulnerabilities, your organization is at risk. Supply chain attacks have increased by 68% and cost 40% more to address than direct breaches.

The traditional approach to managing vendor security – annual questionnaires and occasional risk scores – leaves dangerous gaps. Most organizations lack the time, tools, and expertise to continuously monitor all vendors, identify critical issues, and ensure they get fixed.

## Solution

### Turning Insights into Action with MAX

MAX is a managed service that enables response and remediation capabilities, working through our service partners to protect the entire supply chain ecosystem. Powered by human expertise, threat and vulnerability intelligence, and the latest technology, MAX puts you back in control without getting into the weeds of vendor communications and monitoring. We'll manage your supply chain cyber risk lifecycle or a subset of vendors based on your organization's needs, tolerances, and requirements – so your team can get back to critical projects.

MAX is not another risk monitoring tool. It's a comprehensive Supply Chain Detection and Response (SCDR) solution that strengthens operational resilience, enhances third-party risk management, and mitigates concentrated risk by:

- **Finding security issues** in your vendors' systems before attackers can exploit them
- **Prioritizing the most critical risks** that could directly impact your business
- **Working with your vendors** to fix these issues quickly
- **Tracking remediation** to ensure problems are actually solved

SecurityScorecard's expert partners handle the entire process – from detection through remediation – so your team doesn't have to.

### MAX strengthens your operational resilience by:

**Preventing supplier-related downtime**

MAX continuously monitors third-party risks using to detect issues that can be exploited by threat actors

**Ensuring business continuity**

MAX develops and executes supply chain incident response plans that reduce potential entry points for attackers

**Mitigating concentrated risk**

Advanced security assessments help identify vulnerabilities in nth-party systems that could impact your critical business functions

SecurityScorecard.com
info@securityscorecard.io

# How MAX Works

## Simplify vendor security management:

### Continuous Monitoring

MAX continuously monitors third-party risks using SecurityScorecard's security ratings, proprietary threat intelligence, automated risk assessments and artificial intelligence to constantly scan your vendors for vulnerabilities

### Risk Prioritization

MAX prioritizes the most critical vulnerabilities that could lead to breaches, allowing you to focus on what matters most to your business

### Vendor Engagement

MAX provides a clearinghouse for faster vendor engagement and issue resolution – no more endless email chains or unanswered requests

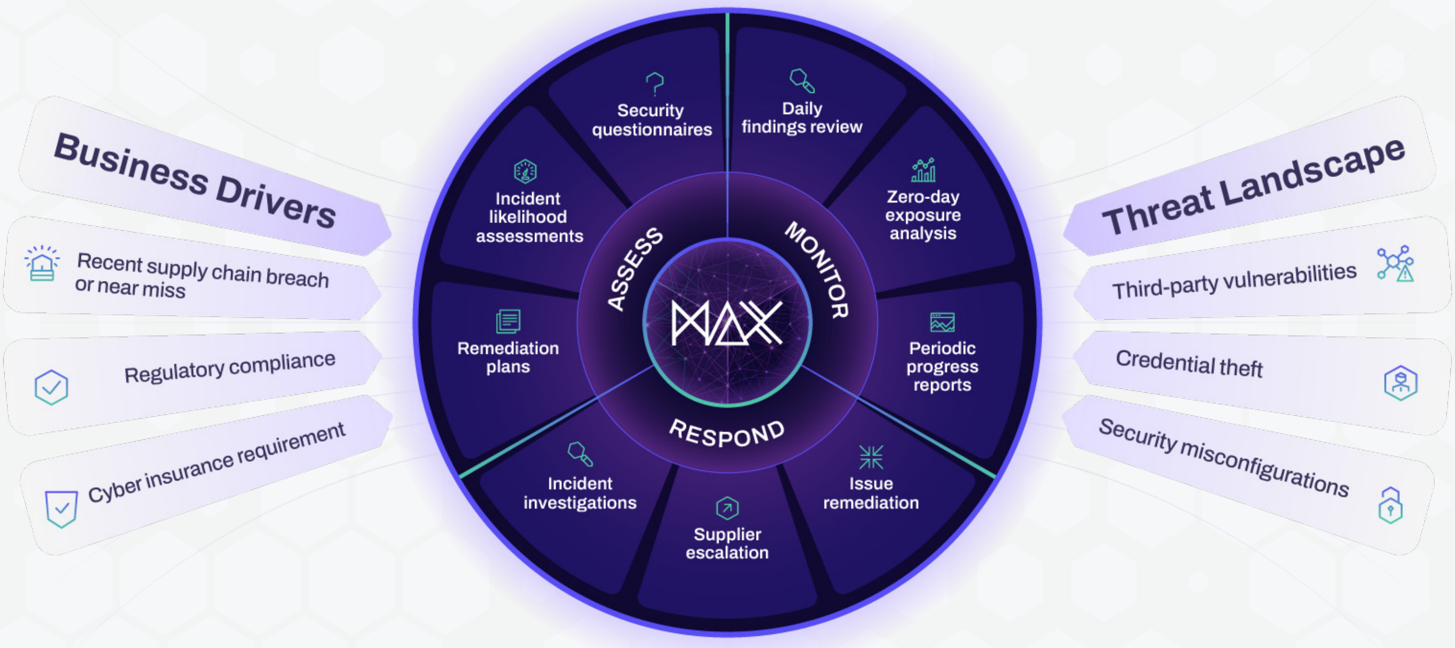
### Remediation Tracking

You'll receive regular updates on progress and confirmation when issues are fixed

### SOC Integration

MAX integrates with SOC workflows for real-time incident response

By operationalizing supply chain security, MAX helps organizations reduce supply chain attack risks, meet compliance mandates, and free up internal teams to focus on core security operations.



