



# EXPECT the UNEXPECTED

**Security from A to F**

Your digital guide to the Q4 '23 Release

# What's included?

Security from A to F is your guide to the Q4 2023 Release.



## Q4 2023 Release Deck

An overview of the 30+ new innovations, services, and integrations, including screenshots and release notes.



## Additional Resources

At the end of this deck, we provide you with additional guides, education and videos that will help you operationalize the Q4 '23 Release.

# The traditional enterprise risk model has changed.



## There is no perimeter

Your attack surface is not limited to your organization, making securing it more challenging.



## Regulatory scrutiny

Regulators around the world are putting a microscope on third-party risk management.



## Expanded view of risk

Security teams' scope is expanding and they are being asked to do more with less.

# Are you prepared to...

**Operationalize your vendor risk management program?**

**Accept the risk of a vendor falling below your risk appetite?**

**Respond to a third-party breach?**

**Comply with regulation that demands a quick response to a third-party breach?**

**Support a sales procurement process to close a deal at the last hour of the quarter?**

**Speak to the board about how your VRM program is driving your business forward?**

**Respond to a zero-day with a team of experts on hand?**

# Third-party risk is a business risk. Expect the unexpected.

SecurityScorecard empowers you to build a resilient third-party risk management program and expect the unexpected with complete visibility of your supply chain, the ability to take instant action, and increase collaboration across your entire ecosystem.



**GAIN  
COMPLETE  
VISIBILITY**

Stay one step ahead of adversaries with a complete picture of your supply chain.



**TAKE PROACTIVE  
ACTION**

Be prepared to quickly respond to emerging threats with a trusted team of experts at your side.



**INCREASE  
COLLABORATION**

Clearly communicate and partner with stakeholders, partners, and regulatory bodies.

# One Platform, Multiple Use Cases



**Enterprise Cyber  
Risk Management**



**Executive-Level  
Reporting**



**Service  
Providers**



**Compliance**



**Third-Party Risk  
Management**



**Cyber  
Insurance**



**M&A Cyber  
Due Diligence**



**Threat  
Intelligence**

We've consolidated multiple data feeds into a single analytics platform that gives you insight into your own attack surface as well as your entire ecosystem.

SINKHOLE  
**2B+**

**malware requests** per day – one of the world's largest malware DNS sinkhole

**100B+**

daily signals.. **analyzed** and **crowd-sourced** with **AI-Powered processing**

**99%**

of data is **collected and curated** by SecurityScorecard

**1,500+**  
PORTS

scanned across the **entire internet** every 7 days

**7B+**

**leaked credential/PII databases** in-house from across dark web and forums

**TOP  
20M**

**websites crawled every week** using full browsers imitating real users

# Comprehensive solution for detecting and collaborating to eliminate supply chain cyber risk.



## External Risk

- Security Ratings
- Security Data API
- Attack Surface Intelligence
- Automatic Vendor Detection



## Continuous Compliance

- Questionnaires
- Evidence Locker
- Regulatory Compliance
- Cloud Compliance



SecurityScorecard  
Platform

## Marketplace of Integrations & Apps



## Professional Services

- Managed Cyber Risk Services
- Digital Forensics & Incident Response
- Proactive Security Services
- Cyber Risk Intelligence



## Board Reporting

- Cyber Risk Quantification
- Reporting Center

# What's new in the Q4'23 Release?



## Third-Party Cyber Risk Management

- Action Plans
- Integrated Questionnaires
- ESG Data
- Natural Language Search
- Expanded Vendor Intelligence
- Vendor Collaboration Invites
- 4th Party Vendor Detection in Portfolios
- Invited Contact manager



## Enterprise Cyber Risk Management

- Evidence & Events in the Digital Footprint
- Automated Board Reports
- Compliance Readiness Assessment
- Asset Categories
- Custom Scorecard Filters
- Subsidiary Scorecards Issue View



## Threat Intelligence

- BreachDetails
- Visual Search in Attack Surface Intelligence
- Table view in Attack Surface Intelligence
- CVEDetails.com *Beta*



## Marketplace

- S&P Risk Indicator
- ProcessUnity
- Jira On-Demand Ticket Creation
- Cybersecurity Risk Insights
- Salesforce Scorecard IMporter
- Threat Quotient
- Netskole CCI Integration



## Platform

- Data Residency Compliance
- Audit Log
- Global Navigation



## Professional Services

- Managed Cyber Risk Services *Soft-launch*
- Zero-Day-as-a-Service *Soft-launch*
- Request Services in Platform



# Third-Party Cyber Risk Management

- Action Plans
- Integrated Questionnaires
- ESG Data
- Natural Language Search
- Expanded Vendor Intelligence
- Vendor Collaboration Invites
- 4th Party Vendor Detection in Portfolios
- Invited Contact manager

# Action Plans

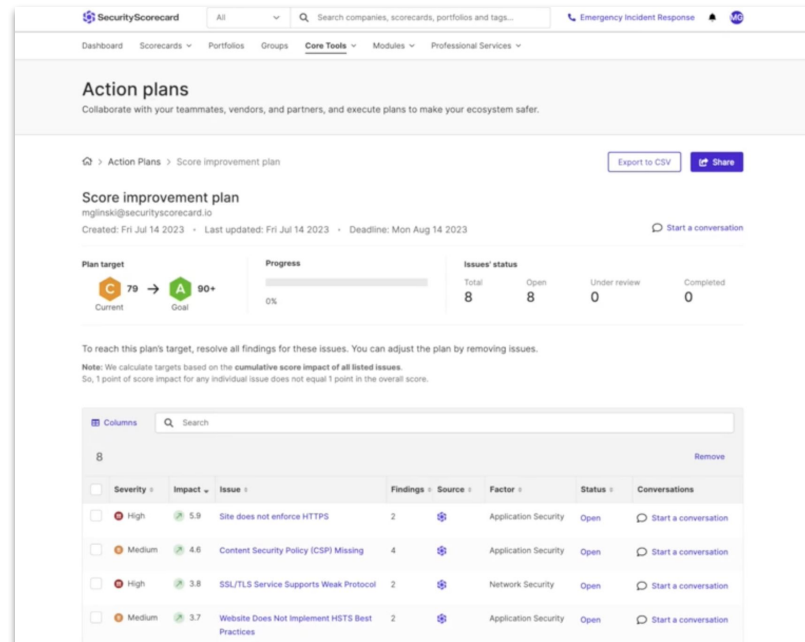
**Collaborate and improve your ecosystem's security posture with confidence.**

Streamline collaboration with third-parties and key stakeholders in one dashboard.

**How this helps you:** Generate dynamic remediation plans, prioritize critical vulnerabilities, assign specific people to fix issues, and see progress in real time, saving you hours and reducing ecosystem risk.

## Other Use Cases this Enables:

- **Third-Party Risk Management:** Ensure that your vendors meet your risk appetite and work collectively to improve their security posture.
- **Enterprise-Cyber Risk Management:** Collaborate with internal stakeholders to assign and prioritize security issues.
- **Cyber Insurance:** Accelerate the application process by eliminating subjectivity and collaborating with applicants at scale.



**Action plans**  
Collaborate with your teammates, vendors, and partners, and execute plans to make your ecosystem safer.

🏠 Action Plans > Score improvement plan Export to CSV Share

**Score improvement plan**  
mgjnski@securityscorecard.io  
Created: Fri Jul 14 2023 · Last updated: Fri Jul 14 2023 · Deadline: Mon Aug 14 2023 Start a conversation

**Plan target** **Progress** **Issues' status**

Current: **C** 79 → Goal: **A** 90+ 0% Total: 8 Open: 8 Under review: 0 Completed: 0

To reach this plan's target, resolve all findings for these issues. You can adjust the plan by removing issues.  
Note: We calculate targets based on the cumulative score impact of all listed issues. So, 1 point of score impact for any individual issue does not equal 1 point in the overall score.

