

Why Does a Single Full Stack Vulnerability Management Solution Matter?

A Disturbing Thought

It is tempting, almost irresistible, not to think and align your Vulnerability Management (VM) efforts individually against each distinct layer of the full stack – network, applications etc. Indeed, It has almost become a bureaucratic, enterprise-norm for a Cyber Security leader to address each layer of the full stack and shop out specialized, point scanning tools and build up staffing expertise to run each of these tools. While this supposed “best-of-breed” individual layer-focused approach might be the norm – it’s actually creating a systemic problem.

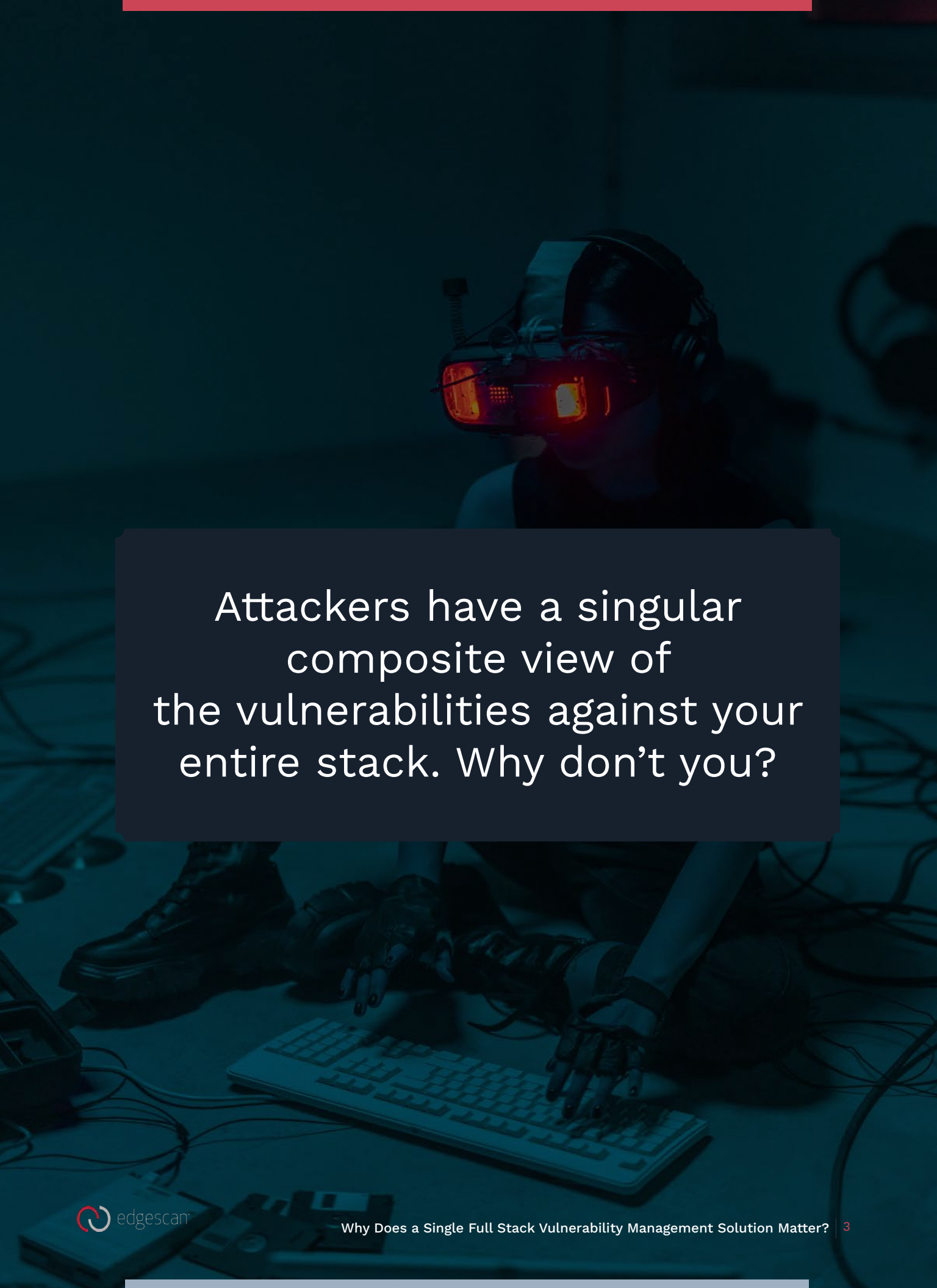
Attackers Have a Composite Full Stack View