SecurityScorecard

# Strengthen Business Resilience Against Supply Chain Disruptions

Supply chain breaches have become the fastest growing concern for CISOs, with attacks through third parties increasing by 68% year-over-year and costing 40% more to respond to than first-party breaches. A SecurityScorecard case study revealed that 67% of security incidents at one global organization involved third parties, directly threatening operational continuity and creating cascading impacts across business operations.

**75%**
Reduction in third-party breaches

**100%**
Remediation rate for zero-day incidents

**3x**
Reduction in high risk suppliers

# Meet Compliance Requirements with Confidence

Regulators and standards organizations now recognize that cyber risks can cascade through supply chains, affecting entire industries. As a result, they've created stringent supply chain security requirements that most organizations struggle to meet.

MAX transforms compliance from a burden into a built-in advantage:

Supports multiple frameworks and regulations

ISO 27001
NIST 800-53
NERC CIP
CMMC
SOC 2
DORA
GDPR
NIS 2

### Audit-ready documentation

Every vendor interaction, assessment, and remediation effort is automatically documented, creating clear audit trails that demonstrate due diligence

### Incident response readiness

When security incidents occur, MAX's advanced forensics capabilities help you determine the broader impact on your organization and meet time-sensitive reporting requirements

### Continuous compliance monitoring

Rather than point-in-time assessments, MAX provides ongoing validation that your supply chain meets regulatory standards

# Streamline supply chain cybersecurity operations

Most security teams face an impossible challenge: properly managing hundreds or thousands of vendor relationships with limited staff. The endless cycle of assessments, monitoring, and remediation consumes valuable resources that could be better used elsewhere.

Consider the reality:

- Continuous vendor assessments overwhelm security teams
- Evolving threats require constant vigilance across your entire supply chain
- Compliance enforcement across complex vendor networks is manual and time-consuming
- Limited cybersecurity personnel can't keep pace with the volume of work

MAX transforms this burden into a strategic advantage:

- **Focus on what matters:** Your team can offload routine vendor security tasks and concentrate on high-value, strategic initiatives
- **Automation that works:** MAX automates risk assessments, reporting, and continuous vendor monitoring, dramatically reducing manual effort
- **Expertise on demand:** Access specialized supply chain security expertise without expanding your team

**50%**
Cost savings over do-it-yourself approach

**131**
Hours saved per vendor per year on supply chain incident response tasks

# MAX service options align to your security priorities

Available in three flexible tiers to meet your organization's needs

| | **SILVER**<br>Manage and monitor non-critical vendors | **GOLD**<br>Outsource vendor management; own vendor communications | **PLATINUM**<br>Outsource vendor management and communications |
|---|---|---|---|
| Max Dashboard | ● | ● | ● |
| Platform configuration | ● | ● | ● |
| Incident likelihood assessment | *Annual* | *Semi-Annual* | *Quarterly* |
| Cyber incident alerts | *Weekly* | *Daily* | *Daily* |
| Regular status reports | ● | ● | ● |
| Vendor onboarding | | ● | ● |
| Zero-day vulnerability report | | ● | ● |
| Custom questionnaire assessments | | *Guidance only* | ● |
| Vendor remediation engagement | | | ● |

**MAX Dashboard**
Customer portal for reviewing supply chain risks, communicating with MAX delivery teams, and understanding the progress being made on behalf of the customer.

**Platform configuration**
Implementation and management of the SecurityScorecard platform by a team of incident responders, digital forensics experts, SOC analysts, and TPRM experts. SecurityScorecard will import and tag vendors, assign them to portfolios, and create and maintain rules to notify customers of events relating to their vendors.

**Incident likelihood assessments**
Expert-curated analysis of current and historical attack surface exposure data collected by SecurityScorecard. This analysis results in a high, medium, or low rating of a vendor's overall likelihood of breach. Improvement recommendations pinpoint specific actions required to prevent breaches based on incident response principles and experience.

**Cyber incident alerts**
Notifications about findings that indicate that a vendor has been breached or is at risk of imminent breach. This report includes reported breaches that vendors haven't broadly disclosed, evidence of leaked credentials, or signs of exposed services.

**Periodic status reports**
Weekly and monthly reporting of supply chain risk management program status and outcomes.

**Vendor onboarding**
Invitation of vendors to adopt SecurityScorecard platform for remediating their issues. SecurityScorecard also personally meets with onboarded vendors to outline the customer's security expectations for the vendor.

**Zero-day detection and response**
Summary of exposure to zero-day vulnerabilities as they emerge. SecurityScorecard identifies impacted vendors and recommendations to strengthen defenses.

**Custom questionnaire assessments**
Development guidance, creation and distribution of security questionnaires for vendors to attest to the state of their security program. Responses are validated against SecurityScorecard data to prioritize follow-up discussions as necessary.

**Vendor remediation engagement**
Development of plan to resolve issues identified in Incident Likelihood Assessments. SecurityScorecard delivers advice to vendors and tracks the progress of implementing recommended fixes.

LEARN MORE AT:
securityscorecard.com/platform/max

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io