What is Smart Vulnerability Management and Why Does it Matter?

edgescan™

We Live in Smart World

Consumer "Smart"

The “Smart” approach has become ubiquitous in technology ecosystem parlance. The savvy homeowner is all too familiar with smart devices for household activity management. The smart home includes multiple smart appliances, smart lighting, smart electricity management, smart security, smart lawn management, smart entertainment and the list goes on.

Enterprise "Smart"

And the enterprise when managing its business processes is no different in integrating smart approaches for effective and efficient business process management – leveraging automated software, intelligence, analytics, client and supply management and again the list goes on.

But when we talk about “Smart” and Enterprise Cyber Security – specifically Smart Vulnerability Management (VM) – is this just marketing speak? Is it just an ill-fitted analogy with the home smart device ecosystem that actually offers no substantive contribution to meaningful improvement of a Vulnerability Management program?

Smart VM represents a new paradigm change.

And the Answer is ...

Smart VM is not just a marketing catch phrase - it offers significant innovation

It is in fact a very important distinction representative of an innovative approach, or rather approaches integrated with emerging scanning technology that has only recently surfaced within Enterprise Cyber Secutity in 2021.

However, the difference between Traditional VM and Smart VM is not explained by pointing to a myriad of so-called smart devices spread around the enterprise, but rather - its essence is contained in its innovative approaches – an approach that contains smartness in every aspect of the vulnerability management ecosystem.

So What Exactly is “Smart” Vulnerability Management?

It turns out that there are a number of ways in which Vulnerability Management can be smart – lets looks at six of them.

Smart VM is much more comprehensive than just deploying smart tools.

Smart VM
Six Significant Approaches

1

Smart Ongoing Attack Surface Management and API Discovery.

The Morphing Attack Surface

All of us are impressed with emerging smart tech with driverless cars. But imagine the challenge if the road itself is every-changing. This is precisely the challenge with attack surface management. You cannot effectively manage what you do not know. As new systems are deployed, decommissioned or a system changes, changes to firewalls occur, and exposed services and rogue deployments are introduced – each one of these events provides continuously evolving avenues of attack for any enterprise.

The Ever Growing World of API’s

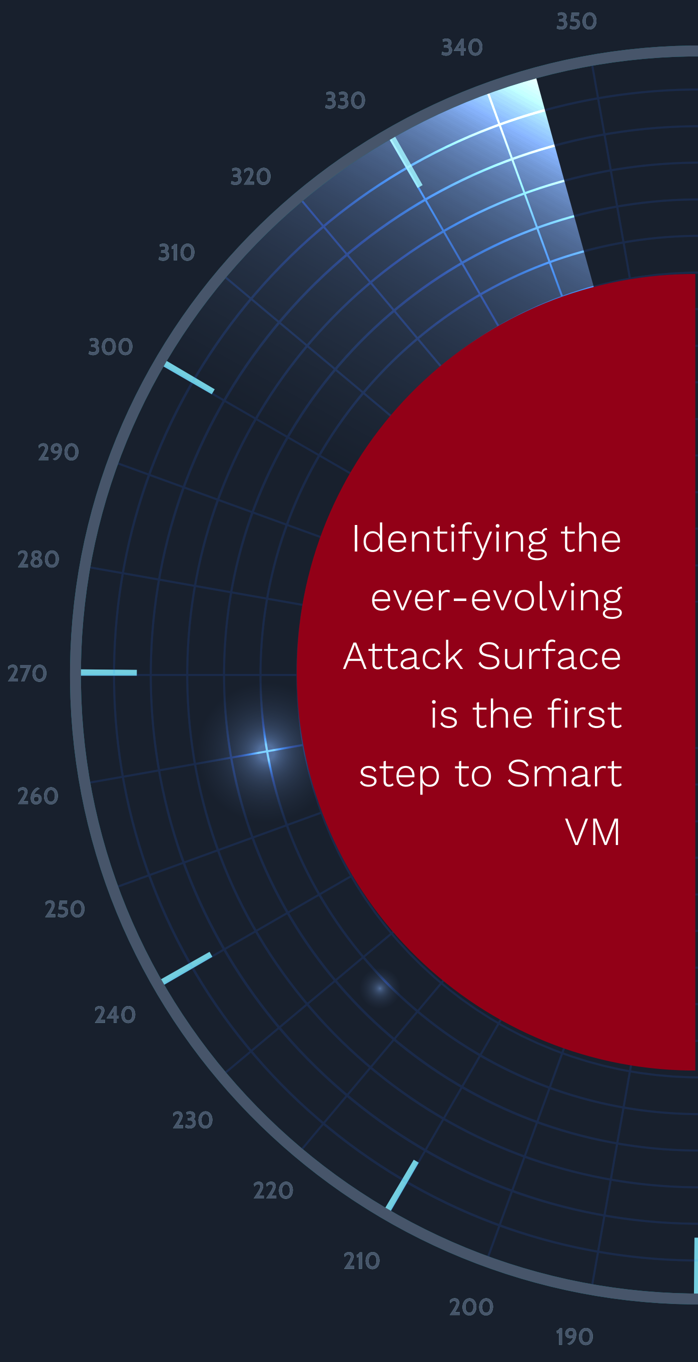
Again like the attack surface, unidentified and unmanaged API’s can lead to blind spots. And API's are becoming ever more popular given the explosive growth in mobile apps and the financial technology (FinTech) sector. Each API exposure can represent a unique attack vector into the enterprise’s systems. And their shapes and forms can be quite varied - including but not limited to SOAP/XML, RESTful and other Web Services.

