THIRD-PARTY RISK ASSESSMENT

EXTEND RESOURCES

Explore vendor security posture and identify potential risks to your organization.

Today, companies rely on vendors and a variety of third-party organizations to operate. From cloud software and IT services companies to an outside bookkeeper or law firm, vendors often have access to your systems where sensitive data is stored.

Without proper management, these third parties—and the fourth parties they depend on—can introduce dangerous information security risks into your environment.

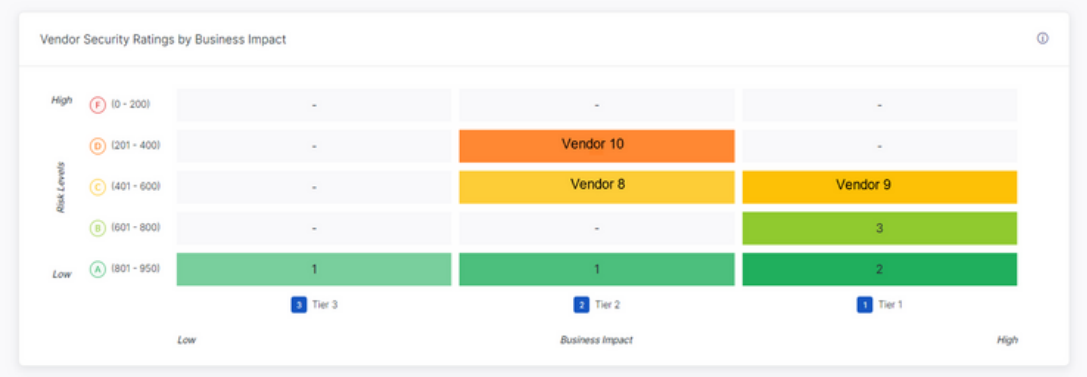
Assessing third-party risk helps you understand the security posture of your vendors, identify any potential risks, and work with those organizations to reduce those risks.

Risk assessments from EXTEND Resources give you the insights you need to address outside threats and enhance your overall security practices.

4 SIGNS IT IS TIME TO ASSESS THIRD-PARTY SECURITY RISKS.

1. It has been more than one year since you last assessed vendor risk.
2. You have not assigned business impact categories to your third parties.
3. You don't know if your third parties have experienced a recent data breach.
4. You don't know if vendors meet the cybersecurity requirements in your contract.

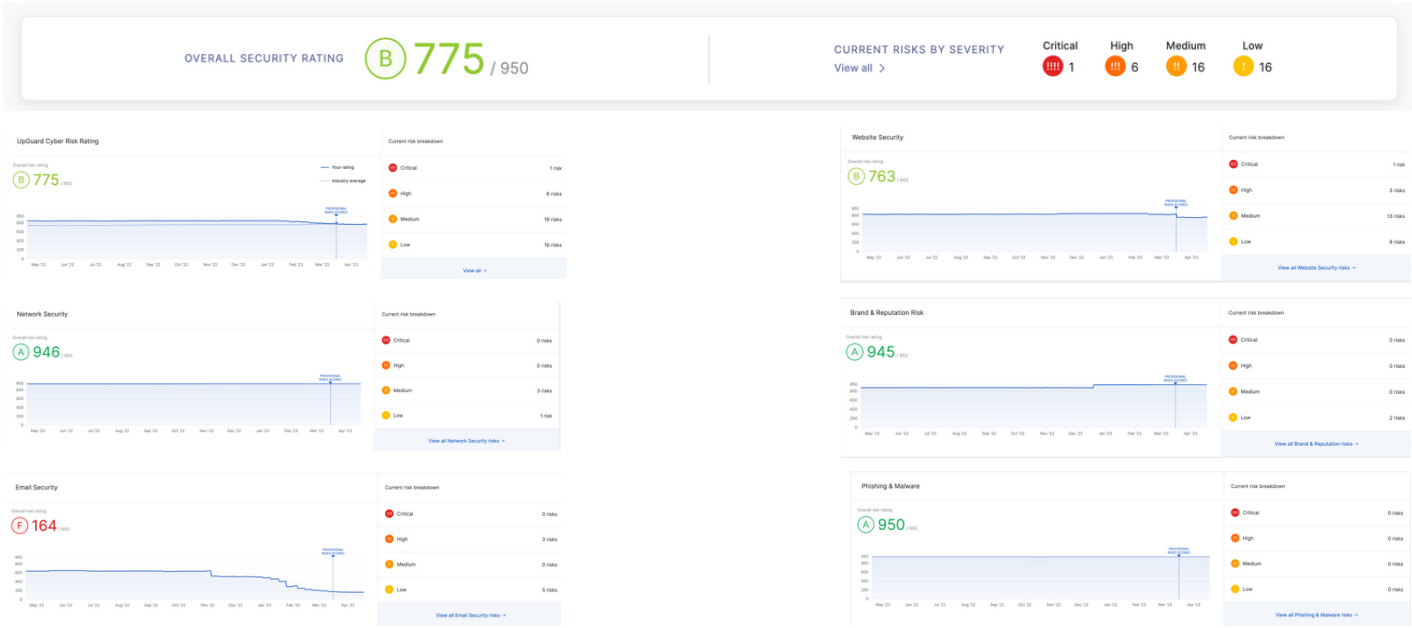
COMPARE VENDORS BY BUSINESS IMPACT AND RISK LEVELS



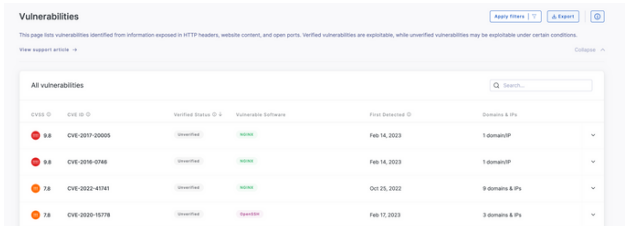
VALUABLE RISK INSIGHTS ACROSS SIX KEY THREAT AREAS

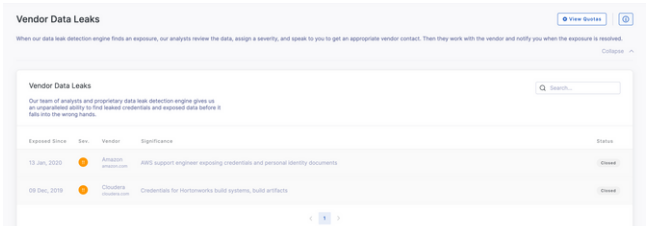
In addition to insights into a vendor's overall security score, EXTEND provides security risk ratings, rating trends, and a breakdown of risk severity in five critical areas. Plus, discover vendors' geolocation to investigate other risks.

- Overall Cyber Risk
- Website Security
- Network Security
- Brand & Reputation Risk
- Email Security
- Phishing & Malware



VISIBILITY INTO VENDOR VULNERABILITIES AND DATA LEAKS





Ready to identify and mitigate security risks throughout your vendor ecosystem?

CONTACT US

EXTEND RESOURCES

T/F (203) 479-9408
info@extendresources.com

1127 High Ridge Road, Suite 170, Stamford, CT 06905
V20230417