Can You have a Single Touchstone of Truth for Your Vulnerability Management Program? (And Is it Worth It?)

edgescan™

The Proverbial Single Touchstone of Truth – Is It relevant for Vulnerability Management?

Every Business Wants a Single Touchstone of Truth, Right?

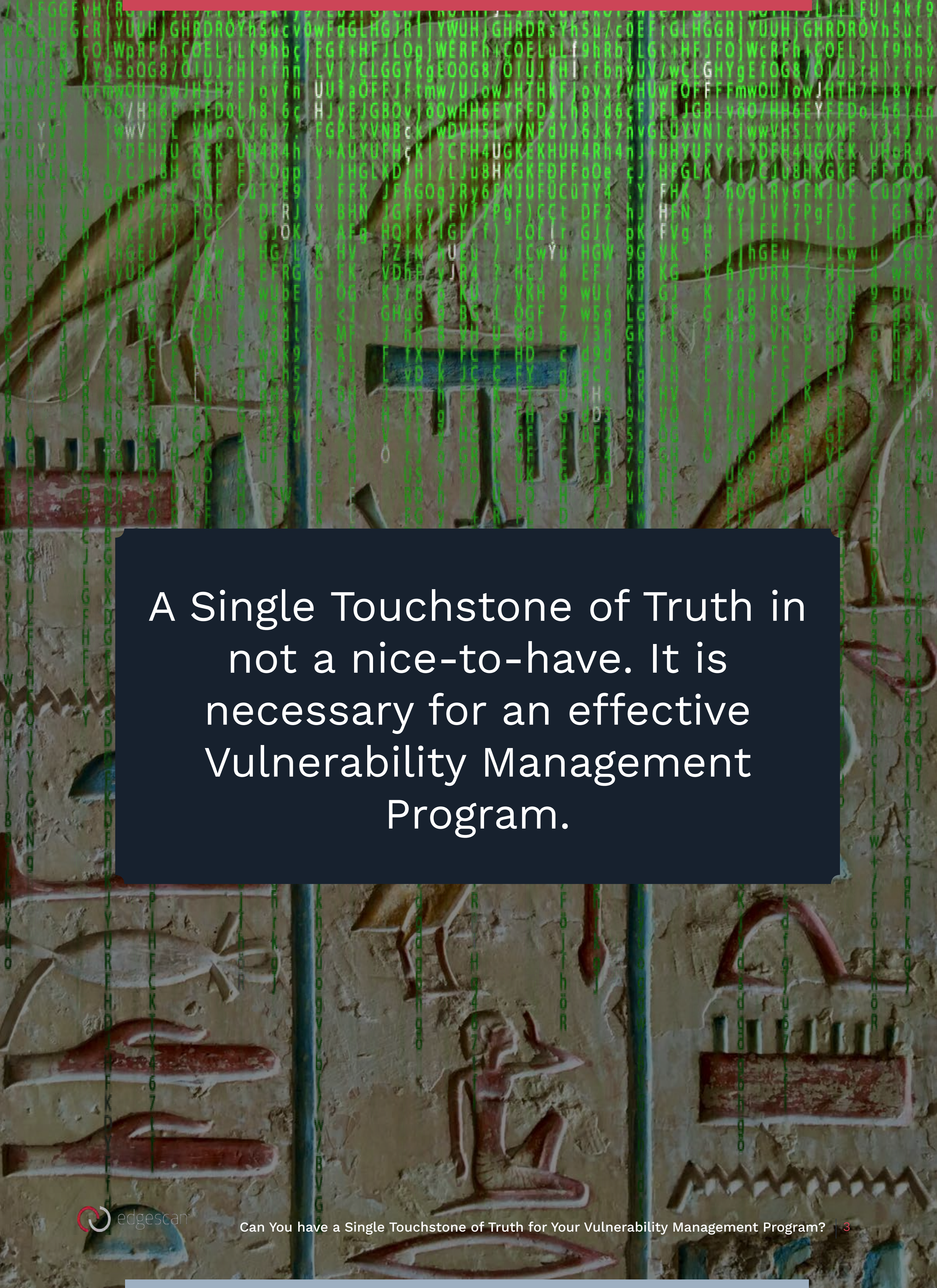
It is not uncommon for every corporate business leader – the captains of their enterprise ship – to have a very visceral desire for the grand master dashboard to guide the enterprise. A single touchstone of truth providing them with every nuanced piece of data to make those "tough" decisions to direct their hands on their large, strategic business levers. And since the 1980's, the enterprise software and business intelligence (BI) suppliers have aggressively ramped up to deliver a wide array of analytics reporting engines tied to every aspect of the business – sales and marketing performance metrics, financial P&L, delivery metrics, supply chain and inventory live real-time status, staffing alignment metrics, social media sentiment about their corporate reputation, marketplace trends and stock market analysis. The business leaders want anything that's tied to measurable, bottom-line performance integrated and normalized on one dashboard – one touchstone of truth.