The Knowing Eye – Flying Blind is Not Smart

The requirement is simple. To be smart, your VM approach needs to provide you the ability to see all services exposed to the public internet across your global estate. And this is not easy. Especially with API detection and scanning – the technology for the API use case is not as mature or focused as general attack surface vulnerability scanning. Smart API assessments also assess logical controls associated with the API - items such as authorization, request flooding, parameter manipulation and attribute injection can be assessed to help establish a strong security posture.

Adaptive Smartness

And so on the question of smartness applied to Vulnerability Management – here we have a case of super smartness. For an effective Smart VM solution will continuously scan and intelligently discover and assess both the perpetually changing attack surface and API. Adaption is smart.



Identifying the ever-evolving Attack Surface is the first step to Smart VM

Smart VM
Six Significant Approaches

2

Integrating Smart Vulnerability Detection and Assessment with Penetration Testing as a Service

Smart Approachs to Achieving Depth and Rigor

Automation can only get you so far. In general, automation and scanning tools do not detect certain issues including business logic and complex data-driven vulnerabitlies. That's where Penetration Testing comes in.

Penetrating the Depths

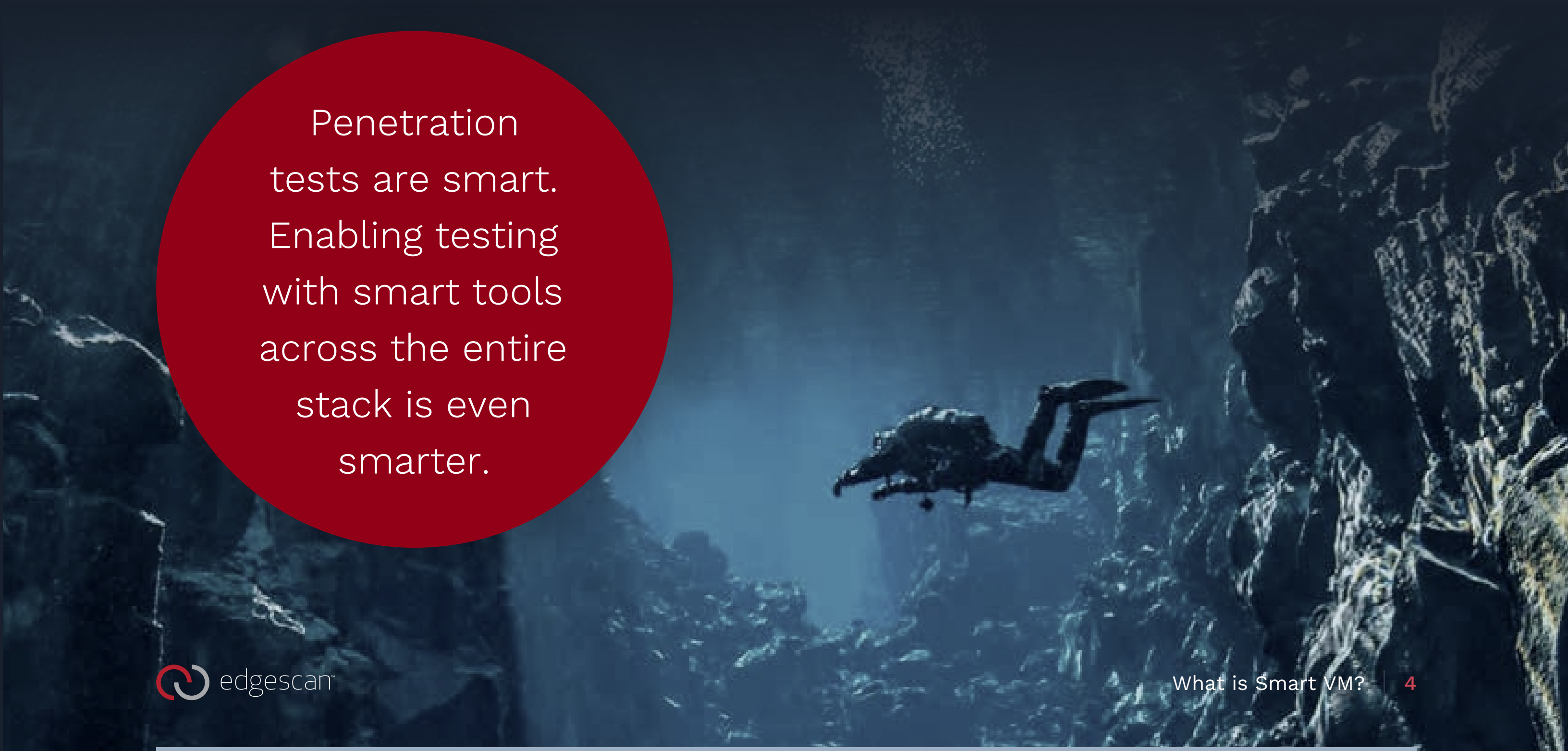
In order to verify and determine that all vulnerabilities have been effectively closed, it is necessary to manually attempt to break the business logic of the application. This needs to be performed by experts whose technical expertise and enterprise business logic knowledge can truly go to the bottom off what the automated scanning tools have surfaced and provide an in-depth analysis and verifiable conclusion to every possible exposure.

