3 WAYS TO EXECUTE YOUR

2022 Cybersecurity Strategy

Why is a Robust Security Strategy so Important?

Cybersecurity is evolving at a rapid pace. Businesses and cybersecurity leaders face numerous challenges on the digital landscape, where they must secure the constantly shifting cloud, manage and train an understaffed and hybrid workforce, and operate with restricted financial resources, all under increasingly complex governance mandates and regulations.

Pervasive ransomware attacks, supply chain threats, and an unsecured remote workforce raise grave concerns about cybersecurity risks for business leaders, according to CSO's recent *Global Intelligence Report: The State of Cybersecurity*[1] in 2021. According to the online survey of 2,741 security, IT, and business professionals around the world, businesses are investing significantly more of their security budgets to protect their sensitive assets from cybercriminals.

Top Cybersecurity Challenges Impacting Organizations

The only constant about cybersecurity is change.

Cybercrime

Global cybercrime costs are expected to grow by 15 percent per year over the next five years, reaching $10.5 trillion annually by 2025.[2]

Ransomware

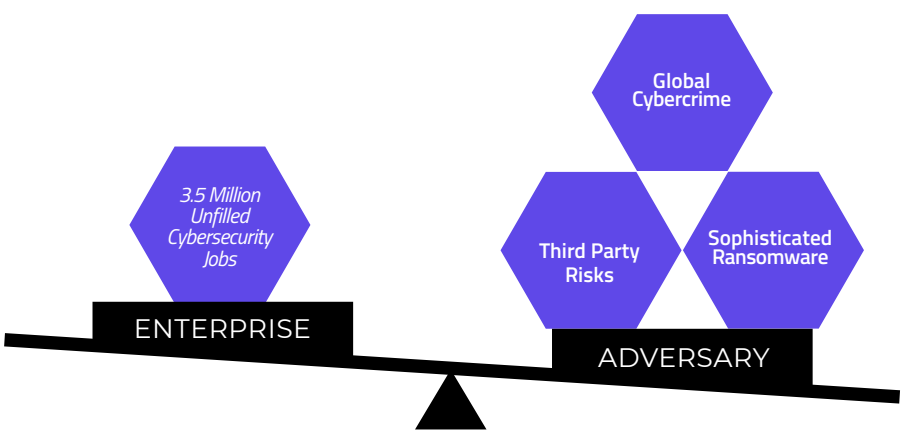
Increasingly sophisticated ransomware perpetrators will strike every 2 seconds, and cost its victims more than $265 billion annually by 2030.[3]

Supply Chain

Approximately 75 percent of third-party applications in the supply chain will sustain a cyber attack due to unprotected vulnerabilities.[4]

Increasing Regulatory Pressures & Mandates

The Shortage of Cybersecurity Talent and the Alarming Skills Gap Put CISOs & Security Teams at a Severe Disadvantage on the Threat Landscape.



As we approach 2022 and beyond, security experts predict more decentralization, regulation, and security implications. This paradigm continues to create complexity for security teams.

How Can You Tip the Scale in Your Favor?

With continuous visibility of your business and third-party risk.

55%

Firms want "real-time" visibility into threats & continuous monitoring of security controls.[5]

87%

Businesses need skilled IT security personnel, yet IT budgets grew only 4%.[6]

59%

Enterprise leaders want more centralized control over their third-party relationships.[7]

Resiliency is a Must-Have for Every Business

THERE IS HOPE ON THE HORIZON:

3 Proven Tactics to Navigate your Security Journey

Threats move fast. To move faster, security leaders and their teams need to continuously identify, integrate, and assess security risks in order to mitigate threats and optimize resources. Here are three proven tactics to increase coverage of security risks, save time, and outpace threats, enabling your business to grow with efficiency and trust.

IDENTIFY 1

Scale Vendor Risk Management (VRM) with intelligence to make strategic and rapid decisions.

Managing supply chain risk at scale isn't easy. But with the right resources, you can enable your organization to tackle complex challenges and gain an operational advantage.

Leveraging a robust VRM program empowers you to streamline portfolio analysis across the vendor ecosystem to rapidly detect potential threats and prioritize accordingly.

With the right security ratings and questionnaire automation platform, you can reduce the vendor questionnaire assessment process by 83%, enabling your organization to confidently onboard and continuously monitor third parties.

INTEGRATE 2

Automated integrations empower you to do more with less and accelerate productivity.

Get the most from your resources by integrating signals and automated rule-based workflows.

Utilizing a flexible, API-driven security ratings platform enriches the findings from your SIEM, GRC, VRM, and risk intelligence platforms with insightful data, and vice versa.