Severity	Impact	Issue	Findings	Source	Factor	Status	Conversations
High	5.9	Site does not enforce HTTPS	2	🔗	Application Security	Open	Start a conversation
Medium	4.6	Content Security Policy (CSP) Missing	4	🔗	Application Security	Open	Start a conversation
High	3.8	SSL/TLS Service Supports Weak Protocol	2	🔗	Network Security	Open	Start a conversation
Medium	3.7	Website Does Not Implement HSTS Best Practices	2	🔗	Application Security	Open	Start a conversation

[LEARN MORE](#)

# Integrated Questionnaires

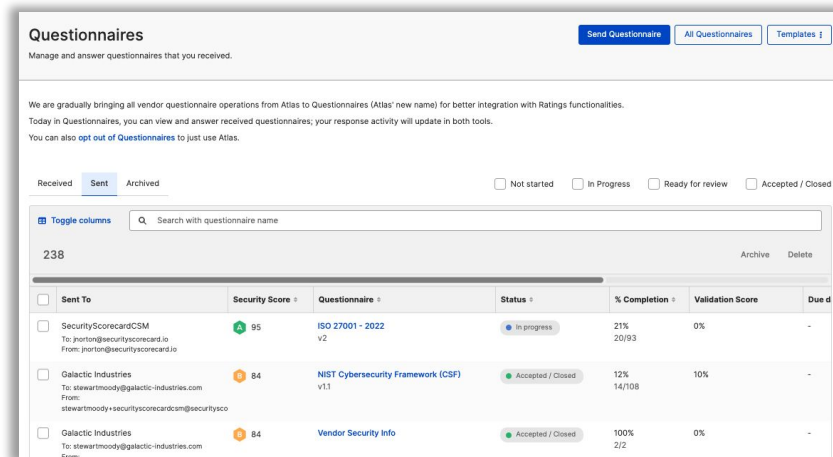
Automatically send and validate vendor questionnaires at scale.

Effectively assess your vendors with smart questionnaires integrated into our ratings platform

**How this helps you:** Use automation and machine learning to validate vendor responses and shorten the questionnaire process by as much as 83%.

## Other Use Cases this Enables:

- **Third-Party Risk Management:** Send, track, and validate questionnaires to your third and fourth parties.
- **Enterprise-Cyber Risk Management:** Conduct internal security assessments with automated questionnaires.
- **M&A Due Diligence:** Assess the cybersecurity risk of a potential acquisition target with security questionnaires.



[LEARN MORE](#)



## ESG Data

### Get critical data for evaluating Environmental, Social, and Corporate Governance (ESG) risk

Get vendor risk data from one trusted source delivered through a customer-facing API.

**How this helps you:** Stay ahead of regulatory activity and investor pressure by adding additional ESG risks to monitor for in your third-party ecosystem.

#### Other Use Cases this Enables:

- **Third-Party Risk Management:** Continuously monitor your entire third-party ecosystem for economic, political, environmental, and ethical risks.
- **Insurance Underwriting:** Integrate ESG risk into your assessment framework for underwriting decisions.
- **Investment Banking:** Consider ESG risk alongside financial and cyber risk.
- **Procurement:** Evaluate current and future suppliers' ESG risk before procuring products and services or renewing.

<ul style="list-style-type: none"> <li>• Adverse Media: Burglary</li> <li>• Adverse Media: Conspiracy</li> <li>• Enforcement: Crime Against Humanity</li> <li>• Adverse Media: Cybercrime</li> <li>• Adverse Media: Environmental Crimes</li> <li>• Adverse Media: Espionage</li> <li>• Adverse Media: Gambling Operations</li> <li>• Adverse Media: Human Rights Abuse</li> <li>• Adverse Media: Kidnapping</li> <li>• Adverse Media: Labor Violations</li> <li>• Adverse Media: Murder</li> <li>• Adverse Media: Peonage</li> <li>• Adverse Media: Piracy</li> <li>• Adverse Media: Pollution</li> <li>• Adverse Media: Pornography</li> <li>• Adverse Media: Stolen Property</li> <li>• Adverse Media: War Crimes</li> <li>• Enforcement: Administrative</li> <li>• Enforcement: Burglary</li> <li>• Enforcement: Conspiracy</li> <li>• Enforcement: Crime Against Humanity</li> <li>• Enforcement: Cybercrime</li> <li>• Enforcement: Environmental Crimes</li> <li>• Enforcement: Espionage</li> <li>• Enforcement: Gambling Operations</li> <li>• Enforcement: Human Rights Abuse</li> <li>• Enforcement: Kidnapping</li> <li>• Enforcement: Labor Violations</li> <li>• Enforcement: Explosives</li> <li>• Enforcement: ISIS Foreign Support</li> <li>• Enforcement: WMD</li> </ul>	<ul style="list-style-type: none"> <li>• Enforcement: Murder</li> <li>• Enforcement: Peonage</li> <li>• Enforcement: Piracy</li> <li>• Enforcement: Pollution</li> <li>• Enforcement: Pornography</li> <li>• Enforcement: Stolen Property</li> <li>• Enforcement: War Crimes</li> <li>• Adverse Media: Bribery</li> <li>• Adverse Media: Corruption</li> <li>• Enforcement: Bribery</li> <li>• Enforcement: Corruption</li> <li>• Adverse Media: AntiTrust violations</li> <li>• Adverse Media: Bank Fraud</li> <li>• Adverse Media: Counterfeiting</li> <li>• Adverse Media: Embezzlement</li> <li>• Adverse Media: Extort-Rack-Threats</li> <li>• Adverse Media: Financial Crimes</li> <li>• Adverse Media: Forgery</li> <li>• Adverse Media: Fraud</li> <li>• Adverse Media: Healthcare Fraud</li> <li>• Adverse Media: Insider Trading</li> <li>• Adverse Media: Insurance Fraud</li> <li>• Adverse Media: Money Laundering</li> <li>• Adverse Media: Mortgage Fraud</li> <li>• Adverse Media: Price Manipulation</li> <li>• Adverse Media: RICO</li> <li>• Adverse Media: Securities Fraud</li> <li>• Adverse Media: Tax Evasion</li> <li>• Adverse Media: Wire Fraud</li> <li>• Enforcement: Bank Fraud</li> </ul>	<ul style="list-style-type: none"> <li>• Enforcement: Counterfeiting</li> <li>• Enforcement: Embezzlement</li> <li>• Enforcement: Extort-Rack-Threats</li> <li>• Enforcement: Financial Crimes</li> <li>• Enforcement: Forgery</li> <li>• Enforcement: Fraud</li> <li>• Enforcement: Healthcare Fraud</li> <li>• Enforcement: Insider Trading</li> <li>• Enforcement: Insurance Fraud</li> <li>• Enforcement: Interstate Commerce</li> <li>• Enforcement: Money Laundering</li> <li>• Enforcement: Mortgage Fraud</li> <li>• Enforcement: Price Manipulation</li> <li>• Enforcement: RICO</li> <li>• Enforcement: Securities Fraud</li> <li>• Enforcement: Tax Evasion</li> <li>• Enforcement: Wire Fraud</li> <li>• Registrations: Marijuana Reg Bus</li> <li>• Registrations: UAE MSB</li> <li>• Registrations: US MSB</li> <li>• PEP: PEP Controlled Bus</li> <li>• Associated Entity: N/A</li> <li>• Associated Entity: Ownership Or Control</li> <li>• Associated Entity: SWIFT BIC Entity</li> <li>• Sanction List: N/A</li> <li>• SOE: Govt Linked Corp</li> <li>• SOE: Govt Owned Corp</li> <li>• Adverse Media: Aircraft Hijacking</li> <li>• Adverse Media: Explosives</li> <li>• Adverse Media: ISIS Foreign Support</li> <li>• Adverse Media: Terrorism</li> <li>• Adverse Media: WMD</li> <li>• Enforcement: Aircraft Hijacking</li> </ul>	<ul style="list-style-type: none"> <li>• Adverse Media: Arms Trafficking</li> <li>• Adverse Media: Drug Trafficking</li> <li>• Adverse Media: Fugitive</li> <li>• Adverse Media: Human Trafficking</li> <li>• Adverse Media: Organized Crime</li> <li>• Adverse Media: Pharma Trafficking</li> <li>• Adverse Media: Smuggling</li> <li>• Enforcement: Arms Trafficking</li> <li>• Enforcement: Asset Freeze</li> <li>• Enforcement: Debarred</li> <li>• Enforcement: Disciplined</li> <li>• Enforcement: Disqualified</li> <li>• Enforcement: Drug Trafficking</li> <li>• Enforcement: End Use Control</li> <li>• Enforcement: Excluded Party</li> <li>• Enforcement: Fugitive</li> <li>• Enforcement: Human Trafficking</li> <li>• Enforcement: Organized Crime</li> <li>• Enforcement: Pharma Trafficking</li> <li>• Enforcement: Smuggling</li> <li>• Enforcement: Arms Trafficking</li> <li>• Enforcement: Asset Freeze</li> <li>• Enforcement: Debarred</li> <li>• Enforcement: Disciplined</li> <li>• Enforcement: Disqualified</li> <li>• Enforcement: Drug Trafficking</li> <li>• Enforcement: End Use Control</li> <li>• Enforcement: Excluded Party</li> <li>• Enforcement: Fugitive</li> <li>• Enforcement: Human Trafficking</li> <li>• Enforcement: Organized Crime</li> <li>• Enforcement: Pharma Trafficking</li> <li>• Enforcement: Smuggling</li> <li>• Enforcement: Una</li> </ul>
--	--	---	--

