

Security Tool Proliferation and Vendor Consolidation



Security Tool Proliferation – The Numbers

It might seem surprising that amongst all the pressing challenge for an Enterprise Security leader – the type of stuff that could potentially be global headline news – that 80% of organizations are interested in of all things - a vendor consolidation strategy! In fact, vendor consolidation is ranked number three as one of the Gartner Top Security and Risk Trends for 2021.

We Have a Proliferation Problem

And if we take a deep dive at the actual number of security tools in play for the average enterprise, its quickly becomes less surprising that vendor consolidation is top of mind. Here are the highlights of the recently published Gartner Top Security and Risk Trends for 2021:

- 1. Security Leaders have too many tools** – What's the number? – 78% of CISO's have sixteen, yes sixteen or more tools in their portfolio! – and 12% have 46 or more!
- 2. What is the problem with tool proliferation?** - Security Operations has become too complex and there is too much headcount to manage it all.
- 3. Who's onboard with Vendor Consolidation as a Strategy?** - 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 integrated single solution?
- 5. It is not an easy problem to solve** - 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 ops and lower security risk.





“The reality of security today is that security leaders have too many tools.”
(Gartner Top Security and Risk Trends for 2021)

How did it get so messy?

No conspiracy theories here – the sheer number of different tools for each attack surface layer is really simply a by-product of the organic evolution of the IT stack itself. With the arrival of new technologies and the recent digital and cloud transformational movements – the Cyber Security tool industry responded in kind by fine-tuning individual point solutions for each specialized layer. And of course, with the emergence of new technologies, then the enterprise purchases specific tools which in turn means that one has to staff with experts against the variety of newly acquired tools.

Considerable Variety in Attack Surface Layers

When one considers how different each layer is, it becomes easier to see how a point solution approach emerged.

Distinctive Layer Features

As an example the security layer could be at the Code Level. So one needs to conduct Source Code Analysis (SCA). Here one is trying to determine if there are any mistakes that could lead to a security vulnerability. This is inherently a static analysis. But then contrast static SCA with Penetration Testing (Pen Test). Here one tests a running system – a dynamic analysis – where one actually tries to achieve success against vulnerabilities. And when one focuses on threat detection and prevention, one now is actively trying to detect malice. And then when one is analyzing protective measures – firewalls for example – one is concerned that the perimeter is secure. Not only are the tools each different – the approach (e.g. static vs dynamic) has to be different.

Vulnerability Management Programs Have Traditionally a Wide Set of Tools

And even if one were to focus solely on their Vulnerability Management (VM) Program, it is easy to see how even automated scanning takes on a different dimension when applied say to automated scanning for vulnerabilities with IOT, API's, Web applications and the Network. And of course the pen tester will use different tools to aid running tests on running systems aided the human dimension of interpretation and trying to break the logic of the system (just like a hacker does). It is clear that Vulnerability Management even if just focused on the IT stack is prone to tool proliferation.





“Too many security vendors results in complex security operations and increased security headcount.”
(Gartner Top Security and Risk Trends for 2021)

The Obvious Benefit from Vendor Consolidation – Lower Cost

When talking about lowering cost with vendor consolidation, one does not even have to focus in on Cyber Security tool suppliers – any Enterprise procurement department will confirm that supplier consolidation in general lowers costs due to several factors:

- 1. Vendor Management** – Lower overhead to manage contracts
- 2. Operations Management** – Lower overhead to manage multiple suppliers
- 3. Volume Discount** – Better chance to lower overall cost by aggregating tiered volume discounts across multiple vendor solutions
- 4. Legal and Procurement Costs** – Less legal and procurement staff to oversee less amount of suppliers
- 5. Favorable Terms** – Better chances of getting favorable terms and VIP treatment with a larger contract with fewer suppliers

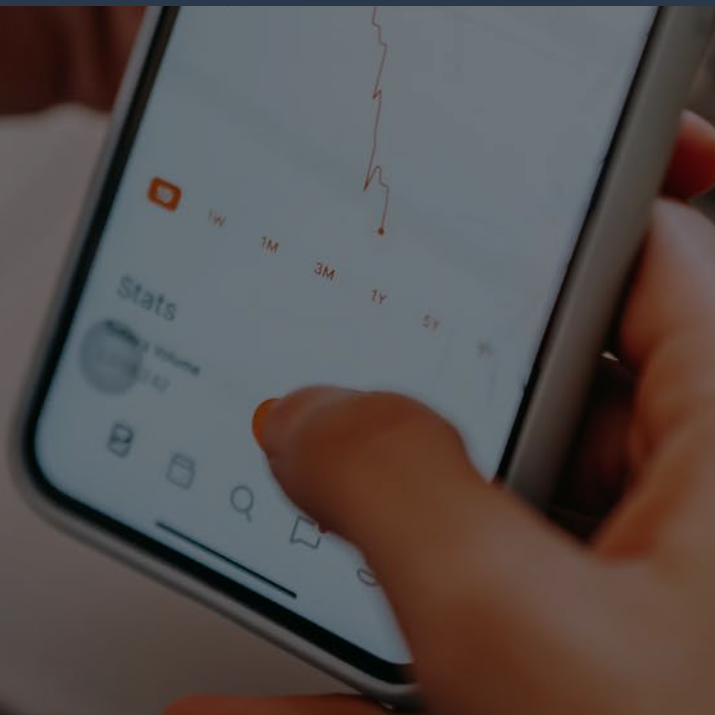
Security Tool Proliferation Presents Layers of Costs