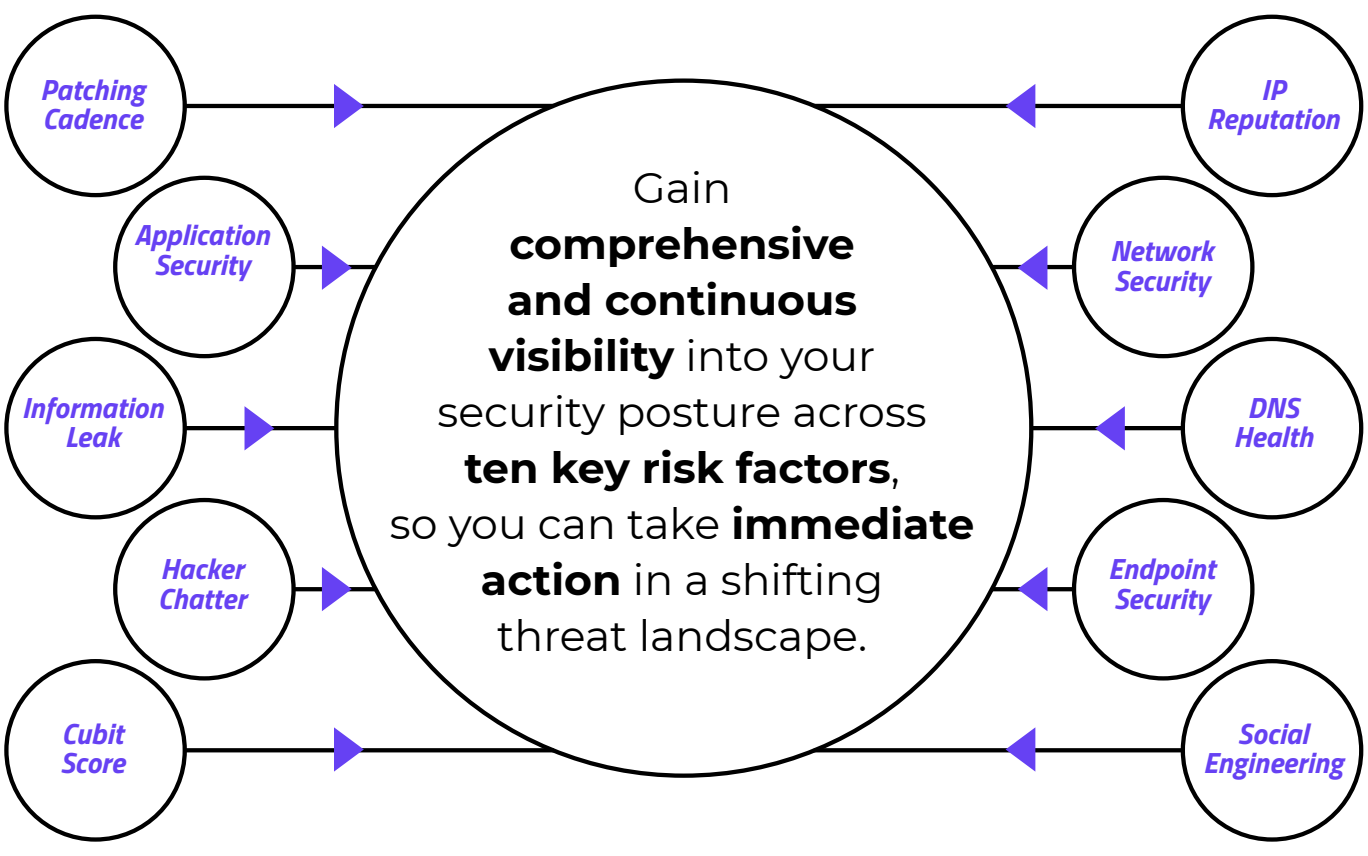
Whether you're on the security operations, infosec, IT, compliance, or vendor risk management team, syncing your existing tools with a comprehensive ecosystem of integrations will improve your capabilities to swiftly deter cyber attacks.

ASSESS 3

Optimize security resources and focus on your business growth.

IT staff wear many hats and often don't have the time to take full advantage of security investments or ramp-up their education to sharpen their edge with the latest innovations. Augment your team's capacity through professional services and ongoing security training and education to optimize and retain your existing resources, ultimately driving more business value.

Incorporate Security Ratings Into Your 2022 Cybersecurity Strategy



Tip the Scale in Your Favor

Let SecurityScorecard Help Build Your 2022 Strategy

Thousands of customers trust SecurityScorecard's cybersecurity ratings platform to make faster and smarter business decisions. Learn how SecurityScorecard's platform, professional services, and services enable security teams to stay ahead of risk.

LEARN MORE

1 IDG, State of Cybersecurity, 2021

2 Cybercrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, 2020

3 Cybercrime Magazine, Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031, 2021

4 CSO, Vulnerabilities in third-party apps cause 75 percent of attacks, 2013

5 MetricStream, State of IT and Cyber Risk Management Report, 2021

6 Palo Alto Networks, Unit 42 Ransomware Threat Report, 1H 2021

7 Ponemon Institute, A crisis in third-party remote access security, 2021

SecurityScorecard