# Natural Language Global Search

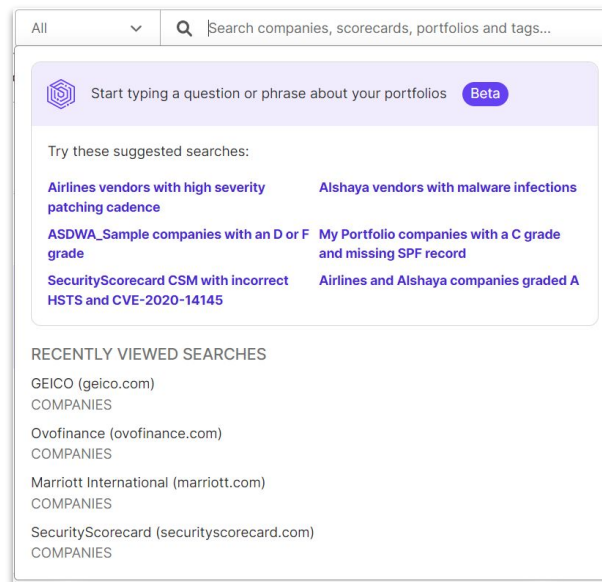
**Accelerate risk analysis simply by asking questions that are top of mind**

Identify which vendors have critical issues by leveraging AI and asking direct and intuitive questions.

**How this helps you:** Spend less time figuring out how to filter through a portfolio by typing for what you are looking for.

## Other Use Cases this Enables:

- **Third-party Risk Management:** Identify which vendors have critical issues
- **Cyber insurance:** Determine a portfolio's exposure to specific security issues



# Vendor Collaboration Invites

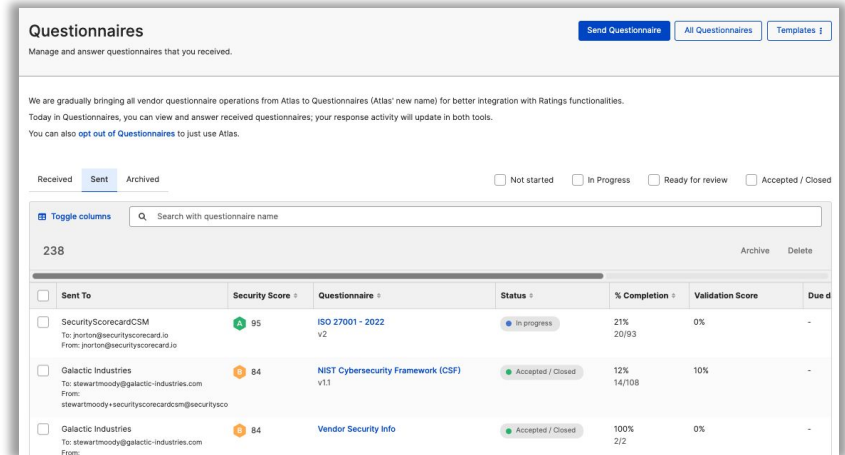
Increase response rates and customize requests when inviting your vendors to SecurityScorecard

A seamless invite flow for both the recipient and the sender.

**How this helps you:** When requesting evidence from the Evidence Locker, personalize your invite to familiar contacts using the Contact Manager. As a recipient of a request, respond to requests quicker without being interrupted and asked to create a SecurityScorecard account.

## Use Cases this Enables:

- **Third-Party Risk Management:** Improve collaboration with your vendors and partners by inviting them onto the platform through a personalized invite and allow them to quickly fulfill the request
- **Compliance:** Requesting evidence from the evidence locker ensures your vendors are complying with standards and regulations.



# 4th Party Vendor Detection in Portfolios

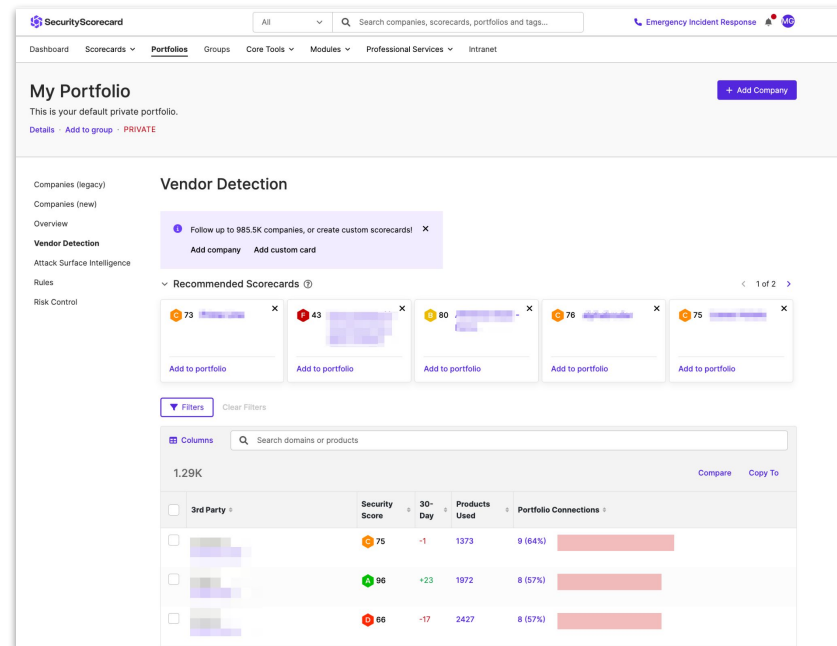
## Instantly assess concentration risk within your Portfolios

Gain visibility into what vendors and products your third parties in a Portfolio rely on to get ahead of concentration risk.

**How this helps you:** When looking at a Portfolio, you can now see your fourth parties connected to the vendors, how they are connected, and their security risk.

### Other Use Cases this Enables:

- **Third-Party Risk Management:** Evaluate the concentration risk posed to your organization by your most critical vendors.
- **Enterprise-Cyber Risk Management:** Protect your organization against potential third and fourth party breaches by getting ahead of concentration risk.
- **M&A Due Diligence:** Stay ahead of threats in your investments or M&A prospects with insight into the organizations and products they rely on.



The screenshot shows the 'My Portfolio' page in SecurityScorecard. The 'Vendor Detection' section displays a notification: 'Follow up to 985.5K companies, or create custom scorecards!'. Below this, there are five 'Recommended Scorecards' cards, each with a score and an 'Add to portfolio' button. At the bottom, a table lists the details for these scorecards.

3rd Party	Security Score	30-Day	Products Used	Portfolio Connections
[Redacted]	75	-1	1373	9 (64%)
[Redacted]	96	+23	1972	8 (57%)
[Redacted]	66	-17	2427	8 (57%)



## Invited Contact Manager

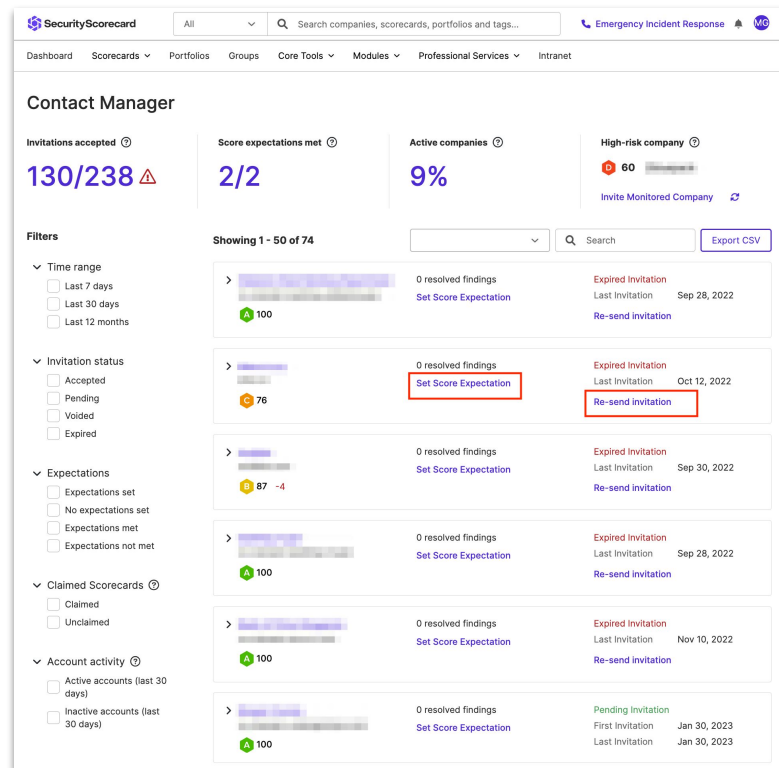
Easily collaborate with key partners to get ahead of ecosystem risk.