If one thinks about their organization’s full stack attack surface like an attacker – a hunter constantly in search for a gap or a lapse in judgement - one might change their view about how they manage their full stack – they might even change how they view the full stack. Like the proverbial jail break - where the prisoner is looking for that precious twenty seconds of opportunity - they do not care where it is – it could be a simple logistical or structural gap – a mismanaged delivery van, a changing of the guard delay, a camera not correctly pointed – the cyber attacker too simply does not care about the individual full stack layers themselves. They have a composite view and simply want the easiest path with the least effort offering the highest chance to secure their goal.

That Raises the Question

If the attacker has a singular, holistic view of your full stack, then why would one not level the playing field and start your entire Vulnerability Management (VM) approach with a single, full stack VM solution approach itself? In this paper we will consider ten reasons why single, full stack matters but first lets agree on what actually full stack means.





Attackers have a singular
composite view of
the vulnerabilities against your
entire stack. Why don't you?

Take a Step Back – What Exactly is Full Stack?

Full stack parlance is quite common in IT and software development circles – having the credentials of a “full stack” developer commands attention as they are seen as more robust and useful if they can develop through the entire stack. But in the context of Vulnerability Management (VM) – what exactly constitutes a “full stack”?

The Vulnerability Management Full Stack Layers

1. Web application layer (layer 7) (including API's, Website, Mobile)
2. Hosting Environment layer (Web Application Server)
3. Operating System of the Host
4. Host Machine Services (Network Protocol and Services and Ports)
5. Underlying Network (Associated Devices including IOT, Firewalls, Router)

While there are several, nuanced layers within a Full Stack, it does not mean you cannot have a Singular, Composite View of Your Security Posture

Why is the Industry Rife with Point Solutions?

It seems almost obvious that a singular, composite view is superior to a layered approach – so one has to ask – Why is the industry proliferated with the point solution approach?

How Did We Get Here?

The most straight-forward explanation is simply the fact that the underlying technology itself developed in a piecemeal fashion. The specialized tools and expertise organically reflects the history of technology development from IT to the network, to web application layer to API's and IOT devices. Attacking itself, predates IT and internet – there were “telephone hacks” for example before IT and web surfaced. And as the attacker developed approaches to leverage access points in each new wave of technology development cycle, so too, the Cyber Security Suppliers would develop a specialized tool for that new layer of concern.