But security tools present further layers of costs reduction including:

- 1. Maintenance** – Maintaining multiple security tools from Network to Web Applications to API and ASM is a lot of work.
- 2. Product Roll Outs** – Orchestrating new product versions for each specialized tool and making sure that alerts and reporting continue to function correctly against each individual tool release again is a lot of work.
- 3. Compiling Insight** – It is easy to forget that the multiple-point solution approach inherently means one has more complex, siloed data sources underneath the tools – all of which requires more work to compile to accurately determine risk.
- 4. Staffing** – Even ignoring the challenges to recruit specialized security engineers – the staffing costs to oversee the multiple security tools is significant
- 5. Burnout** – the blocking and tackling of running multiple security tools and chasing siloed data sources is simply fatiguing and results in security staff increased churn rate and increasing recruiting costs.



**“Most organizations recognize vendor consolidation as an avenue for reduced costs.”
(Gartner Top Security and Risk Trends for 2021)]**



The Deeper, Less Obvious (and more Important) Benefit from Vendor Consolidation – Improved

Typically as one tries to simplify and lower costs, there are inherent trade-offs with performance. In this case, even if one was only to be concerned with security robustness and even if one would allow more budget – the very act of reducing security tools in a smart way, will pay dividends in lowering one's overall risk posture.

Lower Costs, Simpler Solution and Better Security – How could that be?

Tool proliferation and more importantly the siloed and complex data sources that underlie separate point security tools is a serious matter. The actual variety of tools might force one to separate data making the whole process of an integrated, single touchstone of truth that much harder.

Complexity is the Enemy of Security

If 78% of enterprises have 16 or more tools and 12% have 46 or more different tools then the average enterprise is forced to manage the complexity with a sheer brute force of individual staff expertise. But aside from costs, one simply cannot realistically expect everyone to be skilled at everything. And the result is you increase your chances of missing important things.

Eyes Off the Prize - Giving the Attacker an Unfair Advantage

The attacker hopes that the tool proliferation and overhead management does in fact take the CISO's eyes off of a critical matter. It's not a fair competition - the attacker in this game only needs one avenue at any one given more moment to win the prize. The attacker runs a very lean and focused operation. But the CISO function must be on everywhere and at all times. So why, given the uneven playing field to start with, would a CISO saddle the security department with the weight of complex tools and separate data sources to compile alerts and risk evaluation when they should be focused on stopping the vulnerabilities that matter. Why wouldn't they take the lean approach - just like the attacker?





“Although lower cost is often a driver of this trend (vendor consolidation), more streamlined operations and reduced risk are often more achievable.”
(Gartner Top Security and Risk Trends for 2021)

Vendor Consolidation Practical Implications – Use Case

Consider the typical use case of a CISO having to present their overall risk stance to the board. In preparation for the board meeting, 25 percent of the time the CISO will want to present key findings of security audits and relevant remediation plans to the board. But if you are burdened with the complexity, say of 46 tools – how does the CISO present their findings? Again we are back to the basic driving idea that less is more. And then typically, another twenty-five percent of the time, the CISO will want to present a picture of their overall security posture – be it an aggregate risk score, traffic light scoring system, etc. But again if one has 46 different sources of truth, this is a very difficult thing to present. And to compound the issue further, attempting to tie together Key Performance Indicators (KPI's) will be challenging to say the least.


A Fool with a Tool is Still a Fool

All of these security tools are individually complex and expensive. And it takes a highly paid expert to run it. You could run all tools and grab all the data and hopefully catch everything – if you have unlimited budget and people. But it will be very noisy – a lot of false positives – causing fools errands. But of course one could try the spray-and-pray approach. One word of caution - the attackers are not using a spray and pray approach. They know better. They are the hunt for the one vulnerability on the one occasion that will yield the prize.

The Tuning Challenge

Again by definition – without vendor consolidation – there will be a wide array of tools. The network, web applications, IOT and API are all fundamentally different. The alerts need to be each tuned to get good coverage – they simply do not work in each enterprise context right out of the box. It's very unlikely that the typical CISO will be able to overcome the challenge to have every tool tuned in right “key”.



A background image showing a close-up of a music manuscript with a paperclip. The manuscript is slightly out of focus, and the paperclip is in the foreground, partially obscuring the notes. The overall tone is dark and artistic.