But Why is this Relevant for a Vulnerability Management Program?

While the Cyber Security Leader may not be tasked with decisions on sales metrics and supply chain inventory levels – there is an equally varied layer of incoming intelligence data that they need to have a holistic view of their cyber risk. The layers for Vulnerability Management Program are not business performance layers – they are the layers of the attack surfaces themselves.

A Single Touchstone of Truth is VERY relevant to run an Effective Vulnerability Management

While a traditional business-process consolidated dashboard for Enterprise Resource Planning (ERP) offers the convenience of getting the big picture to make it easier to make the proverbial big business decisions - getting to a single touchstone of truth for the Cyber Security leader could be the difference between continued operations and a cataclysmic security incident that the world may reading about on the front page news. Make no mistake about it – attackers simply do not care what layer they use to achieve their goals against their target organization. Winning the prize, is winning the prize no matter what point of entry. Without a holistic view – without a single touchstone of truth – there can be dire consequences. Before we explain how to solve this problem, let's take a step back and see how we got here.



A Single Touchstone of Truth in not a nice-to-have. It is necessary for an effective Vulnerability Management Program.

So why Doesn’t Everyone Already Have a Single Touchstone of Truth? – Some Background

A Byproduct of a Fragmented History

By and large the siloed approach with cyber security tools and services that focus on single layers of the IT stack are simply the byproduct of the evolution of the IT stack itself. The network security focus was a precursor to the web application layer focus which then splits to API’s and IOT devices and so on. Ultimately as the IT stack layers evolved, then so too the security products aligned against those siloed layers developed as well. And so we get the so-called best-of-breed tools and services focused on each individual layer of the stack - the network, for web applications, for mobile, for IOT, for API’s and also for Attack Surface Management (ASM) and also for penetration testing.

Marketing and Industry Analysts Did and Do Not Help the Situation

And almost to solidify a fragmented and siloed approach – marketing teams would position their single layer solution as “the best” within their focused IT layer and the industry analysts would rank them within these layered categories. And eventually the Enterprise Cyber Security Leader would be tasked with onboarding the slew of best of breed tools and service for respective IT layer.

And the Result? – A Heap of Problems

Well one can guess the result – no single touchstone of truth. And if one wanted to manually take on the massive task of integrating the different layered solutions from different suppliers to one normalized dashboard – it would take a herculean effort. And aside from the mammoth costs and time to do so – the typical Enterprise Cyber Security team for the last decade has been faced with huge cyber security staffing issues to shoulder this effort. And the setup while daunting, hides the even more challenging operational challenge – how to manage the upkeep of a unified dashboard with ever evolving tools from ever evolving suppliers. A Vulnerability Management team is supposed to manage vulnerabilities – that’s the day job – not be an ongoing infrastructure works project team.

The fragmented and siloed approach to security tools is largely a byproduct of the evolution of the IT stack itself.

Sounds like a lot of work – Is it Worth It?

Given we can thank the fragmented evolution and history of the IT stack itself for our fragmented, siloed point solutions for Vulnerability Management – perhaps before we even consider approaches and solutions to correct the situation – we should ask - Is it worth the effort?

Answer – A Big YES

For the remainder of this paper we will consider five significant benefits to enabling your Vulnerability Management Program with a single touchstone of truth. But before we flesh out those details – lets remind ourselves of what one would think in the Cyber Security industry is obvious. Its certainly obvious to the would-be attacker.