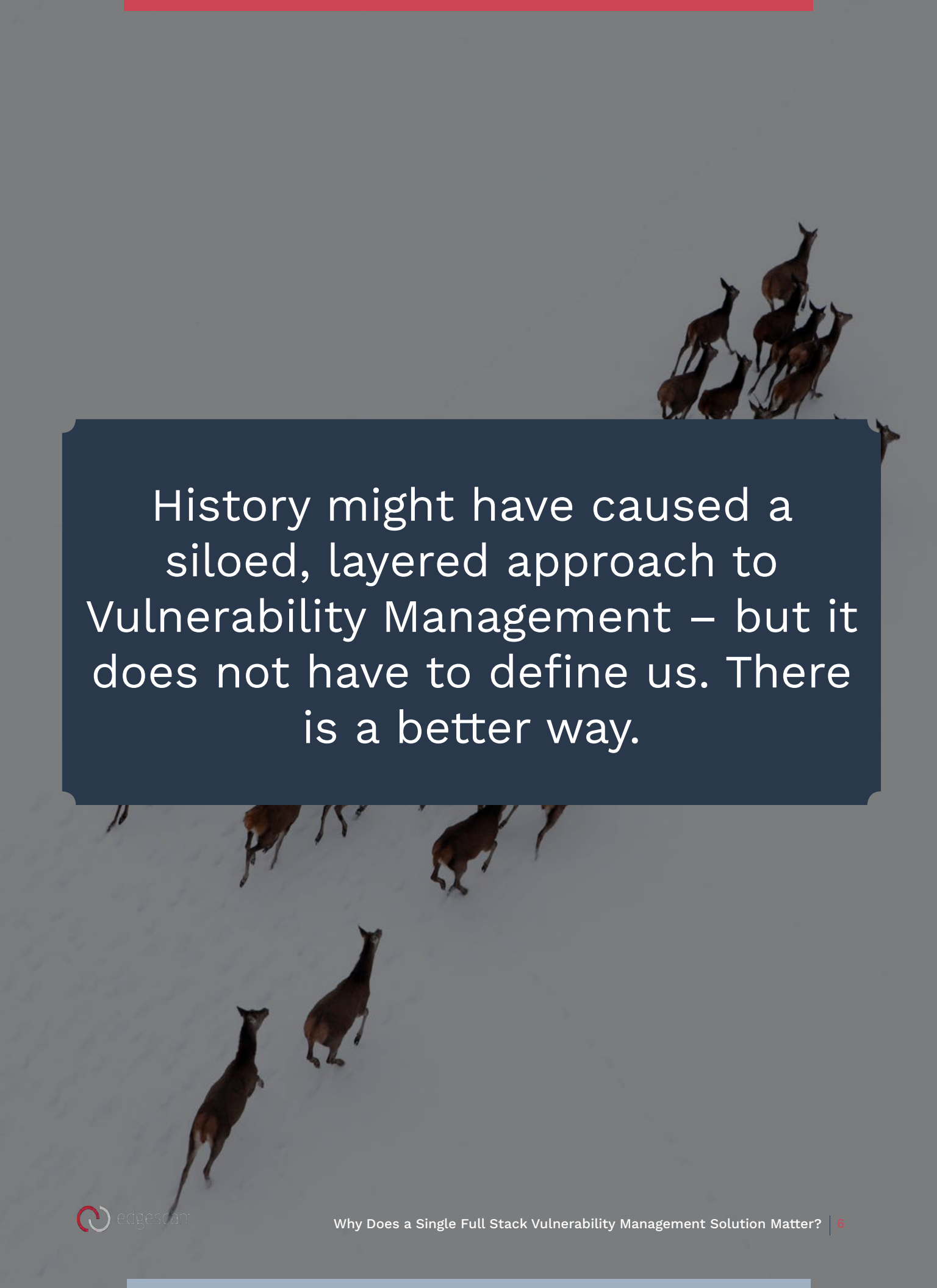
And the Marketplace Itself Embraced Point Solutions

And so of course once each layer-focused tool-set matures, then the analysts and the supplier marketing departs position and rank each of these tools within the scope of the layer. So the Vulnerability Management (VM) buyer is already operating within the paradigm of individual layers – the question was (and still currently is for the industry) what tools is best for each layer? While the more important question should have been (and should be today), how can I arrive at the same composite view as the attacker? How can I have a solution that accurately detects vulnerabilities and weakness that matter to our organization regardless of where in the full stack it occurs?

So Does History Define Our Vulnerability Management (VM) Approach?

Now here is the rub – if the typical Enterprise Cyber Security Department has gone the path of individual layer-approach like the rest of the industry – does one simply have to make the best of a flawed approach by simply focusing on the individual tools and manually getting them to talk to each other? The answer is no – there are Single Full Stack Solutions available to correct our course of action. But first let's just remind ourselves how bad the problem actually is.





History might have caused a siloed, layered approach to Vulnerability Management – but it does not have to define us. There is a better way.

How Bad is the Problem?

While it might seem elegant to advocate for a single, full stack solution – does the industry reality really reflect the fact that we have built up an unwieldy plethora of point solutions dedicated to its own stack layer? Is the CISO officer loaded with an unmanageable amount of point solution tools? The answer is – It's probably worse than you imagined.

Houston We Have Proliferation Problem


Here are some interesting highlights from Gartner's Top Security and Risk Trends for 2021:

- 1. Security Leaders have Too Many Tools** – What's the number? – SIXTEEN. Yes sixteen or more tools in their portfolio! And 12% have 46 or more!
- 2. So What's the Problem with Proliferation?** – Security Ops has become too complex and too much headcount required to manage it all.
- 3. How Many Enterprises Recognize the Need for a Fix** – 80% of organizations are interested in a vendor consolidation strategy!
- 4. Solution Provider Response** – Large security vendors are responding with better integrated products – but who is the leader in full stack single solution?
- 5. Correcting History is Not Easy** – Consolidation apparently is not easy – on average it takes YEARS to roll out.
- 6. Surprising Conclusion** – Lower Cost, Better Results – while Cost Reduction might initially be the driver – consolidation actually delivers both streamlined operations and lower risk.

Takeaway

It is a problem. It's a big problem. And the industry wants to fix the problem. But before we consider solutions to the problem, let's take a deeper dive why having a Single, Full Stack VM Solution really matters.





