edgescan™

DATASHEET

Risk Rated

Let's secure what matters, starting with what matters most.
This is prioritized threat intelligence with a human touch.

What Do I Fix?

With Edgescan's hybrid validation approach, you'll get a list of vulnerabilities across your full stack that's virtually free of false positives every single time.

That's efficiency: unlike scanners or other tools, our continuous security testing and unified exposure management SaaS platform won't serve up an index of 1,100 potential vulnerabilities and leave you to figure out what's what. You'll get all the verified, active threats and nothing more.

When Do I Fix It?

But even once the real problems are separated from the rest—the signal in the noise—there's a next question: "What should But even once the real problems are separated from the rest—the signal in the noise—there's a next question: *"What should I fix first?"*

The answer will yield huge dividends for your information-security team and your business as a whole—if you can find it quickly and consistently. With the right information about which threats to prioritize, you can dramatically improve the efficiency of your remediation process, delivering value back to your business in the form of time and money while strengthening your security posture.

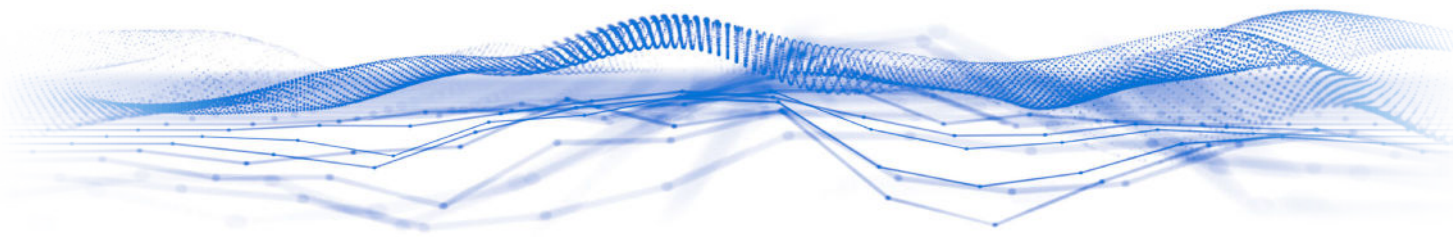
Edgescan consistently delivers those answers to organizations large and small with data-powered tool sets backed by the human element: on-demand support from CREST- and OSCP-certified experts.

Risk-Rating From Every Angle

Once vulnerabilities are assessed across your web-facing assets, a list of them will be compiled in the Edgescan dashboard. That's also where you'll find an all-you-can-eat buffet of risk-prioritization tools to guide you through your remediation process:

- There's the Common Vulnerability Scoring System (CVSS), the generalized scoring system which any vulnerability-management tool would need to provide.
- There's the Cybersecurity & Infrastructure Security Agency's Known Exploited Vulnerabilities catalog (CISA KEV), which speaks to whether the particular vulnerability in question has been exploited somewhere out in the wild today. This framework is constantly updated via API to pipe new common issues into the Edgescan dashboard as they're identified.
- There's the Exploit Prediction Scoring System (EPSS), which tells you how likely it is that a specific vulnerability will be exploited based on the prevailing trends and current landscape.
- And then there are Edgescan's proprietary tools, including the Edgescan Validated Security System (EVSS), which serves up a bespoke score for each client that takes into account everything we know about their organization.

That includes the systems architecture, how many layers of the stack we're testing for them, any context around their network vulnerabilities that affects their application vulnerabilities, and which—if any—compensating controls they have in place.



The internal security team can risk-accept vulnerabilities one by one and let us know why they made each decision. In the end, you're left with a score customized to your organization, from critical all the way down to minimal.

But then there's the ultimate metric for your risk-rating process: the Edgescan eXposure Factor (EXF).

The EXF Difference

What if you could combine all of the resources above to dynamically generate breach probability data in the aggregate?

The Edgescan eXposure Factor does just that, combining metadata from CVSS, EPSS, and CISA KEV to assess each discovered and validated vulnerability on a 0 to 100 scale, where a lower score indicates minimal risk and a higher one signifies greater vulnerability. It's a single unified metric to gauge the degree of exposure and how menacing it may be in the context of your overall security posture.