The Attacker's Point of View

The attacker's preference is certainly for you to have a fragmented approach. They do not have prejudices against any layers of the attack surface. And if they can exploit one vulnerability on one layer to segue into an expanded opportunity within another layer (e.g. now that the corporate system sees me as an employee, let's see where else I can explore ...). They certainly do not want you to have a real-time holistic view on your unified dashboard where you can immediately detect correlations between the layers that automatically kick off alerts to shut down their access. And they certainly hope with your plethora of tools and upkeep routines, that you simply drop your guard on one them and they can get easy access. For the attacker – your multiple tool overhead and siloed focus on each layer and alerts is an opportunity to exploit a timely attack surface exposure.

Five Reasons for a Single Touchstone of Truth

So to sum up – it's just bad. Full stop. You are unnecessarily handicapping yourself against a would-be hacker. Now let's take a look at the five biggest reasons to get onboard with a single unified dashboard across the entire IT stack. And then we will consider how to go about efficiently onboarding a single touchstone of truth for your organization.

Shall we let history define our Vulnerability Program approach or should we reconsider our position?

Benefit #1 – Resilience

The most important reason one would want a single touchstone of truth is that it makes their organization more resilient to attacks. And it's not just a matter of more sophisticated detection tools themselves – it's that if you have a single, unified view across the entire stack, then you can notice patterns that a set of points solutions simply will not pick up.

Staged Attacks Require a Holistic View

Quite often a successful attack requires exploiting multiple, staged weakness across the stack. It could initially say start as a web application vulnerability – perhaps a weakness that allows the attacker to bypass authentication. Once inside, the attacker can now turn to exploiting weakness within the network and so on.

Red Teaming Concerns

With Red Teaming – the attackers do not simply look at one layer – say the web layer – they wreak havoc wherever they can get. It's hard to keep up with a red teaming approach. It is hard because the Red Teaming approach takes a holistic view of your entire enterprise. That's exactly why one needs a composite view of the truth – to detect and anticipate the same creative ways the hacker stages their attacks across your attack surface layers.

False Confidence

And to make matters worse if you have some degree of sophisticated detection tools dedicated to each layer and they are individually not concluding any concerns – they are not picking up on the cross stack patterns - then you are operating with a false sense of security. You are not making the right proactive steps while you are complacent with what the point solutions are reporting.

Managing Risk

Risk, put simply, is the chance of something bad happening. To determine overall cyber risk for an enterprise - it's not sufficient to look at your traditional siloes of individual stack intelligence and then deduce the organization as a whole is not at risk. A robust, holistic view of overall risk means you have an accurate single picture across your entire stack.

Why would you handicap yourself against an attacker with a fragmented view of cyber risk?

Benefit #2 – Strategic Alignment

For any large enterprise, the CISO needs to answer one basic question - Is the corporation as a whole resilient against cyber-attacks? Will the executive management team and board be able to achieve their strategic goals or not? Just like the attacker, business management are not really interested about the details of any particular IT layer or a particular detection tool aimed at mobile or IOT device. The question at hand is much more straightforward than that - When you look holistically across the entire layers of attack surface is there a viable opportunity for an attacker to stage an attack or series of attacks and cause damage to the company? And if one does have a single touchstone of truth – then how does the CISO accurately answer that question?

Reverse Engineering

But if one DOES have a single touchstone of truth then one gets an unadulterated presentation of reality – the good, bad and the ugly. Now when the CISO has a seat at the strategy table, they can actually use their unified dashboard to show potential problems. They can promise that unless they take proactive specific steps, then certain strategic business goals will be in jeopardy. Conversely, they can also leverage a unified view of risk to assure them that from a Vulnerability Management perspective, their strategic goals are indeed attainable.

Vulnerability Management as a Corporate Differentiator

Now that major corporate cyber security incidents are daily front page news – the public (and stock market's) perception of a corporation can be tied to their sense of how secure they actually are. Proactive Smart Vulnerability Program advancements and the empirical verification of resilience via a single dashboard of truth can effectively be an important component of the corporate strategic go-to-market strategy. A fragmented, siloed approach to the security layer stack will make that unified dashboard difficult to become part of the overall strategy.

Only cyber security leaders with a single touchtone of truth get a seat at the strategy table.

Benefit #3 – Costs and Time

As any engineer will attest – one can build out practically anything if they have enough money and time. So why not just take all the point solutions for each stack layer and engineer out a unified dashboard with contextualized detection engines supplied with a master alert bus and normalized dashboard? Unfortunately as we all know the hard reality of any enterprise is that there will always be a finite budget to run any program and that is certainly true for a Vulnerability Management Program. And as far as time goes – there is always the lurking danger of the ever-persistent 24x7x365 would-be attacker. The attacker is perfectly ok with you taking your time to right the ship. But the business leaders need to hit business goals every quarter. Time is not your friend.