“The reality of security today is that security leaders have too many tools.”

(Gartner Top Security and Risk Trends for 2021)

THE LIST – Why a Single Full Stack Vulnerability Management Matters

Well we have seen at a fundamental level – the attacker does not care – they themselves have a holistic and singular view of your attack surfaces. And we have also seen that the Enterprise Security Department is suffering from a siloed, individual point approach to each layer of the full stack. Now lets remind ourselves why the Single Full Stack solution is the superior approach – here are ten of them:

Benefit #1 – Consolidated View of Risk

Full picture of individual assets, consolidation of risk data and a consolidated view of risk.

Benefit #2 – Full Picture of Assets

A composite view requires a composite solution.

Benefit #3 – Comprehensive Protection

if you have a full stack to protect, then you need a full stack solution. Again the attacker does not care what layer they attack – they just want a window of opportunity anywhere

Benefit #4 – Alignment Against What Matters

it is all about software in the final analysis. Validating each alert with world-class experts integrated with a single full stack platform instead of attempting to upskill internal resources to run each specialized tool will ensure you are aligned to act only what matters.

Benefit #5 – Compliance

One needs a full stack assessment. Compliance looks at risk regardless of where it is. Does your tool do that?

THE LIST – Why a Single Full Stack Vulnerability Management Matters

Benefit #6 – Overhead

The overhead costs for siloed, individual layer approach are layered themselves – set up costs, specialize tool skills overhead, maintenance overhead, integration overhead all compound with point solutions. Building a road is only the first cost, road maintenance cost over time is commonly overlooked.

Benefit #7 – Efficiency Means Resilience

A single contained (pre-packaged) solution means that all the same data for the same service is validated in a single place.

Benefit #8 – Costs

Some large enterprises “manhandle” the integration problem to achieve a full stack risk view – but many mid-sized organizations cannot simply afford that approach. And even for those that can – is that the wisest use of your security budget when single full stack solutions are available? And then there will still be the ongoing support costs for a manual integration approach.

Benefit #9 – Operational Headache

With layered, point solutions there will be multiple tickets with multiple vendors over one vulnerability, as opposed to a single solution that can port metadata over simply for a singular view of risk. And there is only one single point of contact for all alerts regardless of issue layer location.

Benefit #10 – Strategic Alignment

If one has a single platform that from the outset they can dictate strategically what level of service against what level of risk is optimal across the entire stack – is that not in one’s strategic interest to simply make it so?



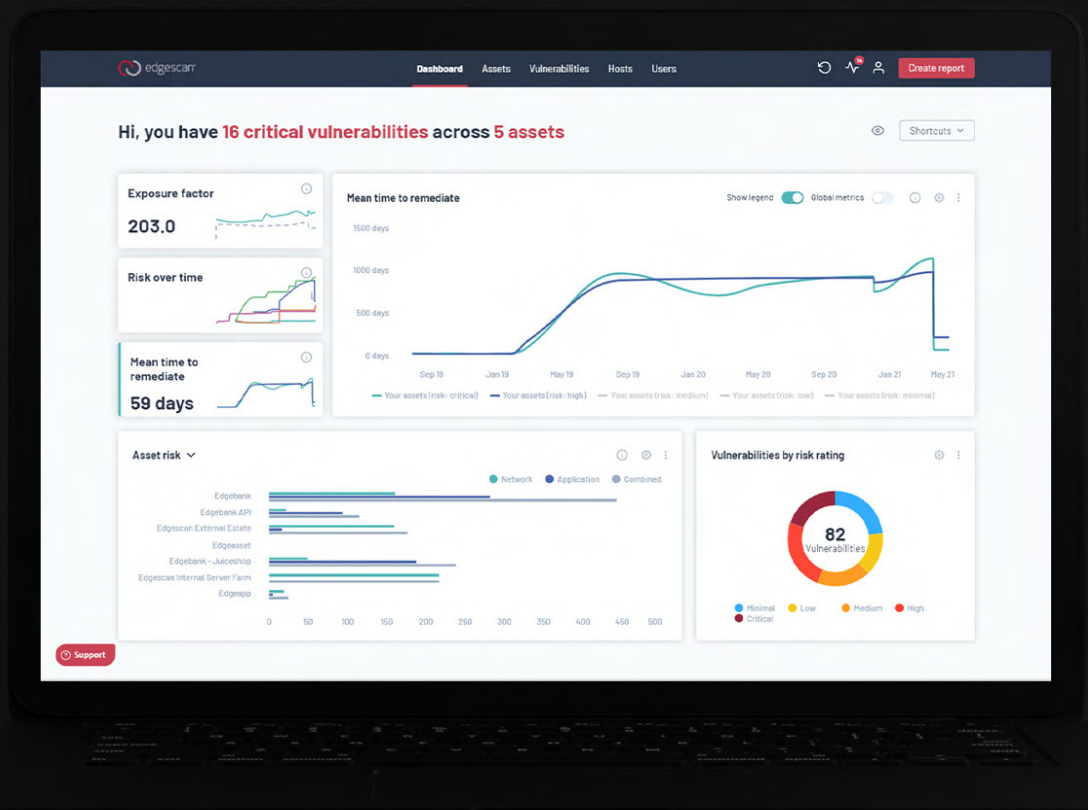
A Singular Full Stack VM Solution Yields a Plurality of Benefits