Widening the Breadth

And the test needs to cover everything – testing both the technical and logical security posture of every asset – including API's, cloud-based infrastructure and web and mobile applications.

Smart Solutions for Smart Penetration Testing

So Pentetration testing combines human expertise on top of the smart scanning technology and the expert testers themselves have their own smart tools - specific consultant tools, such as automated static and automated dynamic analysis for assessing high assurance applications.



> Penetration tests are smart. Enabling testing with smart tools across the entire stack is even smarter.

Smart VM
Six Significant Approaches

3

Smart Security Layer Integration

One Dashboard of Smartness

Returning to our smart home analogy – a table covered with smart controller devices or a smart mobile device littered with smart applications for every layer of home management gets less and less smart as the point solutions proliferate. To go on vacation and have to individually put each device for each application in vacation mode is dumb. And yet when we look at most enterprise's Vulnerabitliy Management approach to dealing with each layer of the stack - network, application, API, mobile, IoT – we find the industry proliferated with individual point solutions.

Can We Just Not Combine Point Solutions?

Well, if one has separate point solutions then yes, one will have to manually combine them to attempt to achieve a composite view of the truth. But one cannot resist pointing out that such an inefficient approach necessitates time, budget and re-engineering to tie disparate systems and reporting and analytics to one dashboard. The smarter question to ask is – Why would you do that? Or put differently – Why would you not just use an integrated full stack solution to begin with?

