
BLACK KITE
auxis
Stay Secure by
Staying Ahead
How to Shift to Proactive Cyber-risk Management

Why Now is the Time to Make a Change

Our latest research shows the number of ransomware attacks nearly doubled from 2022 to 2023, and third-party breaches grew by almost 30% during that same time period. Security teams are well aware of these looming threats and the potential consequences they present. So why does the frequency and impact of cyberattacks continue to grow despite increased spending globally on security and risk management?

We believe it's because third-party risk management (TPRM) hasn't kept up with a constantly evolving threat landscape. Many companies still rely on tools developed decades ago to combat today's third-party risk.

Historical TPRM practices and strategies force many companies into a reactive posture. To deal with today's dynamic risk landscape, these businesses must adopt new tools, processes and cultural norms that allow for a more proactive approach to cyber risk management.

Table of Contents

Where Traditional TPRM Falls Short 4

A New Approach to Third-Party Cyber-risk Management 8

Four Steps to Build a Proactive TPRM Program 11

Choosing a Cyber-risk Intelligence Platform 14

Where Traditional TPRM Falls Short

Many of the principles behind traditional supply chain risk management and TPRM were established decades ago.

For instance, in 2008, FDIC issued Financial Institution Letter 44-2008 (FIL-44-2008): Guidance for Managing Third-Party Risk, which set many precedents we follow today, including the use of questionnaires. A few years later, in the 2010s, a new market emerged that started using new technology to gather and analyze massive amounts of data about organizations' security performance. These solutions applied a scoring methodology to data analyzed by security rating services (SRS), with the idea of providing a simple score to represent a snapshot of an organization's cybersecurity posture.

However, today's threat and business environments look very different from those of two decades ago. An increase in third-party vendors increases an organization's attack surfaces and provides an attractive pathway to sensitive data. Increasingly complex supply chains, a lack of standardized security processes and limited resources (especially at smaller vendors) also contribute to more third-party breaches that compromise data, privacy and operations. In addition, we're facing a massive skills shortage in cybersecurity, meaning that many security teams lack the expertise to stay ahead of third-party risk detection and response.

Today's TPRM Landscape

- Increase in the number of third-party vendors
- Complex supply chains
- Lack of standardized security protocols
- Increasingly limited internal resources
- Massive cybersecurity skills shortage

Key Problems with Security Rating Services (SRS) Scores

- Frequent false positives impact grades
- Black box scoring methodologies
- Variations in scores across SRS companies
- Scores lack the context of each vendor's specific services and relationship
- Scores only reflect a single point in time and become outdated quickly

All of those factors make it hard to get value from traditional TPRM strategies, such as questionnaires. Not only are questionnaires time-consuming for vendors to complete and for security teams to review and analyze, but they also only provide a point-in-time snapshot of a vendor's posture. As companies scale to hundreds or even thousands of vendors, questionnaires become highly resource-intensive exercises with little long-term value.

Historically, SRS hasn't been an effective or trustworthy way to gauge risk either. There are countless instances of false positives in SRS scores, leading cyber teams to waste valuable time trying to mitigate inconsequential or nonexistent issues. And while a letter- or number-grade security rating via SRS might provide a general idea of an organization's cyber hygiene, the nuances between grades (e.g., C versus D) can be harder to decipher. It doesn't help that the SRS organizations offering these ratings often provide little insight into how they actually determine grades. In many circumstances, organizations employ more than one SRS and each may provide the organization with a vastly different score further complicating any ability to determine an organization's true level of risk.

A letter grade also doesn't contextualize risk in relation to a vendor's services. If two vendors have a C grade, for example, it could mean something very different based on the operational impacts your organization would suffer if those vendors were to experience a breach or attack. Consider last year's ransomware attack on port operator DP World Australia. The company manages about 40% of the goods that flow in and out of Australia and the attack crippled those critical operations. A subpar SRS grade for a company like that, which would significantly impact your own business continuity, requires more critical evaluation than a vendor that manages your organization's marketing website, for example.