Gain visibility into the status of all of your invited vendors and their progress on improving their security posture.

**How this helps you:** Eliminate the need for email back and forth with instant visibility into the status of every vendor you've invited and their progress so you can prioritize next steps.

### Other Use Cases this Enables:

- **Third-Party Risk Management:** Partner with your vendors to improve ecosystem risk with visibility into every step.
- **Cyber Insurance:** Monitor the adoption of security ratings as a policyholder benefit amongst your insureds
- **M&A Due Diligence:** Stay ahead of risk within your Portfolio companies by easily inviting them to improve their security posture with visibility into their progress.



[LEARN MORE](#)



# Enterprise Cyber Risk Management

- Evidence & Events in the Digital Footprint
- Automated Board Reports
- Compliance Readiness Assessment
- Asset Categories
- Custom Scorecard Filters
- Subsidiary Scorecards Issue View

# Evidence & Events in the Digital Footprint

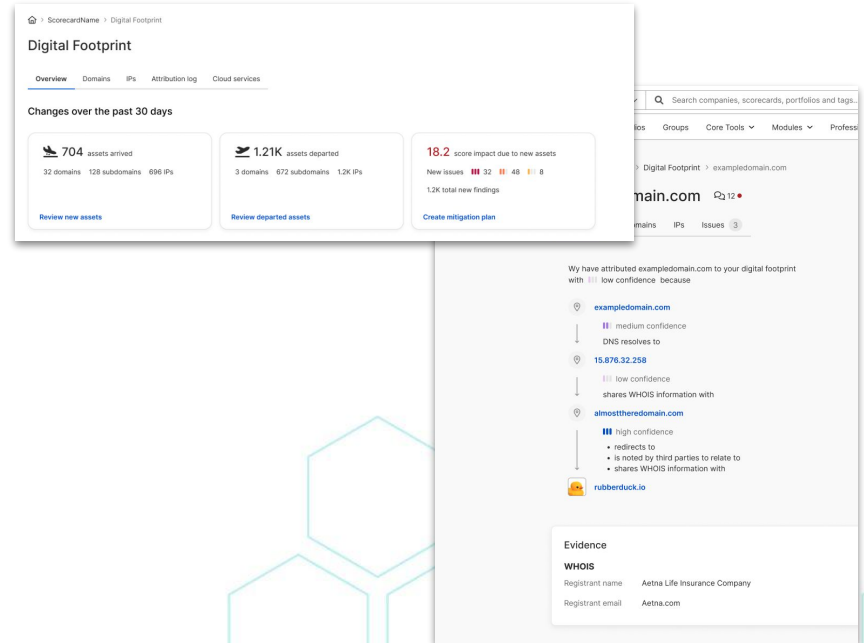
## Clearly identify evidence of attributed domains in your Digital Footprint

Actively assess how assets relate to your organization

**How this helps you:** Clear communication of attribution sources and any underlying evidence for Digital Footprint assets. Easily understand what assets have been discovered and/or decommissioned, providing a clear picture on how those assets relate to their organization.

### Other Use Cases this Enables:

- **Enterprise Cyber Risk Management:** Verify if asset is attributed correctly to your scorecard, before reviewing the associated issues and accordingly allocating internal resources to remediate them.
- **Third-Party Risk Management:** While reviewing issues (that matter to you) on your vendor's scorecard, verify whether corresponding assets are attributed correctly.



LEARN MORE

# Automated Board Reports

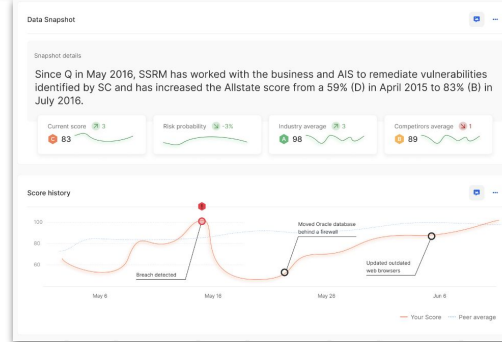
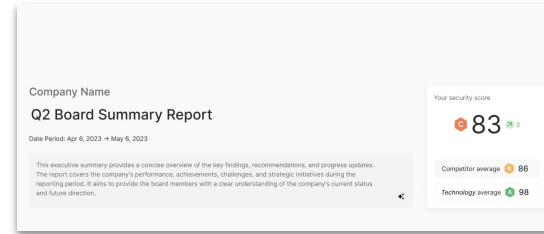
Clearly articulate the work done to improve your organization's score

Contextualize security risks with business risks.

**How this helps you:** Better communicate the most important high-level metrics across a Scorecard. Summarize key information on your organization's self-monitoring, vendor risk management, industry peers, and the competition.

## Other Use Cases this Enables:

- **Executive Level Reporting:** Easily report on your cybersecurity posture, benchmarked against peers and in time, so that I can assess our top priorities and determine if the investments are aligned with the business priorities and risks



# Compliance Readiness Assessment

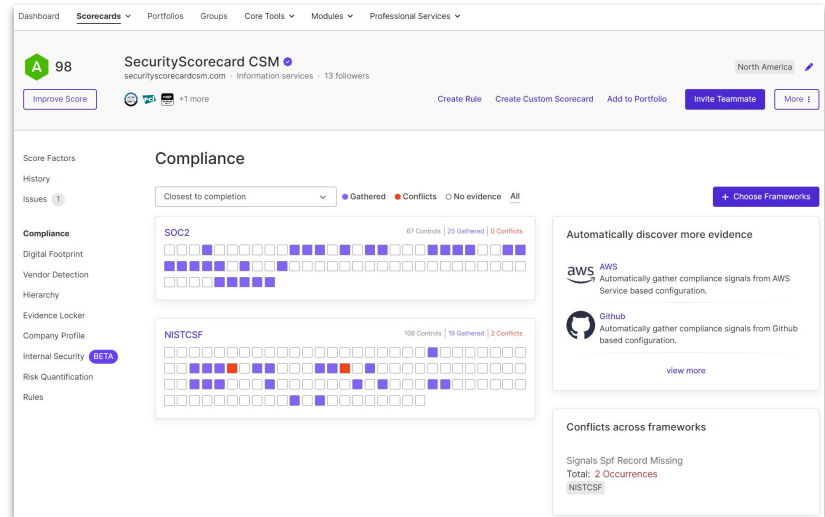
Centralize evidence collection for faster, more effective audits

Automatically gather evidence that indicates adherence to or violation of compliance frameworks

**How this helps you:** Gain a quick understanding of compliance readiness and prioritize where to focus

## Other Use Cases this Enables:

- **Compliance:** Continuously monitor compliance and reduce compliance drift ahead of audits
- **Third-Party Risk Management:** Implement onboarding framework for low-tier vendors that don't require questionnaires
- **Cyber Insurance:** Evaluate insureds against underwriting or insurance renewal guidelines
- **Regulatory Oversight:** Independently monitor regulated entities and their adherence to regulatory requirements



LEARN MORE

# Asset Categories

## Enable more segmented monitoring and risk mitigation

Label assets for easy assignment of ownership for IPs and Domains.

**How this helps you:** Auto-assigned and user-contributed categories for assets, making it easier to determine ownership of assets within teams. These categories provide a more accurate picture of an organization's attack surface and Top Level Score.

### Use Cases this Enables:

- **Enterprise Cyber Risk Management:** Infosec managers can leverage 'asset category' to get visibility on exposure and assign assets to their respective teams for effective monitoring and risk mitigation.

The screenshot shows a search interface with a filter applied: 'Where Asset Category includes all PARKED'. Below the filter, a table lists 18 assets, all of which are tagged as 'PARKED'. The 'Asset Category' column is highlighted with a red box in both the filter and the table.