An Integrated Full Stack View is a Smart View

VM with blind spots is not smart. Smart VM assesses vulnerability across the entire stack. Just as the hacker themselves welcomes any weakness on any layer – they are quite liberal in this respect – so too should the Smart VM solution address any issue in any of the layers.

Detecting Correlations Between Layer Incidents is Smart

And even if you manually attempted to tie insights from each tool dedicated to each layer, there are correlations of incident detection between layers that you may miss. And these correlations are precisely what a single, integrated full stack solution would detect.

A single, integrated full stack solution is key to Smart VM.

Smart VM
Six Significant Approaches

4

Smart Intelligence

Context Matters

Traditional automated scanning solutions will provide incident alerts. They will provide a lot of them. But without knowing their context – what order of priorty both on the business and technical side they should be placed in – then it is a challenge to say the least, how one should respond and with what urgency. And chasing every incident as if it has a Level 1 risk association tied to it, is simply not sustainable.

Installing Smart Intelligence - Its All About the Setup

A Smart VM solution will be built so that in the onboarding phase, vulnerabilities can be classified to reflect both the technical and business risk they represent. So instead of trying to determine potential risk, the alerts with a Smart VM solution will present themselves in context so that significant incidents can be dealt with in a timely and relevant way and conversely, incidents that do not represent significant risk can be handled appropriately.

But Every Business is Different

They certainly are. Put simply a game streaming company will have different concerns than a Financial Service company. And that's why with a Smart VM solution, there is the built-in capability to rank incident type against the specific technical and business risk for that business. And then there is built-in automation to automate security and attack surface alerts with contextualized business and technical priority rankings.

All Incidents are Not Created Equal

Web application Risk Density is typically vastly higher than non-web application assets. It is important that your Smart VM solution can provide you an accurate assessment of the risk density of every threat. Smart VM means you can quickly determine between critical, high, medium and low risk. Context drives everything.

Not all alerts are created equal. Smart VM provides context.

Smart VM
Six Significant Approaches

5

Smart Operations

Smart Remediation Integration

The Smartest of VM solutions will be effectively rendered useless if the insight and practical remediation guidance is not integrated into the daily operational support systems and workflow. The challenge is that typical risk, software development and ticketing systems were not built to capture output from a VM solution.