Multiple Supplier Costs

As much as the procurement department negotiates each contract for each tool for each layer – the cumulative costs as a rule of thumb will always be larger than one contract for a composite solution for the entire stack.

Maintenance Costs

And the initial extra purchase and set up costs for multiple tools pales in comparison to the ongoing support costs. Now for every new tool update you have to manage multiple ongoing tool releases. By definition they will not be in sync as the suppliers are unique and potentially even competitors with each other. And if you are attempting to manually integrate the solutions with each other to approach a unified, composite view, then every update means a new QA cycle to determine and resolve any new update issues for every release for every point solution tool.

Herculean Integration Engineering Project

And the costs to set up automated integrations for every layer-specific tool is a huge project requiring specialized engineers over a significant period of time (i.e. multiple quarters, potentially years) which all translates to costs that typically fall outside of a Vulnerability Management team's budget.

Your Cyber Security Budget would be better purposed for staffing cyber experts than running tool maintenance programs.

Benefit #4 – Overhead Bandwidth

And even if one has unlimited budget and time to achieve an internal manual engineering effort - which we know is simply not the case for any enterprise – there is still the problem of who within your Cyber Security department is going to take this daunting task on?

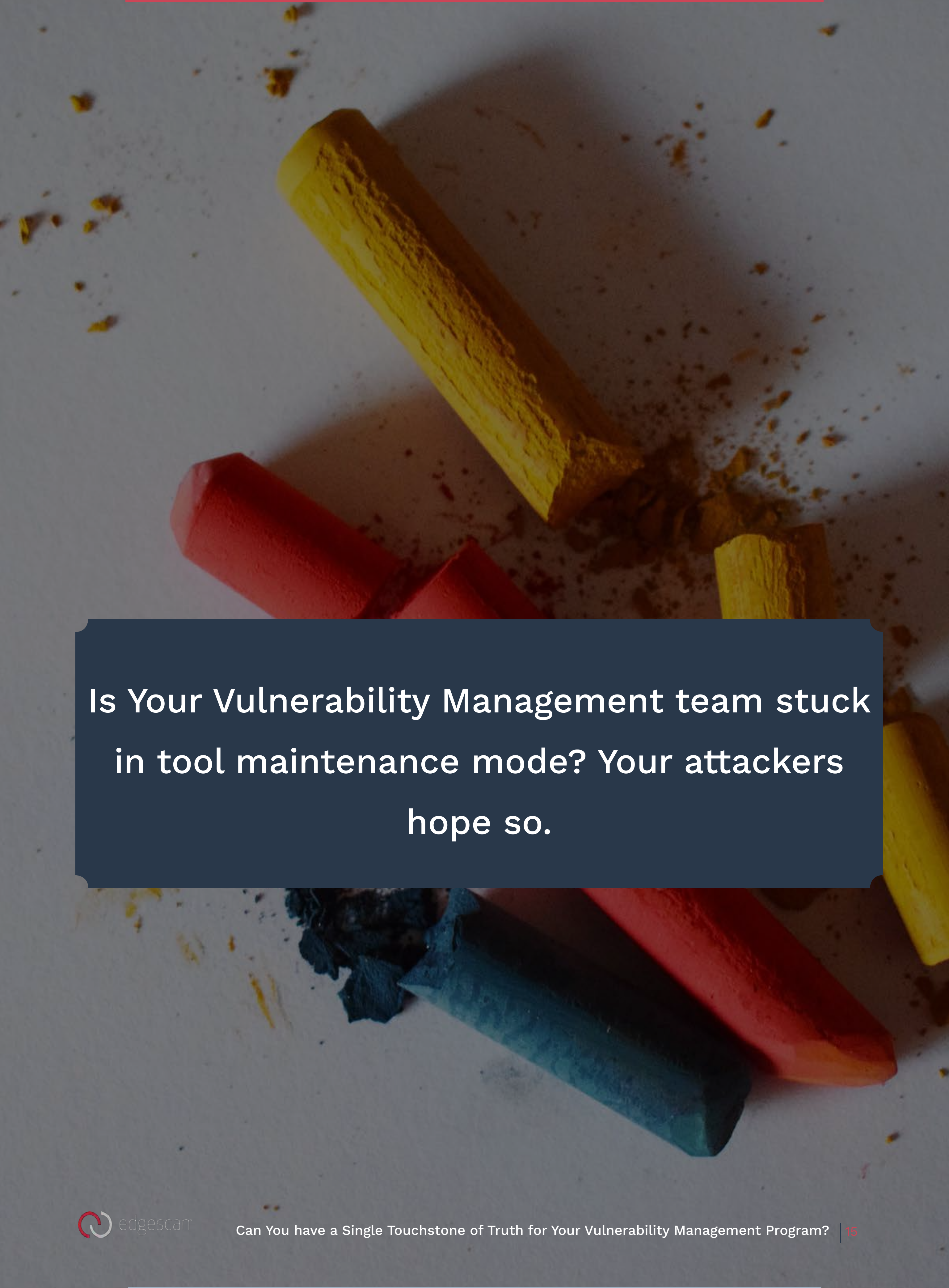
Enterprise Cyber Security Departments are Overloaded

