PREBREACH
RISK BASED SECURITY

PreBreach® – Verify First then Trust

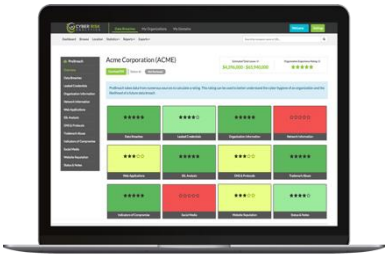
For years, business leaders have been asking the question, "How do I know which companies' security I can trust?" Check box assessments tell only a part of the story and formal audits can be impractical and too expensive when there are hundreds of organizations in the supply-chain to evaluate.

"PreBreach gave real teeth to our vendor selection and due diligence process. Without it we were flying blind."

— Supply-Chain Manager, Fortune 500 Bank.

PreBreach is Risk Based Security's answer to the security trust question, providing subscribers with the ability to make informed risk decisions about current and potential suppliers, insureds, clients, partners, acquisition targets, websites, cloud services, and even their own Internet security posture.

An organization's risk profile changes over time. PreBreach is constantly gathering and analyzing millions of global security attributes to measure security performance and help subscribers make informed judgments about security risk at business associates, partners and suppliers.



PreBreach provides risk profiles in nine categories based on over 1,000 security attributes, 49,000+ data breaches, 400,000+ specific indicators of compromise checks, 4.4 billion exposed email addresses and 244,000+ software vulnerabilities.

IMPROVE SECURITY THROUGHOUT YOUR SUPPLY CHAIN

PreBreach is perfect for organizations that want to implement a true due diligence program, but need help gathering data. PreBreach is designed to improve security posture awareness throughout your supply chain by enabling you to rate your vendors in twelve security categories. Whether it's evaluating one critical supplier, or quickly gauging the aggregated risk of your entire portfolio of suppliers, PreBreach provides visibility into supply chain risk to help you chose suppliers and focus on the ones that need improvement.

When used with Risk Based Security's Cyber Risk Analytics and VulnDB™, PreBreach™ empowers you to assess a given organization's risk level so you can avoid high-risk vendors and acquisitions or improve the resilience of those you have already engaged.

Why PreBreach?

- Solve your supplier due diligence and monitoring resource gap
- Get security posture data without hiring expensive full-time security staff
- Jump start your supply-chain management program with an easy-to-use, cloud-delivered SaaS program
- Conduct due diligence on partners, clients, and potential acquisitions
- Utilize best-in-class methods for identifying potential supply-chain risks
- Develop effective risk mitigation strategies for addressing higher-risk vendors
- Align vendor management controls with current performance risks
- Implement on-going supply-chain oversight utilizing metrics and external alerts
- Quickly scale your security monitoring operation as your vendor and supply chain partner base grows

Contact Risk Based Security

3308 W Clay St,
Richmond, VA 23230

(855) RBS-RISK

sales@riskbasedsecurity.com

www.riskbasedsecurity.com

vulndb.cyberriskanalytics.com

www.cyberriskanalytics.com

PreBreach Metrics

PreBreach includes a high-level summary of an organization's breach experience and security posture along with the details in twelve categories.

1. **Data Breaches** include both aggregated breach statistics for the organization as well as links to the specific breach events directly involving the organization. The organization's overall breach experience for the previous five years is reflected in a five-star rating. The rating is a combination of factors including individual breach severity scores, frequency and date of incidents.
2. **Leaked Credentials** provide an overview of the breaches that leaked users' credentials including an email address within the monitored domain.
3. **Organization Information** includes business type and subtype classification, links to the organization's website, address map and publicly available financial highlights.
4. **Network Information** is divided into six sections, covering domain and server information as well as detection of various control settings.
5. **Web Applications** displays detected applications running on the monitored domain. This information is useful for understanding how the site may be vulnerable to new or possibly unpatched weaknesses based on the technology deployed.
6. **SSL Analysis** alerts subscribers to the presence of SSL implementation – the standard for creating an encrypted link between the browser and the webserver.
7. **DNS and Protocols** is a list of the DNS resource records detected.
8. **Trademark Abuse** is a list of potential trademark infringements found on the site.
9. **Indicators of Compromise** checks the domain against numerous sources and entries, looking for potential signs the domain has been implicated as a part of a botnet, distributor of malware and other indicators of malicious activity taking place on the site. If an issue is detected, it indicates the site's IP has been flagged for suspicious activity.
10. **Social Media** the detection of social media engagement across the site.
11. **Website Reputation** includes a validation image of the home page for the monitored domain, provides site statistics and site size analysis useful for understanding the overall attack surface of the domain.
12. **Status & Notes** is where the organization can capture the organization's status and leave notes for team members.