Finally, grades only offer a point-in-time snapshot and are significantly impacted by past events, like a previous breach. Reporting on incidents after they happen isn't a good indicator of future risk. A former breach, for example, may actually be a good thing if it illuminates a previously unknown vulnerability and leads to a patch. A score based on a vendor's posture 30 or 60 days ago also doesn't fully represent a vendor's current position. The vendor may have implemented changes in its environment this month that could dramatically change its score, such as introducing new features or partners that incur additional risk.

Third-Party Cyber-risk Management: A New Approach

Cyber-risk management, the process of proactively identifying, analyzing and mitigating risks in an organization's cyber ecosystem, is the next evolution of vendor risk management. While traditional TPRM strategies are reactive, cyber-risk management identifies and mitigates risks before they become an issue.

The Key Components of a Proactive Cyber-risk Management Program Include:

- Continuous risk intelligence to supplement and contextualize cyber ratings.
- Alerts to changes in risk posture prioritized by business-specific risk tolerances.
- Forward-looking risk scoring tied to known threat vectors to highlight vendors most at risk of an attack.
- Actionable intelligence to understand the impact of emerging threats throughout the supply chain.
- Asset-level findings with clear steps toward incremental improvement.
- AI to free teams from manual processes, such as filling out questionnaires, so they can focus on more strategic work.
- Streamlined communication mechanisms that allow for seamless vendor collaboration.

Top Warning Signs That Your Company Is Susceptible to Attack

In today's cybersecurity landscape, threat actors are increasingly targeting supply chains and vendors to maximize the impact of their attacks. Therefore, it's crucial to monitor third parties and recognize the early warning signs of potentially disruptive attacks.

Here are some key indicators to watch for:

Critical Vulnerabilities: A critical vulnerability that has been or could be exploited by threat actors poses a significant risk. In addition, exploiting vulnerabilities remains the primary attack method for ransomware groups. But with thousands of vulnerabilities (CVEs) published monthly, not every vulnerability is necessarily a threat indicator. Rigorous analysis and vulnerability intelligence are essential to assess the actual risk.

Concentration Risk: When a significant portion of an organization's operations, data, or services relies on a single vendor, system or geographic area, a cyberattack targeting that concentrated point can have widespread and severe consequences. This centralization creates a single point of failure, increasing the potential impact of an attack and making the organization a more attractive target for cybercriminals. Diversifying dependencies can help mitigate this risk by spreading potential vulnerabilities across multiple areas.

Leaked Credentials: A high number of leaked credentials can indicate susceptibility to credential-stuffing attacks. This method, where attackers use stolen credentials to gain unauthorized access, is a common and effective tactic that is frequently a precursor to more serious incursions.

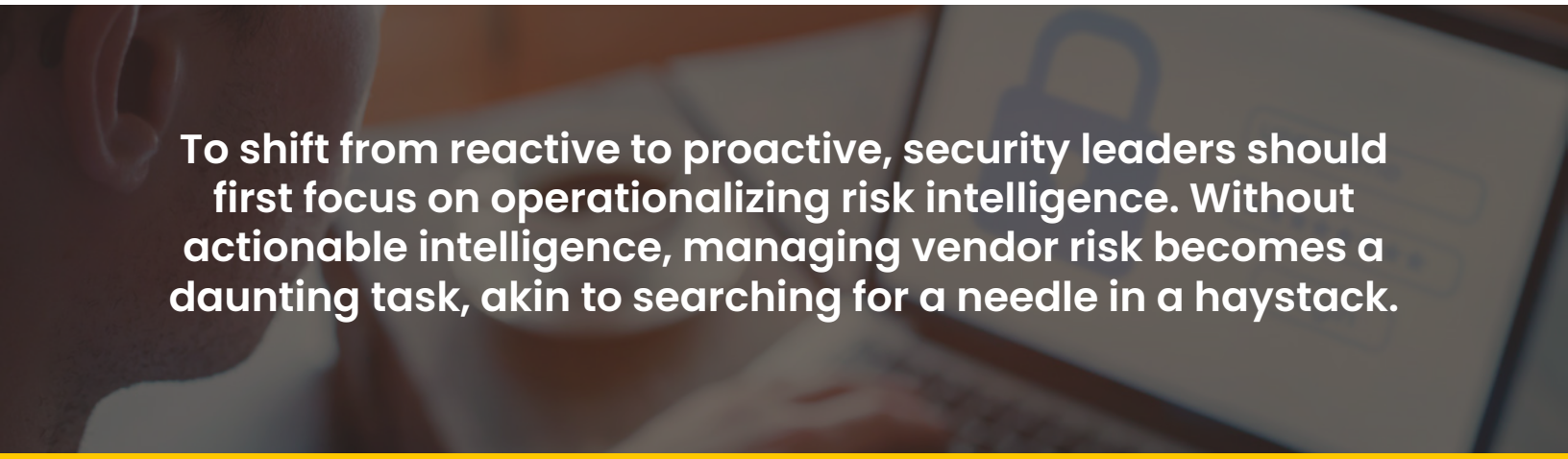
Past Breaches / Attacks: If a vendor doesn't properly address existing vulnerabilities, it remains at risk, and if data was compromised in a previous attack, it may be used to aid subsequent attacks. As our 2025 Ransomware Report shows, these repeat attacks are happening in quicker succession by different operators, indicating that ransomware groups are monitoring each other's attacks so they can strike while a victim is still weak.