It's almost like a bad joke to think that the typical enterprise cyber security team – the team that always seems to be behind in keeping up with the exponential rise and sophistication of global attackers – to add basically a new day job. This new day job of managing multiple tools requires the cyber staff to do a few things:

1. **Onboarding Point Solutions** – For the next few quarters, have your staff go out for bid and determine best-of-breed point solutions and then learn each of the tools and then integrate them into your program. And do that across your entire security stack.
2. **Integrate All of the Point Solutions** – We will now give the staff 12-18 months to home-grow an integration solution that takes each disparate tool and normalizes the data and present the relevant business alerts across the entire stack in a unified dashboard.
3. **Support the Complex Machine** – Now you have created your multi-headed monster, time now to dedicate
4. significant parts of your staff's week to rolling out individual tool updates, fixing issues that arise and re-engineer your home-grown integration solution as each tool release update upsets the apple cart.

Your HR Department will Love You

Your HR department has already made you keenly aware that staff morale is already at an all-time low – each staff has expressed in varying ways that they are overworked and yet still anxious that they do not have clarity on whether they are delivering resilience. Now the head of HR would like to have a one-on-one meeting with you. Only one topic in the agenda for that meeting – who authorized that all the cyber staff take on a new job handling multiple tool overhead?



Is Your Vulnerability Management team stuck in tool maintenance mode? Your attackers hope so.