Domain	IPs	Status	Issues	Findings	Impact	Domain type	Asset Category	Custom Tags	
<input type="checkbox"/>	custom-scorecard.com	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
<input type="checkbox"/>	cvdetails.info	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
<input type="checkbox"/>	cvdetails.net	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
<input type="checkbox"/>	cvdetails.org	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
<input type="checkbox"/>	malwaregrader.com	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
<input type="checkbox"/>	questionnaire.app	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
<input type="checkbox"/>	scorecard.app	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
<input type="checkbox"/>	scoring.io	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag

LEARN MORE

# Custom Scorecard Filters

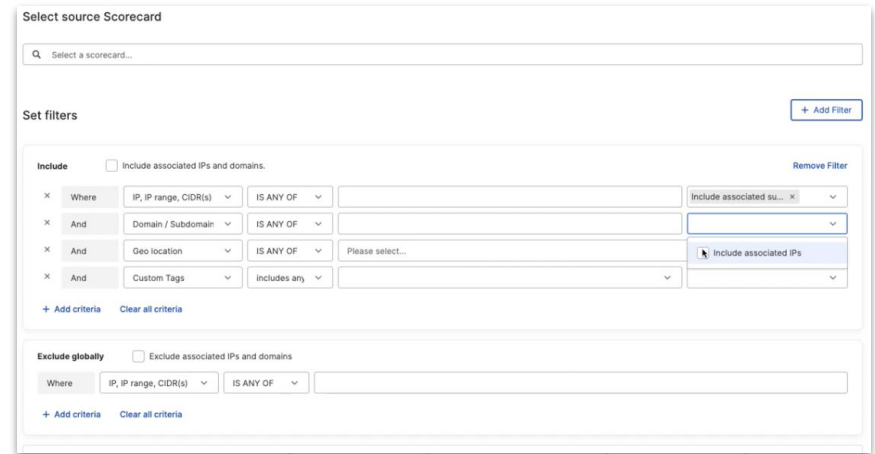
More tagging and filtering criteria for quickly building Custom Scorecards.

Better geolocation and subdomain filtering for segmented Scorecards

**How this helps you:** Expedite the allocation of assets and easily select associated IPs, domains and subdomains for selected assets, and geo-location based on options made available to them in these filters.

### Use Cases this Enables:

- **Enterprise Cyber Risk Management:** Build custom scorecards for your organization to have a more accurate view of your organization and prioritize remediation based on geolocation, subdomains, and other filtering options.



LEARN MORE

# Subsidiary Scorecard Issue View

Continuously monitor the security posture of your organization and subsidiaries.

Access complete issue evidence for your subsidiaries

**How this helps you:** Improve the overall security posture of an entity faster and understand common risks to quickly prioritize subsidiaries that require additional resources or attention to reduce cyber risk.

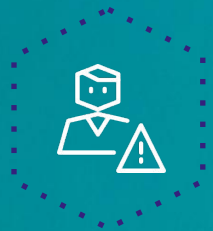
### Other Use Cases this Enables:

- **Enterprise Cyber Risk Management:** Faster remediation and hence risk mitigation for overall organizational posture.
- **Executive Level Reporting:** Accurately report on and analyze the security posture and efforts of certain business units within the entire entity

The screenshot displays the 'Subsidiaries' section of the SecurityScorecard interface. It features a search bar and a list of subsidiaries with their respective security scores and issue counts. A 'Company details' sidebar is open for 'Company Name', showing a score of 85 and a score history chart from March to August. The chart shows a score starting at approximately 75 in March, rising to 85 in April, peaking at 95 in July, and ending at 85 in August. The sidebar also lists 5 immediate subsidiaries and 3 administrators/32 users.

Subsidiary	Score	Issues
Root company	B	0
Company A	C	1
Company AA	A	0
Company AB	D	1
Company B	A	3
Company C	F	1
Company D	B	0

LEARN MORE



# Threat Intelligence

- BreachDetails
- Visual Search in Attack Surface Intelligence
- Table view in Attack Surface Intelligence
- CVEDetails.com



## BreachDetails

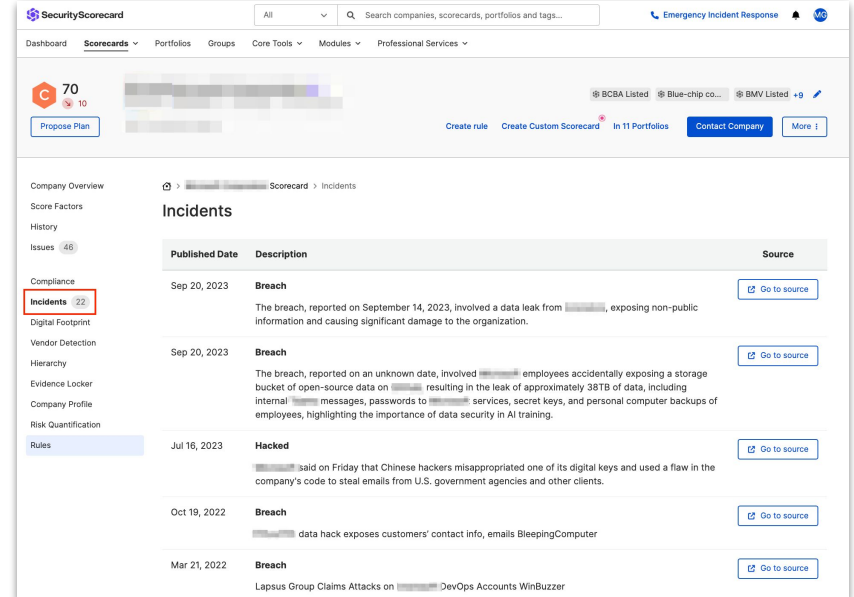
Respond with confidence when a breach is detected in your business ecosystem

Accurately identify breaches, reduce false positives, improve timeliness of breach notifications, and increase geographic coverage.

**How this helps you:** Using an in-house method for collecting and analyzing breach data provides greater control over breach notices and on-demand addition of breach detection sources providing you with even more detail for a breach.

### Other Use Cases this Enables:

- **Third-Party Risk Management:** Continuously monitor your entire third-party ecosystem for any detected breaches and be prepared to comply with regulatory guidelines.
- **Enterprise-Cyber Risk Management:** Effectively report and respond to breaches impacting your own organization with timely and accurate Breach Notices and Incidents.
- **Cyber Insurance:** Validate application responses regarding past claims and identify breaches that could be covered under claims made policies



[LEARN MORE](#)



## Visual Search in Attack Surface Intelligence

Surfacing threat intelligence fast and intuitively.

Enabling users without query syntax knowledge to quickly and efficiently conduct searches to gain the answers they need to drive decisions.

**How this helps you:** **Save time** with an effortless view of threat results with the ability to search, sort, and see more details without multiple clicks.

### Other Use Cases this Enables:

- **Third-Party Risk Management**
- **Enterprise-Cyber Risk Management**
- **M&A Due Diligence**
- **Cyber Insurance**

The screenshot shows a user interface for visual search. At the top, there are tabs for 'Visual Search' and 'Query', with a link to 'Learn how to use this search'. On the right, it says 'Track your total searches this month'. Below this is a section for 'Add filter' and 'Try these searches: My Organization CVE Threat Actor Port Ransomware All | Clear'. The main search area contains two criteria: 'Where Portfolio is SecurityScorecard' and 'And Has infections is True'. There are buttons for '+ Add criteria' and 'Clear all criteria'. At the bottom right, there are 'Clear filters' and 'Search' buttons. A preview of the query is shown on the right: 'Preview your query (portfolio\_id:"7055e42a-0003-5d88-a8c2-4a945cb41c3a" AND has\_infection:true)'. The interface is clean and modern, with a white background and blue accents.



## Table View in Attack Surface Intelligence

Gain a consolidated and searchable view of threat intelligence search results .

Effectively and efficiently find what you are looking for without leaving the results page.

**How this helps you:** Save time with an effortless view of threat results with the ability to search, sort, and see more details without multiple clicks.

### Other Use Cases this Enables:

- Third-Party Risk Management
- Enterprise-Cyber Risk Management
- M&A Due Diligence
- Cyber Insurance

The screenshot displays a table view of threat intelligence results. The table has columns for IP, Infections, Vulnerabilities, Breaches, and Threat. A sidebar titled 'IP Details' is open for the IP 716.234.7, providing additional context such as geographic location, ASN, hostname, and attributed technology.