Open Critical Ports: Open ports such as RDP (Remote Desktop Protocol) or SMB (Server Message Block) serve as an invitation to attackers. Identifying and securing open critical ports is vital.

Misconfigurations: Certain misconfigurations or missing configurations signal a weak cybersecurity posture. For example, the absence of SPF (Sender Policy Framework) or DMARC (Domain-based Message Authentication, Reporting, and Conformance) records leaves your organization vulnerable to spoofing and phishing attacks.

Cyber Ratings: Sudden changes in cyber ratings can signal emerging risks. But to leverage cyber ratings accurately, organizations must look at up-to-date ratings that reflect the latest threat intelligence.

Four Steps to Build a Proactive Third-Party Cyber-risk Management Program



To shift from reactive to proactive, security leaders should first focus on operationalizing risk intelligence. Without actionable intelligence, managing vendor risk becomes a daunting task, akin to searching for a needle in a haystack.

1 Collect Actionable Risk Intelligence

It's crucial to have a robust risk intelligence system that translates data into actionable insights. Generic questionnaires overwhelm vendors and drastically slow down the procurement process. Plus, they are often left unfinished, making it impossible to pull intelligence from the information. Instead, collect and analyze additional data from open-source intelligence (OSINT) sources and fill gaps with more targeted questionnaires when needed. Use that supplementary data to extract real intelligence from the information you collect.

Expert Tip: Ensure Data Quality

You must ensure data quality before turning data into intelligence. It's important that risk data is accurate, timely and complete so it doesn't compromise your ability to make good decisions. With that in mind, ensure the tools you're using provide high-quality data, then cross-verify that data, check sources and update your data regularly.

2 Implement Continuous Monitoring

Monitor vendors' risk scores regularly. To prevent information overload and resource strain, determine your key risk thresholds and set up alerts based on them. This way, you will only get alerts for the most pertinent concerns.

3 Form Strong Partnerships with Vendors

Establish a collaborative relationship with vendors. Don't burden them with questionnaire requests. Instead, collaborate using high-quality intelligence to foster trust and share incremental improvements. Communicate alerts and tactical guidance/support to vendors when you identify a vulnerability that requires action, like a spike in ransomware susceptibility.

