riskrecon
mastercard

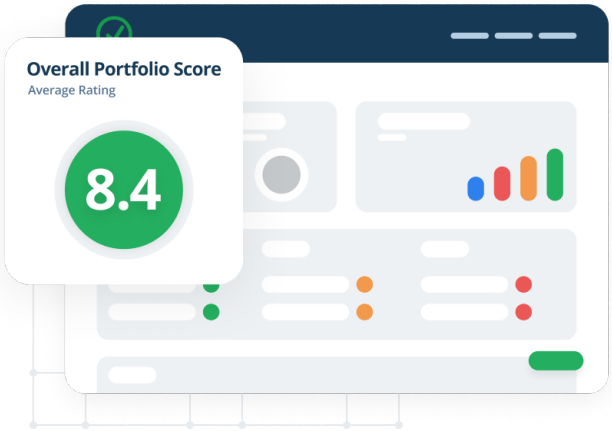
EASILY UNDERSTAND AND ACT ON YOUR THIRD-PARTY CYBER RISK

# Solve your third-party cybersecurity risk at the speed of business

## Automation tuned to match your risk appetite

RiskRecon makes it easy to gain deep, risk contextualized insight into the cybersecurity risk performance of all of your third parties. Simply give us the names of the companies you want to assess and we'll give you deep, continuous risk insight spanning 11 security domains and 41 security criteria.

RiskRecon assessments are custom fitted to match your risk appetite, focusing your analysts and your vendors on the issues that matter most to you. This capability is built on RiskRecon's core proprietary differentiation – our ability to automatically risk prioritize issues based on issue severity and the system value at risk.

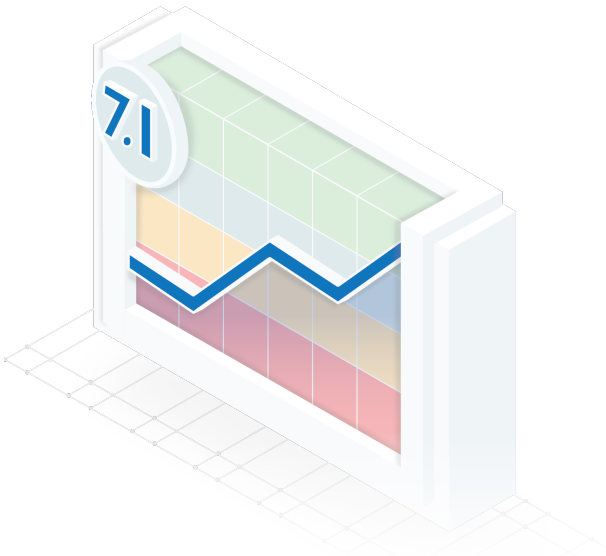



## Maximize Efficiency

RiskRecon provides risk assessment automation that streamlines every stage of your vendor cyber risk management process. Select new vendors faster. Prioritize your third-party assessments based on RiskRecon-rated vendor performance. Focus your vendor assessments on areas where you know they violate your risk requirements. Enable your vendors to understand and address issues faster.