IP	Infections	Vulnerabilities	Breaches	Threat
128.163.45.219	pva.torrent.openinternet, conficker	CVE-2021-38368, CVE-2021-39268	-	APT29
716.234.7	pva.torrent.openinternet	CVE-2020-14145, CVE-2021-38368, CVE-2021-39268, +5	hetzner.com	REvil, L
28.163.45.211	pva.torrent.openinternet, conficker	CVE-2020-14145, CVE-2021-39268, +4	hetzner.com	LAPSU
128.163.45.219	conficker	-	-	Wizard
208.56.245.121	-	CVE-1678-5252	-	-
108.16.248.124	pva.torrent.openinternet, conficker	CVE-2020-14145, CVE-2021-38368, CVE-2021-39268, +5	-	REvil, L
78.113.45.11	-	CVE-1678-5252	-	-
28.163.45.211	pva.torrent.openinternet	CVE-2021-38368,	-	Conti



## CVEDetails.com *Beta*

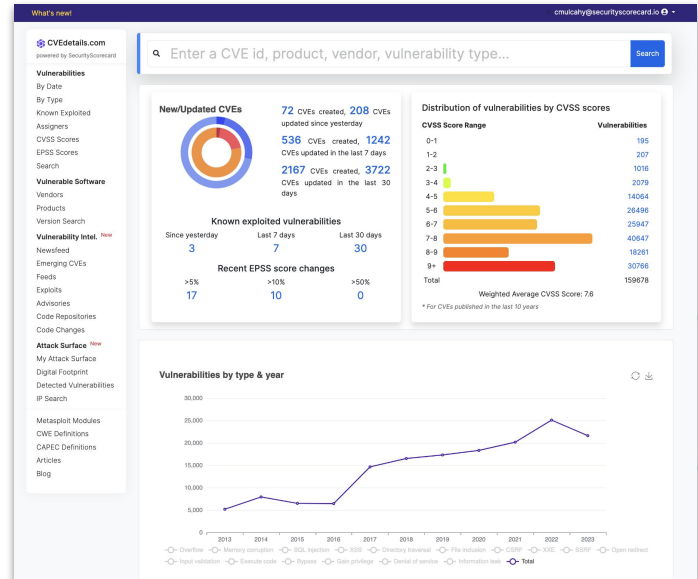
Harness vulnerability intelligence to understand the impact to your attack surface.

Gain a comprehensive understanding of details associated with all published and upcoming CVEs to drive remediation decisions.

**How this helps you:** Make faster decisions with insight into the severity of a CVE and any known exploits to determine the impact to the business.

### Other Use Cases this Enables:

- Enterprise-Cyber Risk Management
- Vulnerability Management



[LEARN MORE](#)



## Professional Services

- Managed Cyber Risk Services  
*Soft launch*
- Zero-Day-as-a-Service *Soft launch*
- Request Services in Platform



# Managed Cyber Risk Services *Soft Launch*

## Operationalize your third-party cyber risk program to stop attacks before they happen

Augment your existing cyber risk program alongside cybersecurity professionals to proactively identify the likelihood of a cyber incident in your vendor ecosystem.

**How this helps you:** Partner with cyber experts to assess, monitor, and mitigate blindspots across your supply chain to reduce cyber risk and increase efficiencies across your third party risk program.

### Other Use Cases this Enables:

- **Third-Party Risk Management:** Using the powerful risk signals and threat insights from the SecurityScorecard platform, proactively analyze and mitigate cyber risk associated with your vendor landscape.



[LEARN MORE](#)



# Zero-Day-as-a-Service *Soft Launch*

**Early warning and detection service for new and emerging zero-days across your vendor ecosystem**

Comprehensive report detailing newly-identified zero-days, third-parties potentially susceptible, and actionable steps to track and combat the zero-day.

**How this helps you:** Safeguards your organization against emerging security threats across your third party vendor ecosystem.

## Other Use Cases this Enables:

- **Third-Party Risk Management:** Using the powerful risk signals and threat insights from the SecurityScorecard platform, proactively analyze and mitigate cyber risk associated with your vendor landscape. Available as part of the Managed Cyber Risk Services offering or as an individual offering.



[LEARN MORE](#)



## Request Services in Platform

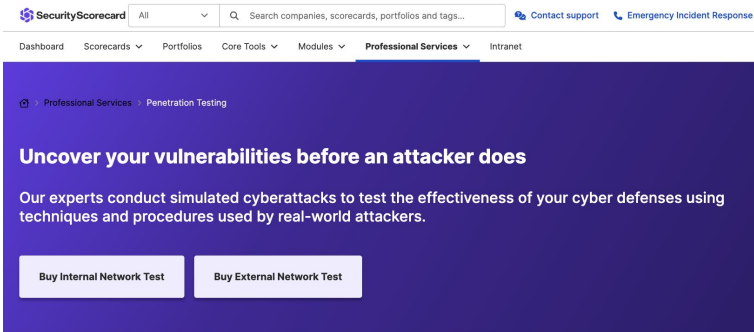
### Purchase or schedule a consultation for Professional Services within the platform

Tabletop Exercises, Penetration Testing, and Incident Response support are available to be purchased or to schedule a time with our team on-demand.

**How this helps you:** Saves time and streamlines gaining access to SecurityScorecard Professional Services to help you strengthen your cybersecurity defenses.

### Other Use Cases this Enables:

- **Enterprise-Cyber Risk Management:** If you're under attack or simply looking to proactively strengthen your controls, our Services team is here to help! Quickly gain access to the team on-demand from the platform.



### Penetration testing services

On-demand services

<p><b>Internal Penetration Test</b> \$13,500 \$12,240</p> <p>Emulate an attacker or insider's tactics, techniques, and procedures (TTPs) using privilege escalation to gain elevated access to the internal network.</p> <p><a href="#">Buy now</a></p>	<p><b>External Penetration Test</b> \$11,500 \$10,400</p> <p>Conduct a controlled attack simulation that uncovers vulnerabilities across applications, systems, and networks accessible from the internet.</p> <p><a href="#">Buy now</a></p>
---	---

[LEARN MORE](#)



## Marketplace

- ProcessUnity
- Jira On-Demand Ticket Creation
- S&P Risk Indicator
- Cybersecurity Risk Insights
- Salesforce Scorecard IMporter
- Threat Quotient
- Netskole CCI Integration



# Gatekeeper

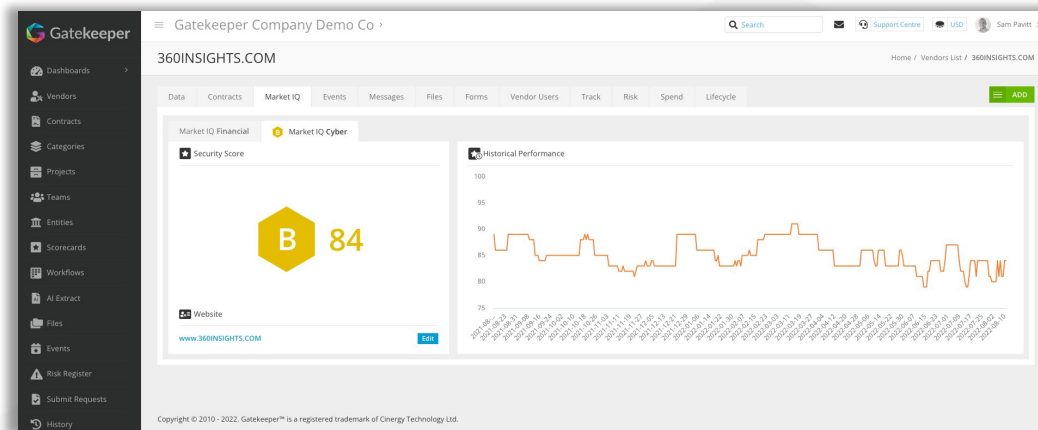
Deliver total visibility and awareness of security risks through the lifecycle of engagement with your third-parties



**How this helps you:** View top-level SecurityScorecard grades without leaving the Gatekeeper MarketIQ module

## Use Cases this Enables:

- **Vendor Risk Management:** Monitor cyber risk from your third-parties and work with them to manage issues that arise



[LEARN MORE](#)