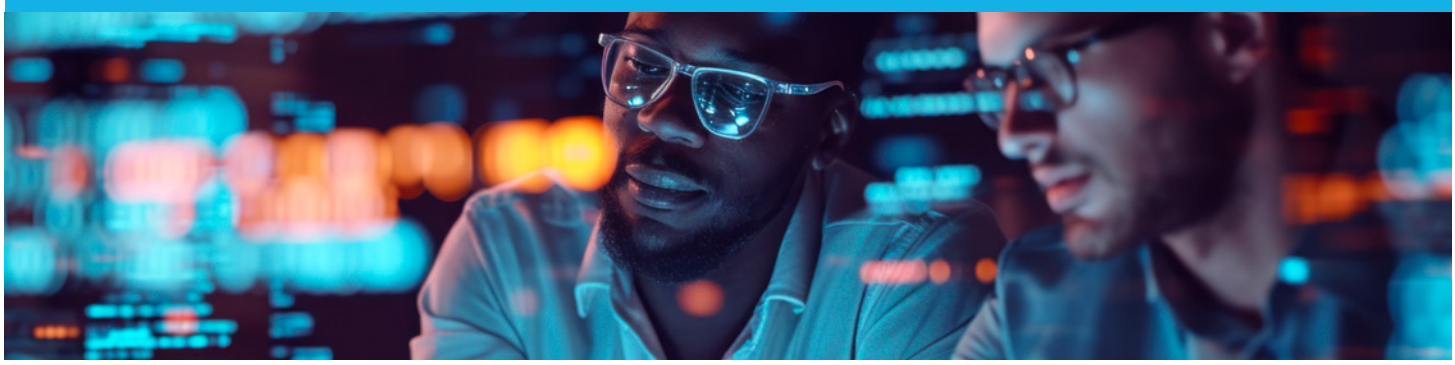
Expert Advice: How to Handle Risky Relationships

If a vendor is unresponsive or fails to remediate identified risks, more drastic measures may be necessary. Communicate your concerns about the vendor to internal stakeholders and decision-makers. Depending on the nature of the relationship with that vendor, and how embedded the vendor is within your environment, you may want to suggest a few follow-up actions to isolate systems connected to the vendor, withhold payment, or terminate the business relationship. Advise internal decision-makers to set up contractual terms that allow these types of actions when necessary. Clearly communicating these expectations from the beginning of the contract can set the right tone for vendor compliance.

4 Leverage Technology and Automation to Free Up Time

Use advanced tools and automation to continuously scan for vulnerabilities and monitor risk indicators. Set risk tolerances and automate alerts to notify you about emerging threats. A reduction in manual efforts will help your team focus on the most important risks and vendor relationships, freeing up valuable time to focus on strategic initiatives instead of transactional work.

Cyber-risk platforms, such as Black Kite, offer a centralized location to continuously monitor the health of your entire vendor ecosystem and make it easy to implement automation.



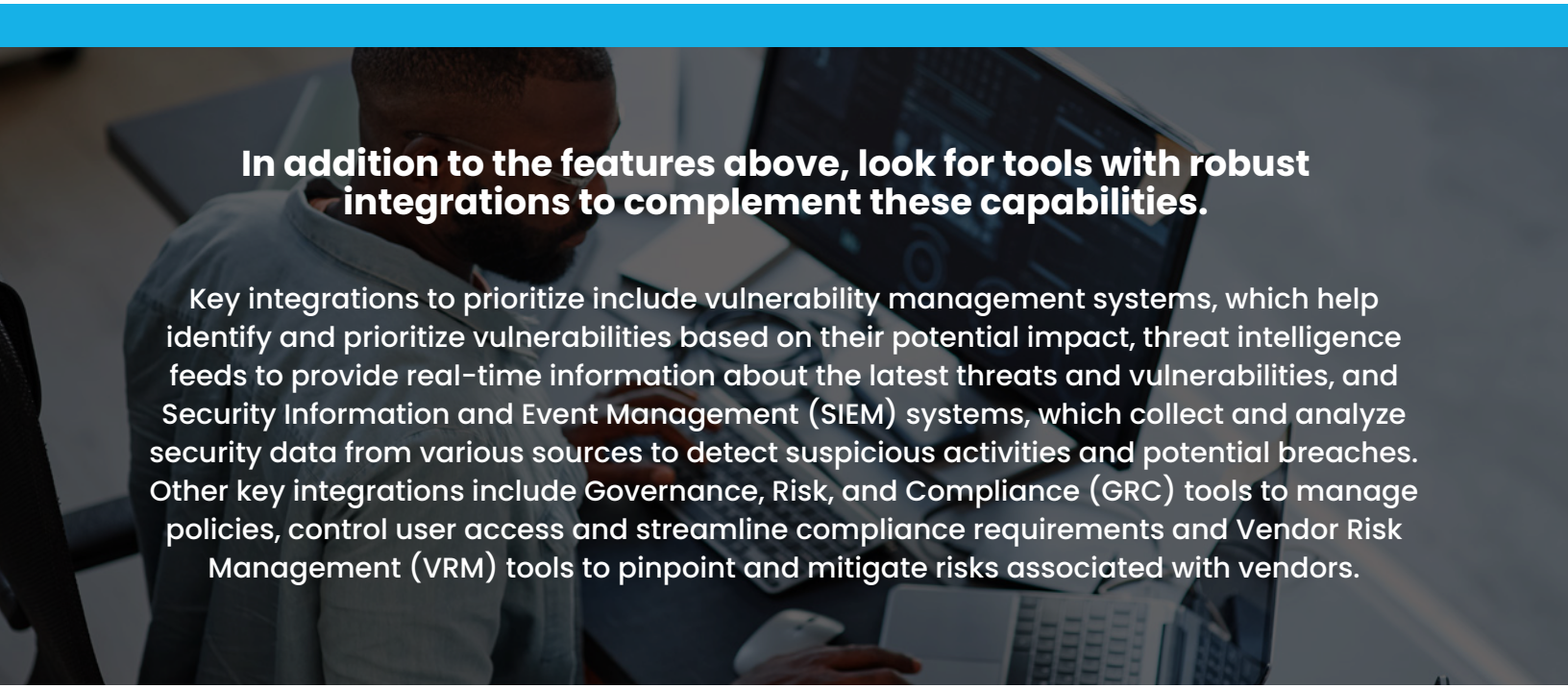
Choosing a Cyber-risk Intelligence Platform