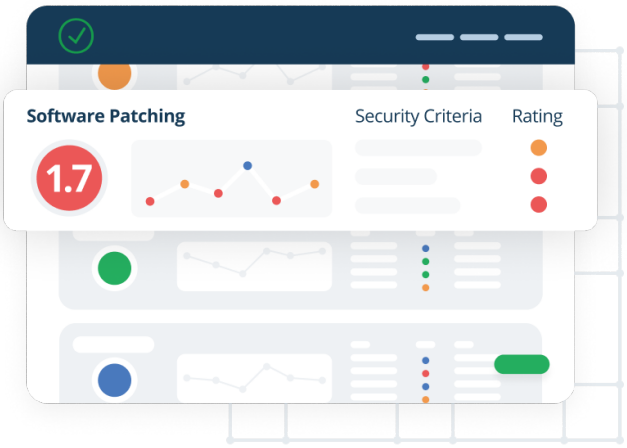
## Minimize risk

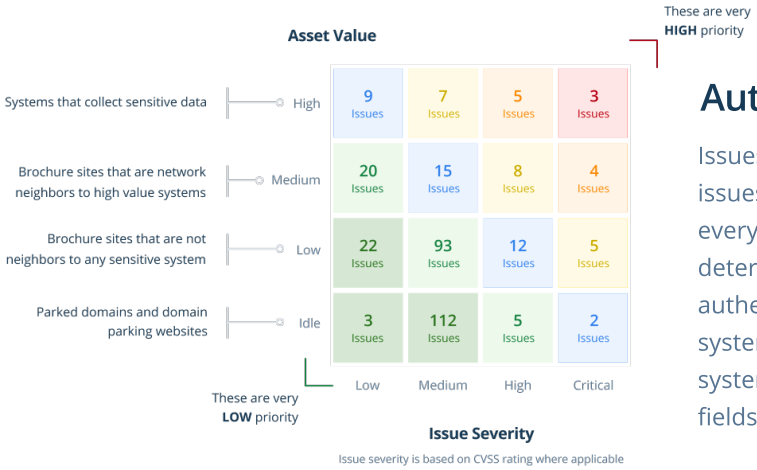
RiskRecon gives you the deep, continuous risk insight necessary to rapidly understand and act on your risks. Point RiskRecon at any enterprise, and RiskRecon returns to you deep risk assessment spanning 11 security domains and 41 security criteria – software patching, network filtering, ip reputation, web encryption, application security, and more. All fully risk contextualized and tuned to match your risk appetite.



## Continuous, Comprehensive Assessment

RiskRecon gives you the visibility to know the cybersecurity risk performance of your vendors by continuously assessing their performance across 41 security criteria spanning 11 security domains. Areas assessed include software patching, web encryption, email security, network filtering, IP reputation and malware defense, DNS security, web application security, and more. All vendor issues are automatically risk prioritized based on asset value and issue severity, providing you a clear understanding of their performance and the issues that matter most.



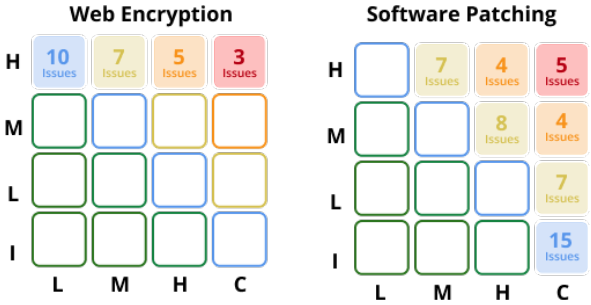



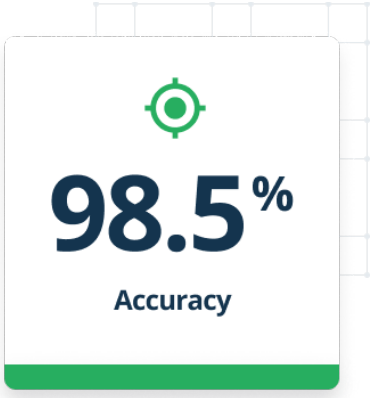

## Automated Risk Prioritization

Issues are not risks. Knowing risk requires understanding the security issues and the value at risk. RiskRecon automatically risk prioritizes every finding based on issue severity and asset value. RiskRecon determines value at risk by discovering the data types collected, authentication capabilities, and transaction capabilities for every system. This is accomplished through machine learning analysis of system code, content, and configurations to identify, for example, form fields collecting email addresses, credit card numbers, and names.

## Custom-tuned to Match Your Risk Priorities

RiskRecon puts your risk priorities front and center, enabling you to custom tune RiskRecon assessments and vendor action plans to match your risk priorities. Simply configure your risk policy once, using RiskRecon's graphical risk policy module, and every vendor assessment and action plan will be custom-fitted to match your risk priorities.




## Accurate Data

RiskRecon's asset attribution is independently certified to 98.5% accuracy. And we don't hide any of the assessment details. It's all visible to you and your vendors at no additional fee. Action requires accuracy and transparency. RiskRecon provides you both.