Benefit #5 – Staffing Issues

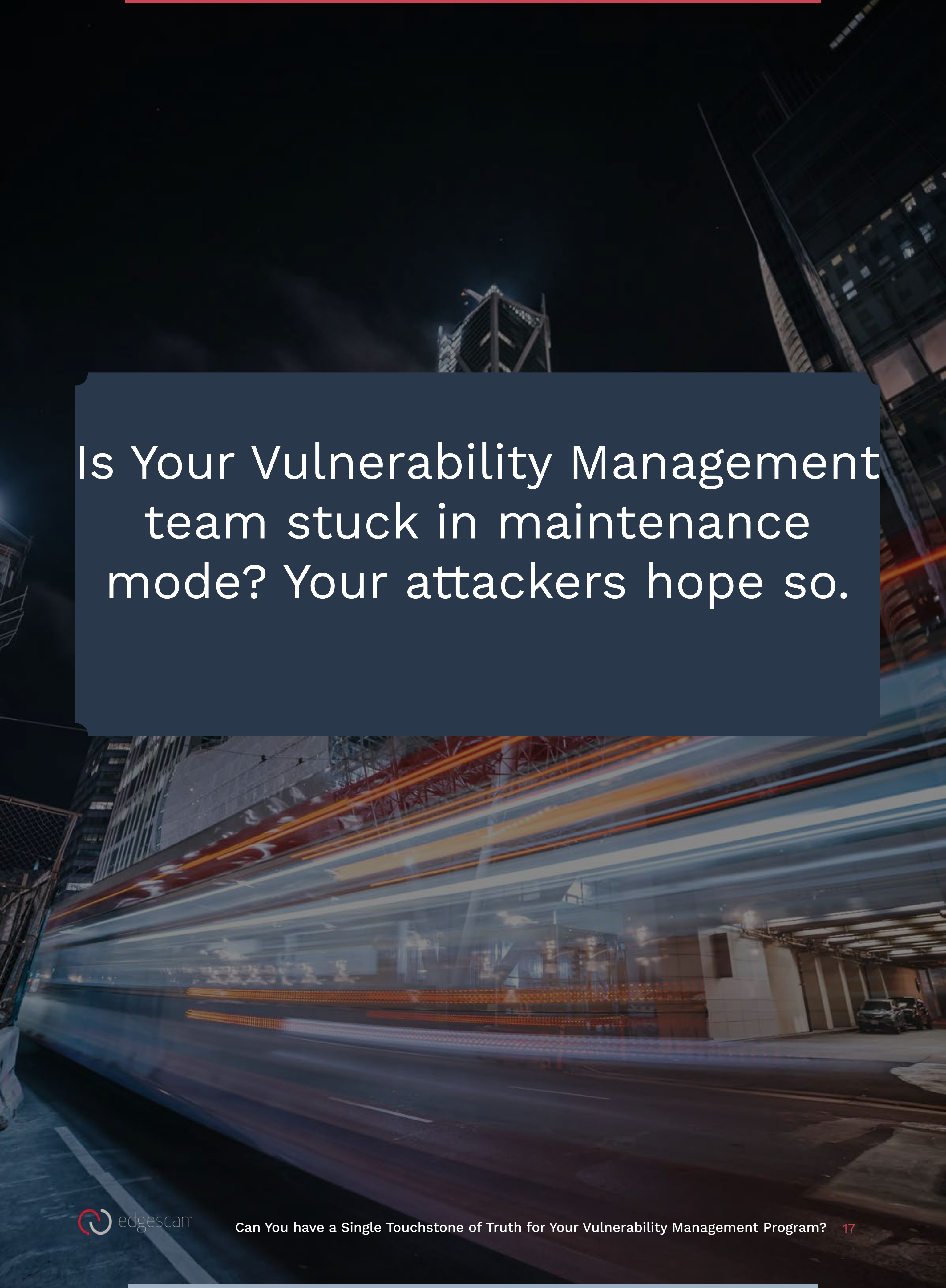
Well now we have seen how the extra bandwidth tied to the overhead of managing a host of tools for each security stack layer presents an operational problem, the problem gets even worse when thinking about the challenge in today's market to recruit cyber professionals.

Leveraging the Expertise of Your Cyber Security Staff

Back to the land of reality – with a limited budget and limited number of cyber security staff inhouse and the challenge of recruiting in general – the prudent thing for any Vulnerability Management Program leader is to determine how can they get the most value out of the expertise they have within their staff. And certainly one wants the experts doing "expert-things" – e.g. proactively determining if there any issues and proactively remedying any situation that arises. But putting them on the equivalent of a "city-works" project or rather, multiple ongoing city-works projects is certainly going to result in them taking their eye off their strategic responsibilities.

Attracting the Best and Brightest

Aside from salary and benefits packages – the real thing that gets a cyber professional excited about coming onboard is doing meaningful cyber security work – planning out the strategy and effectively in the day-to-day operations making meaningful steps to actually identify significant vulnerabilities and resolving them. They would like to actually become a hero for the company by avoiding becoming the next bad front page news incident. Managing the overhead and endless updates of a plethora of scanning tools and manually trying to come to terms with what is real and how it all ties together into one touchstone of truth is hardly the job that gets them out of bed in the morning. A single touchstone of truth will enable and inspire.



Is Your Vulnerability Management team stuck in maintenance mode? Your attackers hope so.

Is it Achievable?
Yes – the Edgescan Way

While the Vulnerability Management industry has mostly gone the path of individual point solutions with only alert dashboards specific to each focused security layer – there is one solution provider that has actually gone all in with a single touchstone of truth centric-approach. And that company is Edgescan.