To achieve proactive cyber-risk management, teams need the proper tools to anticipate, identify and respond to threats effectively. A cyber-risk intelligence platform is a great place to start in responding to risk indicators proactively.

When selecting such a platform, consider the following features and functionality:

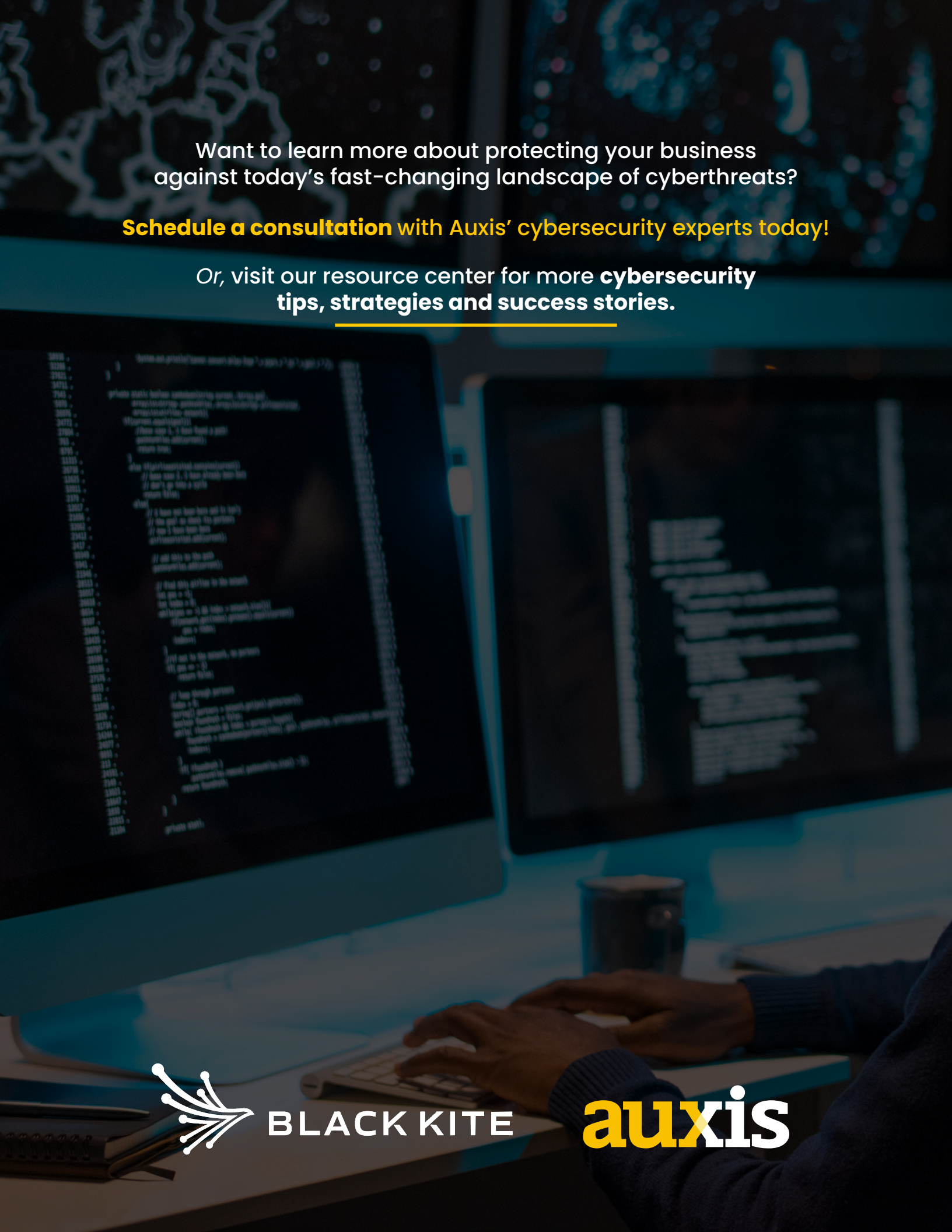
Feature / Functionality	Value
Multi-faceted Intelligence	**Relying on one score for overall cybersecurity posture is insufficient.** Look for platforms that offer several different ways of identifying and communicating risk, such as a cyber rating for overall posture, cyber-risk quantification (CRQ) and indicators of susceptibility to ransomware events. This multidimensional approach offers a clearer and more actionable picture.
Open Standards	**The platform should leverage commonly used open standards (e.g., MITRE's Att&ck Framework, Open FAIR™) rather than proprietary algorithms.** Open frameworks are transparent and widely accepted by practitioners, making their findings more objective and reliable. For example, if one platform rates something as low severity and another as medium, the rating based on open standards is more trustworthy.
Data Accuracy	**Sharing inaccurate intelligence with a vendor can damage trust and hamper future communications.** Ensure the platform provides a confidence level for each piece of intelligence so you can gauge its reliability before acting.
Speed of Intelligence	**If a platform delivers information too late, it loses its value.** For instance, if a vulnerability like MOVEit, exploited by the CL0P ransomware group, is reported weeks after its discovery, it's too late to mitigate the risk effectively.

Interpretability	**The platform should make it easy to interpret findings, understand asset vulnerability and define remediation steps.** With clear insights and action items, it's easier to communicate and collaborate with vendors and other stakeholders to remediate issues.