# Jira On-Demand Ticket Creation

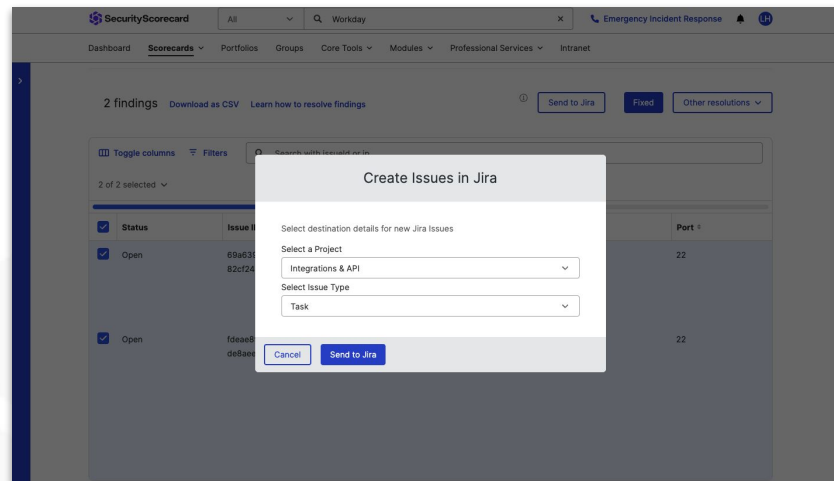
Automatically create actionable and detailed Jira tickets for individual Issue Findings from SecurityScorecard.



**How this helps you:** Triage individual issues in SecurityScorecard based on severity and score impact.

## Use Cases this Enables:

- **Enterprise Cyber Risk Management:** Automatically create actionable and detailed Jira tickets for individual Issue Findings selected from SecurityScorecard.



[LEARN MORE](#)



# S&P Supplier Risk Indicator

Evaluate any organization's supply chain risk.

**S&P Global**  
Market Intelligence

**How this helps you:** Evaluate supplier's with a single score based on key risk factors including cyber, financial, and ESG. Receive trusted data from two of the industry's leading Ratings companies.

### Use Cases this Enables:

- **Supply Chain Risk Management:** Monitor for and quantify supply chain risk with a single Supplier Risk Indicator (SRI) score. Drill down into the factors comprising the score to prioritize individual issues that could put your organization at risk.

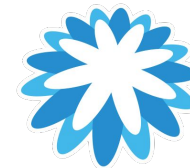


[LEARN MORE](#)



# Cybersecurity Risk Insights App for Coupa

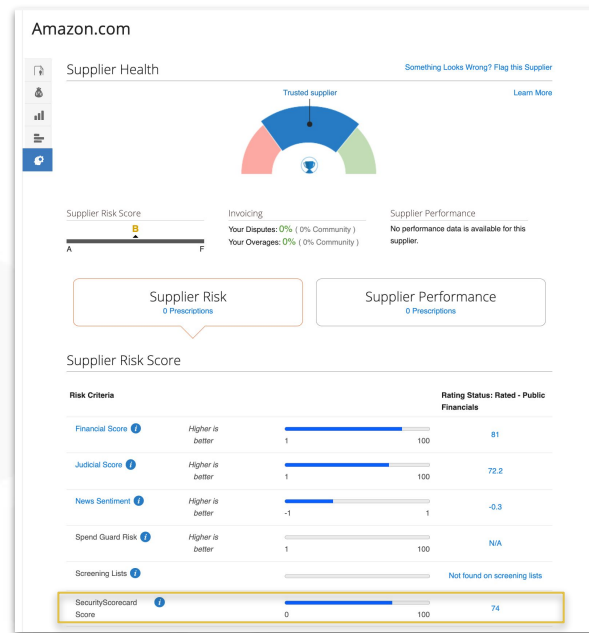
Understand how cyber risk impacts your Supplier's overall health in Coupa.



**How this helps you:** Continuously monitor and understand a supplier's overall cyber security posture across the entire procurement and supplier lifecycle to make more informed business decisions.

## Use Cases this Enables:

- **Vendor Risk Management:** Use SecurityScorecard's trusted cyber scores to evaluate suppliers during due diligence, onboarding, payment, and on an ongoing basis.
- **Procurement:** Automate approval workflows based on acceptable cybersecurity ratings. Automatically flag high-risk suppliers.



[LEARN MORE](#)



# Salesforce Scorecard Importer

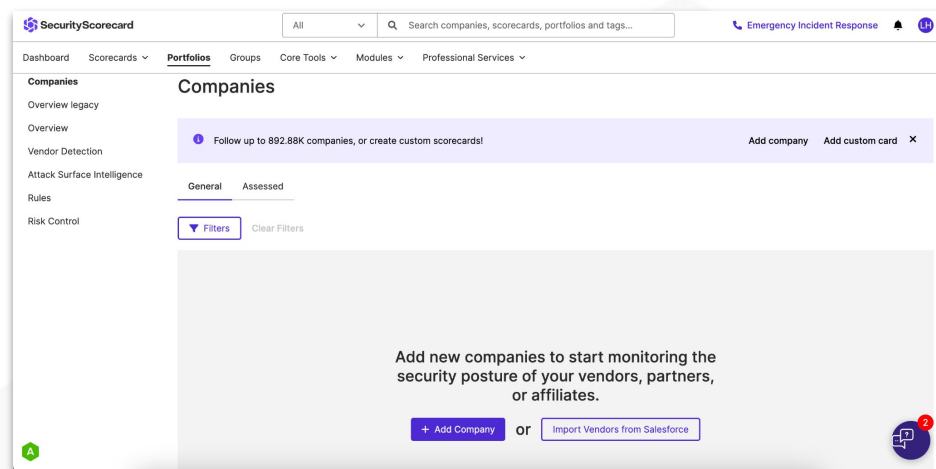


Bulk import vendor accounts from Salesforce to automatically create Scorecards.

**How this helps you:** Monitor Scorecards for your Salesforce vendor accounts with one-click using the Salesforce Scorecard Importer.

## Use Cases this Enables:

- **Vendor Risk Management:** Bulk import vendor details to fast from salesforce to fast-track SecurityScorecard onboarding.
- **Cyber Insurance:** Import client details from Salesforce to hit the ground running collaborating in SecurityScorecard



[LEARN MORE](#)



# ThreatQuotient Ratings Integration

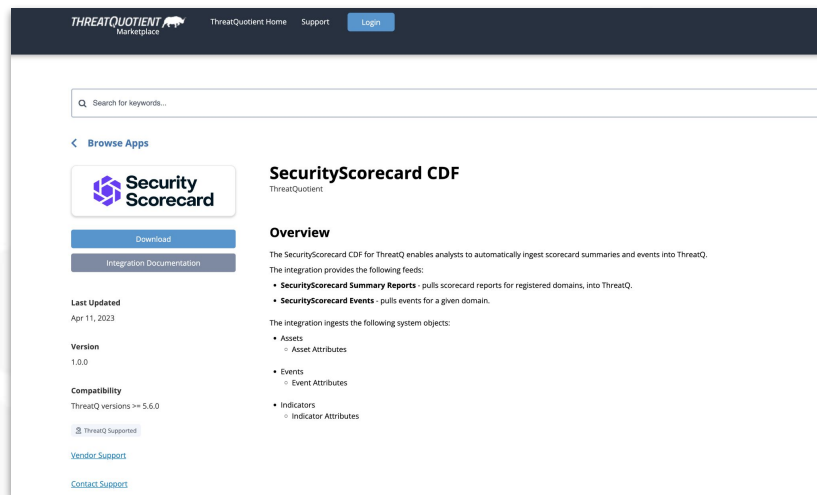


Automate continuous monitoring of your cybersecurity posture and that of your third-parties.

**How this helps you:** Accelerate threat detection and response with important data on your security posture.

## Use Cases this Enables:

- **Third-Party Risk Management:** Automatically monitor for vulnerable third-parties in your ecosystem by ingesting scorecard reports for registered domains into ThreatQ.
- **Enterprise Cyber Risk Management:** Import your organization's Scorecard data on 10 key risk factors into ThreatQ.
- **Security Ops:** Prioritize investigation and remediation based on events identified by SecurityScorecard



[LEARN MORE](#)



# Netskope CE Integration

Confidently make policy decisions based on accurate and comprehensive security risk data for your SaaS applications.

**How this helps you:** Understand the risk of applications being used by employees and how your ecosystem could be affected.

## Use Cases this Enables:

- **Third-Party Risk Management:** Enhanced vendor risk management with out-of-the box enablement of timely and actionable information on vendors' cybersecurity posture.
- **Enterprise Cyber Risk Management:** Get important risk information and IoCs to help security teams focus on the most critical threats in real-time.