State of The Industry – Does Single Full Stack VM Exist?

While Gartner suggests that big security suppliers are starting to consolidate, they also suggest that historically, it takes years for Enterprises to consolidate (Gartner Top Security and Risk Trends for 2021). Well of course, if the approach to achieve a composite view of risk against the full stack is only to remove some of the point tools and perhaps manually integrate these disparate, siloed tools to achieve a singular view – its makes sense that it would take years to consolidate. But if you jettisoned the siloed, layer approach altogether – what if you took a Single Full Stack platform as your only solution? What are you options – if any?

Edgescan in 2021 is the Only Full Stack Vulnerability Management Solution

As far as truly Single Full Stack VM solution's go – only Edgescan currently in 2021 can truly offer that approach. Their platform is not only full stack, but it also comes fully integrated with expert pen testers and analysts to ensure accuracy across the stack by removing false positives. And it also offers automated integration to presents its single composite risk view to operational and support staff, so ranked business intelligence and relevant vulnerability remediation guidance is incorporated into daily operational workflow. While its sobering to think that in 2021 there is only one Enterprise-ready single, full stack platform available – it is still refreshing to think at least supplier has made the paradigm-shift to Single Full Stack.



Hi, you have **16 critical vulnerabilities** across **5 assets**

Exposure factor

203.0



Mean time to remediate

1500 days

1000 days

500 days

Adopting a True Single Full Stack VM Platform is key to achieving consolidation in months as opposed to years.

Asset risk



Putting Single Full Stack Into Action – Some Practical Suggestions

So you are about to make the jump to single, full stack – we have given you ten reasons why it does truly matter. Now here are some practical tips on things to consider as you embark on your new course of unified risk nirvana.

Be Smart About Full Stack Solution Pilots

Do not cherry pick one layer from a Single Full Stack Solution Vendor – that misses the point. Instead pilot in with a singular, full stack solution – but perhaps scope the pilot in at one business division or one geography to truly come to terms with the ten benefits we listed above.


Leverage Your New Enlightened View of Risk

Risk is not linear – how one communicates risk is traditionally challenging. One thousand issues with a score of 1 (say out of a 1-100 score) yields a risk score of a 1000 as opposed to one issue ranked at 98. But it's that one 98-ranked issue that's going to have significant impact on your business. With your new composite view of risk you can build your platform to alert you on say a significant business concern like the 98 score vulnerability. Basically with a full stack single solution you can build alerts out exactly regardless of layer to signal what matters the most. And that's the whole point of the approach – to gain that holistic view.

Correlations are Key

Remember – you now have a pre-packaged singular solution. No more manual attempts at leaking vulnerability source data from layer to layer. So things like correlating a network with web application issues are now easily attainable. It's much more intuitive with a combined view of risk against full stack. Indeed your composite correlation-detecting view, puts you on a level playing field (if not superior position) than your attacker.





With power comes responsibility. Leverage all the value of your new Single Full Stack VM Platform.

Full Circle – Questions for You

So we circle back to our would-be attacker from the beginning of our paper – shall we allow them to dance? Shall we allow them to leverage the fact that you have a cacophony of point solutions – ever in need of overhead management and insight integration? Or shall we take the stance of the attacker? Shall we not concern ourselves about the individual layers and associated point tools but instead respond to a composite ranked risk view of the entire stack and accurately and quickly respond where it matters regardless of the layer? Is this not Smart Vulnerability Management?

Your attacker is hoping you do not go Single Full Stack.