edgescan™

DATASHEET

Full Stack

Many security teams rely on a growing number of partial, disparate, and siloed solutions to maintain their security posture, sometimes dozens at a time. But bad actors have a holistic view of any organization's attack surface. Why shouldn't your security team have the same? You can—with Edgescan.

Too Many Tools

Cybersecurity technology has developed in a piecemeal fashion.

As new types of web-facing assets grow in prominence and become integral to the operations of large organizations—applications, APIs, IOT devices—they also become targets for malign actors. Attackers gradually expose vulnerabilities in each new component and the cybersecurity field continually responds, springing into action to develop new, specialized tools to manage each new region of the attack surface.

This is the arms race between bad actors and security professionals, and each defense technology matures over time through innovation and competition between different firms offering rival solutions to manage each area.

But in this model, the two competing tools both still focus on one layer of the stack, and the market for cybersecurity solutions has thus developed as a bunch of different markets for a bunch of different specialized products.

For most security leaders at large organizations, the question is still, "Which tool is best to protect this layer?" But too few security teams are asking, "How do I think holistically about my attack surface, just like an attacker does? And is there a solution that will accurately detect vulnerabilities that are critical threats to our organization, regardless of where they might occur across the full stack?"

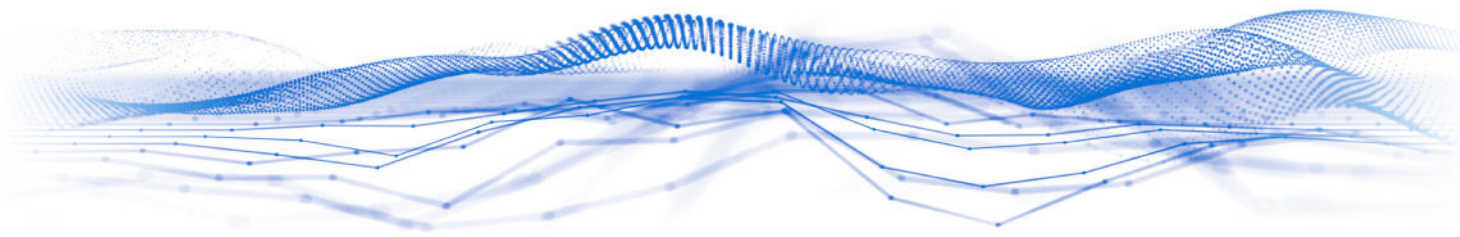
Wait—What is the Full Stack?

It's a common term in IT and software-development circles—a "full-stack developer" is often in high demand—but what does this term signify in the context of vulnerability management?

The stack has five distinct layers:

1. Web Application Layer
   (including APIs, website, mobile)
2. Hosting Environment layer (Web Application Server)
3. The Host Operating System
4. Host Machine Services
   (network protocol, services and ports)
5. Underlying Network
   (associated devices including IOT, firewalls, router)

These layers have nuanced differences, but that doesn't mean they each require different tools from different vendors. And yet...



Siloed Solutions

The main result of the point-solution paradigm is that many organizations have built up an unwieldy set of solutions, each dedicated to its own layer of the stack. In many cases, this array of different tools is unmanageable because of the sheer number of moving parts and the difficulty in getting them—and the security team members managing them—to talk to each other effectively.

"The reality of security today is that security leaders have too many tools," Gartner's Top Security and Risk Trends for 2021 found. Security leaders reported having an average of 16—yes, sixteen—or more tools in their portfolio. 12% said they had 46 or more!

These arrangements are far too complex and require excessive human resources to manage, which is why 80% of organizations are interested in a vendor-consolidation strategy. Large security vendors are responding with more integrated products, but these projects are still developing and in some cases are operating on a timeline of years.

If you're going to transform your security approach into a consolidated, full-stack strategy—and present this plan of action to other stakeholders within your organization—it needs to be a question of months, not years.

The Superior Approach

The good news is that there's already a comprehensive solution on the market, and it will streamline your operations, lower your risk, build efficiency, and save you money.

With Edgescan's continuous security testing and exposure management SaaS platform, you get:

The Full Picture: Get a comprehensive view of your attack surface across all your web-facing assets, from applications to APIs to the host network and more. Map all your vulnerabilities and assess them with breadth and depth, regardless of where they might be lurking in your network infrastructure.

Validation: With a hybrid verification approach, automated assessments are backed by human expertise from dedicated penetration testers, so you can have full confidence that all the threats identified across every layer of your stack are real, free of false positives, and all in one place: the Edgescan dashboard.

Streamlined Operations: With point solutions targeting different layers, there will at times be multiple tickets with multiple vendors targeting one vulnerability. With a single solution, you get one alert in a single point of contact—the Edgescan dashboard—for a singular view.

Unified Strategy: With a single platform featuring risk-rated results, the security team can pinpoint the most critical threats across the whole stack for prioritized remediation and develop a holistic strategy for continuous risk management.

Compliance: Whatever your specific regulatory framework, it is likely to feature demands that span across the whole stack. It's about managing risk, regardless of where threats emerge. Why not use a single solution to ensure continuous compliance?

Cost: The overhead expenses with a siloed-layer approach have many layers themselves: setup costs, training to build your staff's skills to operate specialized tools, maintenance on multiple software sets, costs to build integration and communication between point solutions. Even if yours is a large organization that can afford to "manhandle" the integration problem to piece together a full-stack view of your risk—an option not available to small and midsize companies—why not put your money into setup, training, and maintenance on a singular, comprehensive solution?

Think Like an Invader

It has become the norm for many organizations' internal security teams to address each layer of the stack separately, shopping out specialized, point-scanning tools and building up staffing expertise to run each of these tools. This is known as a "best-of-breed" approach, but while the focus on each individual layer might be the norm, it has actually created a systemic problem.

Think about the attack surface of your web-facing assets like an attacker would. Bad actors are constantly scouring your entire stack, hunting a security gap or awaiting a lapse in judgment. The attacker is not fixated on one layer or another of your stack, be it an application or an API or your core network. They don't care about the individual layers, they have a composite view and simply want the easiest path with the least effort offering the highest chance to secure their goal. They scour the entire attack surface for the most critical vulnerabilities, anywhere there's a window to wedge open. Once they're inside, they seek to escalate privileges and maximize their penetration—and the havoc they can wreak—throughout your systems.

 |

The typical enterprise cybersecurity department has gone down the path of a siloed, individual-layer approach. That's become the industry standard by default based on how technologies have been developed and how markets have grown up around them. But there's no need to make the best of—or even double down on—a flawed approach by devoting more time and resources to those individual tools and building a system to share data and information between them.

Effective consolidation of disparate platforms could take years to implement, but there's a comprehensive, full-stack solution available to leave this paradigm behind. We don't have to allow history to define us, particularly when we know one thing for sure: Your attacker is hoping you do not go Full Stack.

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