The screenshot displays the SecurityScorecard dashboard for the company 1password.com. The main score is 96, with a grade of 'A' and a change of -1. The dashboard includes a navigation menu with options like Dashboard, Scorecards, Portfolios, Groups, Core Tools, Modules, Professional Services, and Intranet. The main content area shows the 'APPLICATION SECURITY' section for 'Netskope Security Cloud Confidence Index Data'. It includes a 'Data Source' of 'Netskope CE' and a 'DESCRIPTION' of the CCII database. A 'RISK' section indicates an 'INFORMATIONAL SIGNAL' that does not affect the company score. A 'RECOMMENDATION' section advises on assessing the need to use applications with a CCI score below 60 or a CCL below Medium. The interface also features buttons for 'Propose Plan', 'Add Tag', 'Contact Company', and 'More'.

[LEARN MORE](#)



# Platform

- Data Residency Compliance
- Audit Log
- Global Navigation

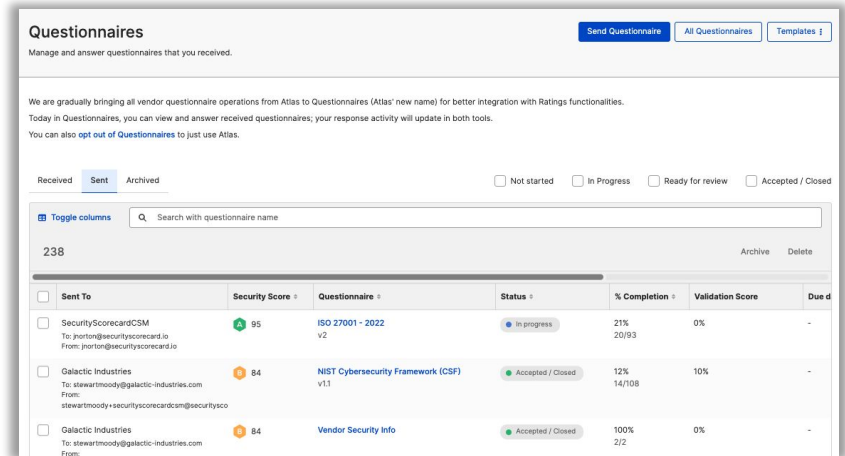
# Data Residency Compliance

Collaborate with your global vendors in one platform.

Confidently send and receive questionnaires with your partners in Europe and APAC.

**How this helps you:** Data residency requirements define which types of sensitive data need to be stored or processed within a specific geographic location in order to meet local data privacy laws.

Sensitive data provided by customers in Europe or the Asia Pacific region in Questionnaires, Evidence Locker, and other parts of our platform now resides locally.



**Questionnaires** Send Questionnaire All Questionnaires Templates

Manage and answer questionnaires that you received.

We are gradually bringing all vendor questionnaire operations from Atlas to Questionnaires (Atlas' new name) for better integration with Ratings functionalities. Today in Questionnaires, you can view and answer received questionnaires, your response activity will update in both tools. You can also [opt out of Questionnaires](#) to just use Atlas.

Received **Sent** Archived  Not started  In Progress  Ready for review  Accepted / Closed

Toggle columns

238 Archive Delete

<input type="checkbox"/>	Sent To	Security Score	Questionnaire	Status	% Completion	Validation Score	Due d
<input type="checkbox"/>	SecurityScorecardCSM To: jpurton@securityscorecard.io From: jpurton@securityscorecard.io	95	ISO 27001 - 2022 v2	In progress	21% 20/93	0%	-
<input type="checkbox"/>	Galactic Industries To: stewartmoody@galactic-industries.com From: stewartmoody@securityscorecard.com@securityscorecard.com	84	NIST Cybersecurity Framework (CSF) v1.1	Accepted / Closed	12% 14/108	10%	-
<input type="checkbox"/>	Galactic Industries To: stewartmoody@galactic-industries.com From:	84	Vendor Security Info	Accepted / Closed	100% 2/2	0%	-

# Audit Log

Easily track activities and actions that are taking place on the platform.

Improve internal controls and data security by regularly monitoring user audit logs.

**How this helps you:** Easily track who is accessing your data, what data is being accessed, and where it is being accessed from to improve internal controls, data security, and meet compliance and regulatory requirements

## Other Use Cases this Enables:

- **Enterprise-Cyber Risk Management:** Enhance your continuous monitoring efforts with a live Audit Log to track which teammates and which activities have been taken within the platform
- **Compliance:** Improve internal controls and meet regulatory requirements with continuous tracking of platform activity

**My Settings**

**ACTIVITY LOGS**

Creation date: 1 Jun, 2023 to 17 Jul, 2023 | Base Role: Select... | Status: Select... | Refresh Filter

Columns: Search

7 | Export all | Export selected

User	Last Login	Base Role	Activity Type	Status
Moreau, Martin martinmoreau@martinmoreau.tech	July 12, 2023 11:56 AM	Customer Admin	Password Login	Success
Moreau, Martin martinmoreau@martinmoreau.tech	July 5, 2023 11:21 AM	Customer Admin	Password Login	Success
Moreau, Martin martinmoreau@martinmoreau.tech	June 27, 2023 4:49 AM	Customer Admin	Password Login	Success

LEARN MORE



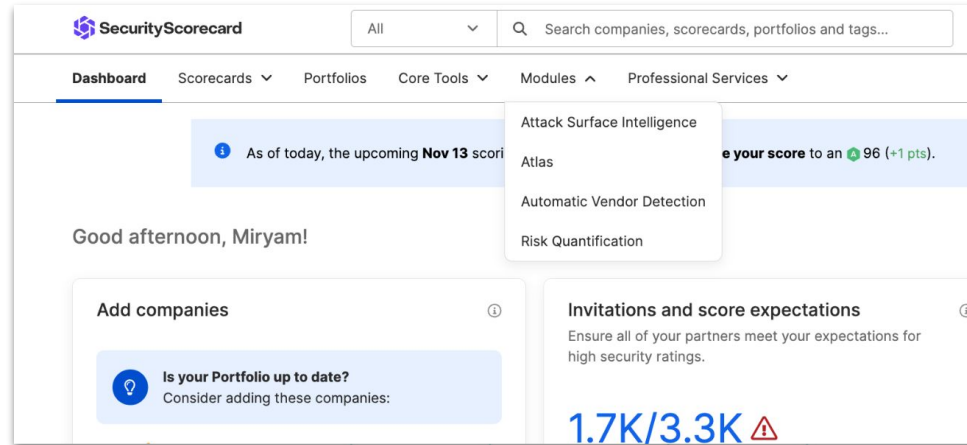
# Global Navigation

Simplify your workflows in SecurityScorecard with a smarter menu.

Harness the full power of the SecurityScorecard platform with an even easier to navigate navigation bar.

**How this helps you:** We've enhanced our navigation menu within the SecurityScorecard Platform, enabling you to accomplish what you need, faster.

Find what you need more easily with all Scorecard tools – including Scorecards, Portfolios, Core Tools, and Services – condensed into a simpler interface.





# Additional Resources

**EXPECT** the  
**UNEXPECTED**

# Live Webinar

October 31st, 2022  
2pm EST

Join us and learn how  
you can prepare to expect  
the unexpected.

[REGISTER HERE](#)



Prepare to Expect the Unexpected in our Q4 '23 Release

Learn how to build a resilient  
third-party risk management program  
and **expect the unexpected.**

WEBINAR

TUESDAY, OCTOBER 31, 2023



**Miryam Meir**  
Sr. Director,  
Product Marketing



**Perry Robinson**  
Sr. Solutions Engineer



## Q4 '23 Release Notes on our Help Center

Visit our Help Center to learn more about the Q4 '23 Release, see our release notes, and learn more about the SecurityScorecard Platform!

<https://support.securityscorecard.com/hc/en-us/articles/19207337800603>



## Learn more with our resources linked here!

### Learn about:

- [\[Ebook\] Expand your Vendor Intelligence to Identify Active Threats](#)
- [\[Video\] Building a Resilient Security Program with Moriah Hara, vCISO and Advisor](#)
- [\[Video\] What does it mean to Expect the Unexpected in third-party risk?](#)
- [\[Whitepaper\] DORA and Cyber Risk: A New Framework for Third-Party Risk in the European Union](#)
- And more!



Thank You

EXPECT<sup>the</sup>  
UNEXPECTED