The Edgescan eXposure Factor is displayed to the user on the Vulnerabilities page of the Edgescan dashboard under the title EXF. It's recalibrated daily via dynamic feeds from all the constituent sources to keep pace with exploitation intelligence in the wild and incorporate changes to your organization, your network, and your overall security posture.

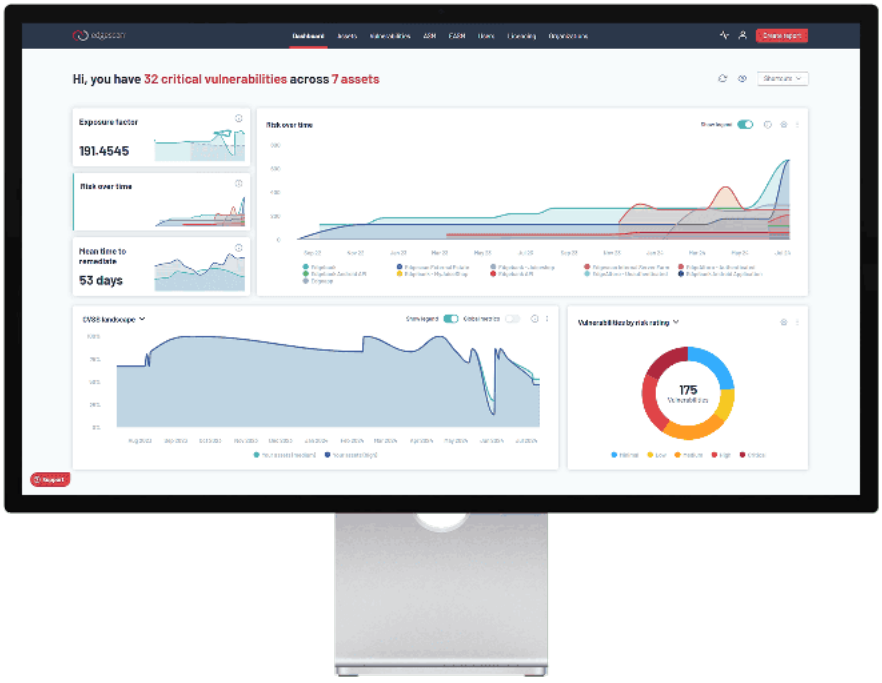
The Human Element

The range of tools included in the Edgescan platform will deliver context around your vulnerabilities using vast data resources and proprietary analytical techniques.

But the real power of Edgescan lies in backing all this mechanical power with the dexterity and depth of human intelligence. If you're looking for further insight into a particular vulnerability, the Edgescan support team is on call to provide a guiding hand when making your remediation priority decisions.

These CREST- and OSCP-certified experts are full-time Edgescan employees who've been with the firm an average of seven years, and you can request to speak with a licensed penetration tester at any time.

This bespoke service enables us to meet our ultimate goal: to fit into and enhance your security program as it stands.



 |

Small Org, Big Org

Your ideal tool will vary according to your organization's needs, but the Edgescan eXposure Factor (EXF) often proves particularly valuable to smaller organizations with internal security teams of commensurate size. Some may have a handful of employees, others just one, who are focused on information security.

While these shops will typically have fewer web-facing applications and less expansive network architecture than their larger peers, they're still likely to run into a threat matrix that's challenging or even overwhelming. With lots of potential vulnerabilities to address and limited resources to do so, the EXF becomes a key tool in their remediation assignment process, offering a quick, simple, and dependable blueprint for a team scrambling into action.

That said, the EXF is also a boon to large security teams managing the sprawling web-facing infrastructure of a major organization. No matter how great the organization's resources, the internal security team is unlikely to have all the personnel necessary to devote huge amounts of time to remediating any one vulnerability.

The EXF becomes their blueprint, too, and when they can move quickly and decisively against major threats, the security team can produce concrete results on the record—a crucial element to operating within a large enterprise with many stakeholders. When you can point to 12 security gaps exploitable to malign actors that you've closed over the last month, it goes a long way.

That's one of the many benefits of compiling all the real threats in your Edgescan dashboard, rated for their level of risk so you can fix the worst first and power on from there. That's risk-rated remediation intelligence with Edgescan.

For more information on how Edgescan can help secure your business, contact: *sales@edgescan.com*