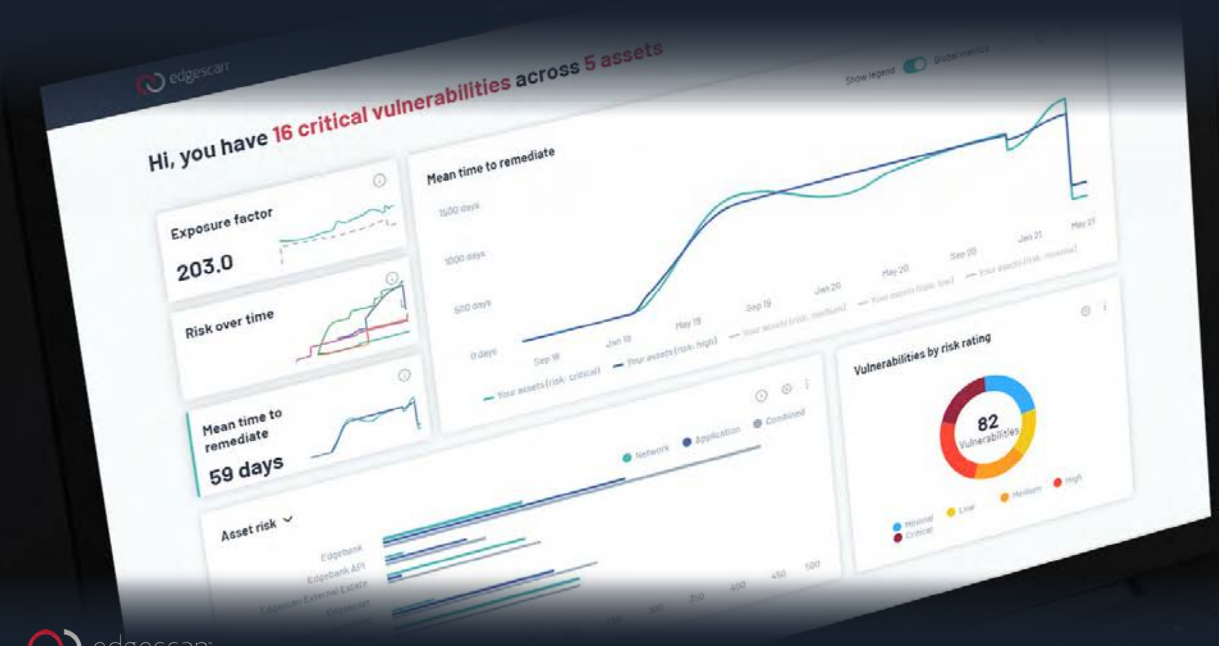
Tackling the Single Touchstone of Truth Problem Head-on

Back in 2014, Edgescan decided with the plethora of siloed, layer-focused detection tools available and yet no ability to have one composite view of the truth readily and easily available – they simply needed to start from scratch. They did not want to inherit the baggage of a siloed approach, so their proverbial insight was to create one single Vulnerability Management platform tied to one single source of truth across the entire stack.

It was a lot of work

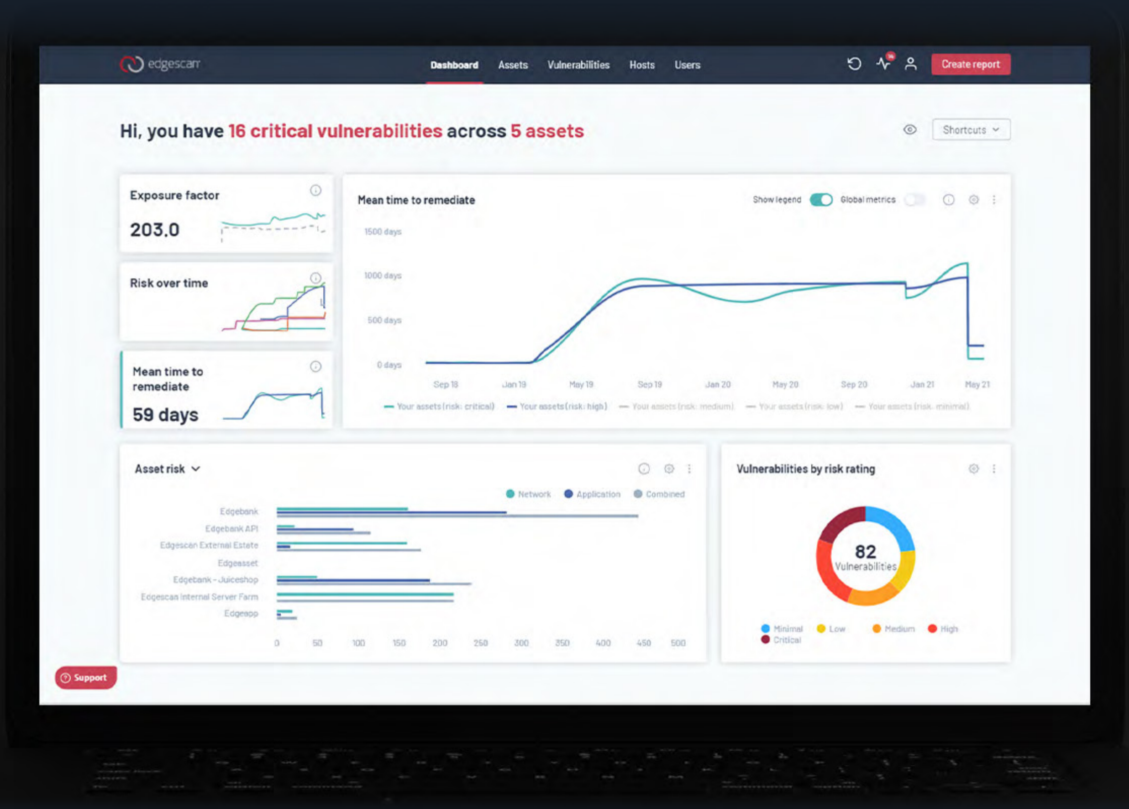
To achieve a complete holistic view of risk associated with verified vulnerabilities across the entire stack they needed to:

1. **Creating custom scanning engines** – To feed the single touchstone of truth with alerts across the stack, custom scanning engines has to be developed for each layer.
2. **Introduce robust Web Application, API and IOT scanning engines** - As the industry in general did not have a mature web application and API and IOT scanning engines – considerable development time had to occur to make these as robust as the more mature networking scanning tools
3. **Evolving Attack Surface** – from the outset it was realized that if one does have an accurate real-time picture of the attack service itself, then there would be no confidence in what the single touchstone of truth showed as alerts. So significant effort went into tools and approach to come to terms with accurate representation of the entire attack surface itself.
4. **Integration Penetration Testing Intelligence** – While penetration testing is more expensive and slower and less scalable than using automated tools, the benefits are game-changing – it simply detects more complex
5. business logics issues than scanning can – those insights also needed to be integrated into the entire picture of risk.


Hi, you have 16 critical vulnerabilities across 5 assets

Is it Achievable? Yes – the Edgescan Way

5. **Accuracy and Human Judgement Integration** - while scanning engines can scale they do produce noise – false positives – which make the dashboard less actionable – so again from the outset, Edgescan built the platform to integrate with their own world-class cyber security experts so the unified intelligence dashboard is accurate and offers human guidance on timely remediation.
6. **Create a Master Vulnerability Service Bus** – In order to present business-ranked intelligence across all of the above channels – a master bus needed to be developed - tying all the alert sources from each layer together into a single dashboard - a very massive engineering effort.
7. **Create a Normalized View** – Extensive UX and Data Visualization work went into presenting each of the alert feeds in a normalized view so the viewer can easily see where they need to take action regardless of attack surface location.
8. **Host the Platform so No Maintenance Overhead** – and finally to avoid the huge costs and bandwidth sucking activities we identified earlier – all the updates and maintenance is done by Edgescan in the background leaving the customer only to focus on acting on accurate, business ranked alerts across the entire enterprise and ensure their strategic goals are being achieved.



Hi, you have 16 critical vulnerabilities across 5 assets

Exposure factor 203.0

Risk over time

Mean time to remediate 59 days

While in 2021 the industry only offers pointed tools for each security layer, Edgescan has taken a decidedly different approach - One platform across the entire stack delivers one compete single touchstone of truth.

In Conclusion – Sometime the Easiest is the Best

We have seen how we arrived at the less than desirable siloed, IT stack layer-focused approach. And we have seen in detail the problems of this approach and the multiple layers of value in realizing an single touchstone of truth across the stack for your Vulnerability Program. And finally we have seen this is doable. The Edgescan Hybrid approach indeed provides exactly that.

A Happy Closing Note

And we will end with the irony that while the industry and enterprises themselves in 2021 still seem wrapped in the point solution approach and manually home-growing a burdensome and inaccurate single touchstone of truth – it's refreshing, yet ironic that the solution to deliver an accurate and composite single touchstone of truth is actually the easiest one to take on. Sometimes you can have your cake and eat it too.

In 2021, every enterprise can enjoy the benefits of a single source of truth for their Vulnerability Management Program