“Consolidation is challenging.
And it takes years to roll out.”
(Gartner Top Security and Risk
Trends for 2021)

The Security Tool Consolidation Marketplace is Not Mature

If the Gartner Top Security and Risk Trends for 2021 underscored anything with the state of security vendor consolidation - it's certainly not mature. One may say it's practically non-existent. (reminder alert - 78% have 16 tools or more and 12% have 46 or more). And yet the conclusion of the report suggests that the majority - 80% of organizations - are interested in a vendor consolidation strategy. In fact, vendor consolidation is ranked number three as one of the Gartner Top Security and Risk Trends for 2021.

What Gives? - Why is Supply Not Aligned with Demand?


Why is a Top 3 ranked-concern not aligned with the supplier marketplace? Well, cyber maturity in general and vendor consolidation strategy should be aligned with IT maturity. IT maturity frameworks in 2021 are a well... mature thing. There has been a "lean" movement for some time that addresses vendor reduction concerns. But as we have seen, the emerging technology layers in fact organically spawned out dedicated point security tools - causing this conundrum in the first place. And in 2021, the CISO's find themselves with a timing problem - the security tool providers have not caught up to the need to simplify. Instead they attempt to remain competitive by simply being best in class for a specific security layer - IOT, web applications, the network, API's, pen testing etc.

So is All Lost - Are there Consolidation-Centric Security Vendors?

Well there is one vendor - Edgescan - that has developed a solution to integrate a vulnerability management program across the entire IT stack. Actually not only has it taken the herculean step to offer a platform across each IT stack layer, it also has integrated an Attack Surface Management (ASM) solution in one single platform. Specifically, it effectively manages the entire attack surface including - Cloud, Data Centers, Firewalls, IOT Devices, Servers, Services and the challenging API's - basically anything facing public internets. (Read more in the Evolving Attack Surface thought paper). So to suggest Edgescan's approach is vendor consolidation-centric friendly would be an understatement - it represents vendor consolidation on steroids.

Let's consider its approach given the supplier marketplace is not mature in terms of vendor consolidation goals.





Large security suppliers are responding with better integrated products.
(Gartner Top Security and Risk Trends for 2021)

How to Reset the Tool Proliferation Table – Paradigm Change

If the tide for security tools over the past decade or two is simply to refine and refine better tools at each of the security layer attack surfaces – then vendor consolidation will simply not happen. In order to invoke change one must change the model. Or more specifically – the tool vendor landscape has to change. One vendor has come out with disruptive change. One vendor has invoked a paradigm change – Edgescan.

How Much Consolidation are we talking about?

Well it would be disingenuous to suggest in one pass one can take those 46 tools and reduce them to one. But that does not mean you cannot start making significant vendor tool reduction efforts by simply focusing on Vulnerability Management Tools. In this domain of security tools – Edgescan has gone “Smart”.


How does Smart Vulnerability Management work?

Recognizing that the lion’s share of a Vulnerability Management staff is spent chasing false positives (noise) while managing multiple tools, Edgescan wiped the board clean and came up with a new hosted platform where the entire IT security stack is supported with tuned automated scanners whose output is verified with a team of seasoned security experts combined with smart technology. The net result is zero false positives and better prioritization and improved Attack Surface Management (ASM) and one solution to manage across the entire stack.

So from a Vendor Consolidation Perspective – How Much Consolidation Can be Achieved?

Well of course every client’s initial complexity is different but on average the CISO can eliminate conservatively 25%. So for those with 46 tools that translates to ten to twelve tools. Twelve tools is considerable especially when you think of the siloes of data that need to be correlated and business-ranked. That effort reduction could also result in offloading or refocusing four consultants. This is significant and can be realized within weeks of implementation (not years as Gartner suggests with traditional solutions).





If the CISO's table is overflowing with security tools – perhaps it's time to change how they set the table.

Parting Thought – Less is More

Complexity is the enemy. In the current cyber security supplier landscape – there is not a focus on reducing tool complexity. Point solutions are all the rage and the incremental improvements are only focused with improving the individual point solutions themselves.

The Problem is Serious – VERY Serious

And while the driver for security vendor consolidation might be reducing classic vendor overhead and associated costs - the real concern is a very serious one indeed. The irony of security tool proliferation is that it creates a massive burden on the enterprise security team. So much so that managing the inherent siloes of underlying data across the sheer scale of security tools to achieve insight into one's overall security risk posture is not realistically achievable. And worse – it takes the security team's eye off what really matters - catching the vulnerability before the attacker does.

Full Circle – Back to the Gartner Findings

So according to Gartner and to repeat – 80% of organizations are interested in a vendor consolidation strategy and it is the top three security concern overall. Edgescan has been actively delivering tool consolidation benefits now for years and they are typically allowed a seat in the client's management room simply because of the fact that its platform covers a number of tool application layers. If you are part of the 80% that sees merit in security vendor consolidation, perhaps you should at least start consider a platform like Edgescan. One can counter that there is always risk with a new approach. But in this case as we have seen - the risk – the real serious security risk – lies with those who do not change.