AI and Machine Learning Capabilities	**Technology like AI/ML can quickly analyze vast amounts of data and identify patterns that indicate emerging threats.** It can automate threat detection, predict potential attacks, and provide actionable insights, allowing teams to respond faster and more effectively. AI also aids in compliance, quickly mapping internal documentation to frameworks like NIST and ISO to evaluate gaps in compliance.
Third-party incident response workflows	**These features help manage and coordinate the response to third-party security incidents.** They provide capabilities for investigating incidents, tracking remediation efforts, and documenting the response process. Efficient incident response is critical for minimizing the impact of a third-party breach.



In addition to the features above, look for tools with robust integrations to complement these capabilities.

Key integrations to prioritize include vulnerability management systems, which help identify and prioritize vulnerabilities based on their potential impact, threat intelligence feeds to provide real-time information about the latest threats and vulnerabilities, and Security Information and Event Management (SIEM) systems, which collect and analyze security data from various sources to detect suspicious activities and potential breaches. Other key integrations include Governance, Risk, and Compliance (GRC) tools to manage policies, control user access and streamline compliance requirements and Vendor Risk Management (VRM) tools to pinpoint and mitigate risks associated with vendors.


Want to learn more about protecting your business
against today's fast-changing landscape of cyberthreats?
Schedule a consultation with Auxis' cybersecurity experts today!
Or, visit our resource center for more cybersecurity
tips, strategies and success stories.
BLACK KITE
auxis