From Insight to Action

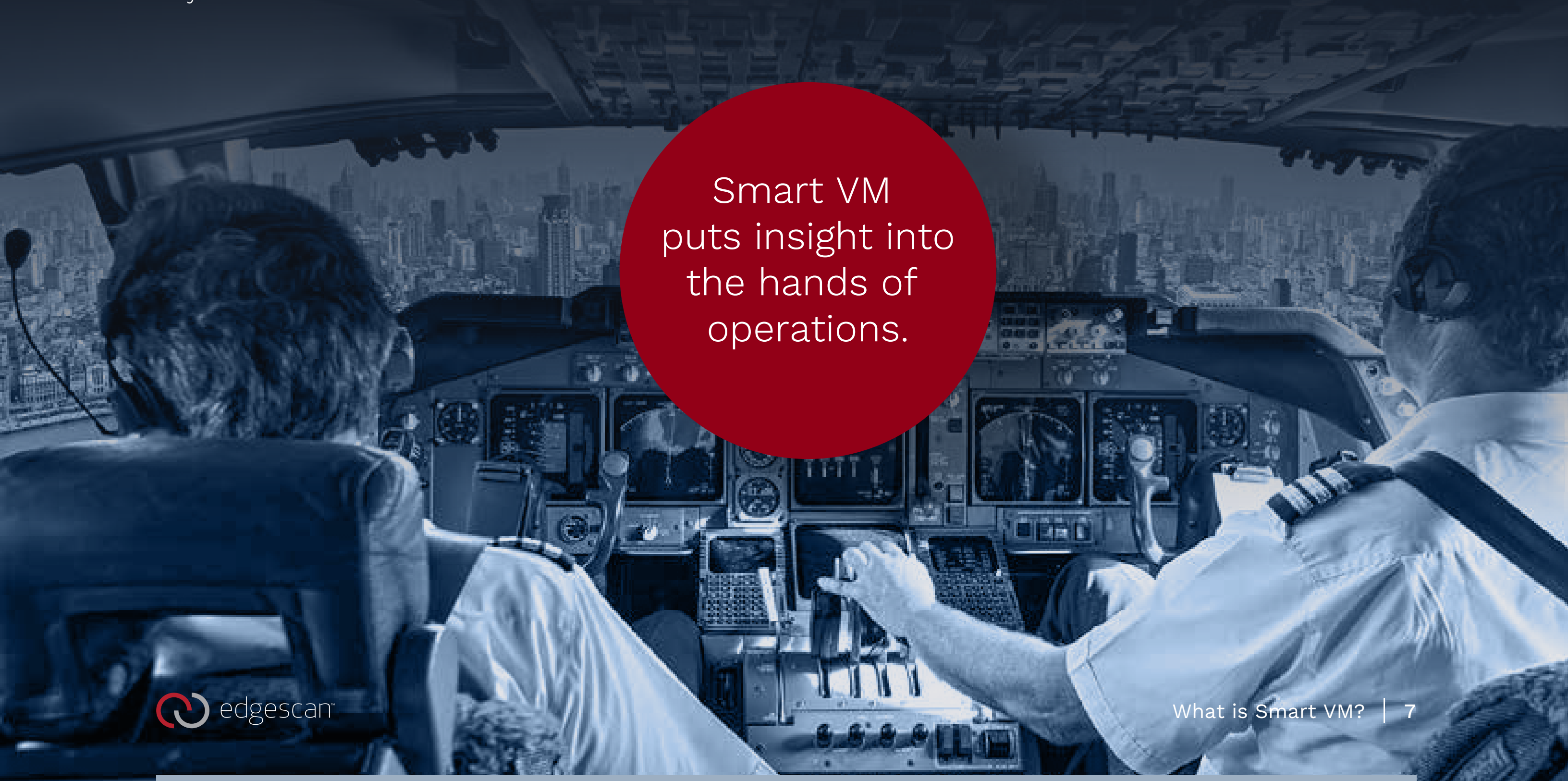
The smart approach is to automate VM intelligence and remediation guidance into daily operational workflow systems. So risk managers, software development managers and operational support staff can readily see within their systems, the vulnerability issues as they arise and are presented with tactical guidance on how to resolve them.

A Wide Integration

So what type of systems are we speaking of here? – in short, all of them. Notifications can be sent through Webhooks/API integrations, Ticketing systems, Instant Messaging, Risk Platforms, Bug Tracking, Asset Management and SIEM systems. Some of the typical brand names are Webhooks, Risksense, Jira, Axionus, YARO, Zapier, Microsoft Teams, and Slack.

Being Proactive is Smart

And with automated integration between remediation and operational support in place, this means that expert guidance can not only provide timely instructions for incidents as they happen they can also point to patterns and preventative ways to avoid issues in the future.



Smart VM puts insight into the hands of operations.

Smart VM
Six Significant Approaches

6

Human Security Expertise - The Granddaddy of VM Smartness

Automated tools provide scale. Human expertise provides meaning.

Injecting Human Smartness

It is an interesting irony in that with our original analogy with the smart device ecosystem for the smart home – the goal there was to use technology to ape the smartness of the human managing the home themselves. This final and perhaps most important approach with Smart VM is to bring the human back in front and center.

Hybrid is Smart

To determine the meaning of each incident and what it truly represents in terms of real risk to the business it takes a human – a skilled security expert – to make that assessment. And we call the overlay of human security experts on top of the automated scanning tools a hybrid approach. And its smart in a number of ways. One of the most important is simply taking out the noise.

Take Out the Noise Please

Ask any cyber security staffer what is one of the most drudgerous, repetivie, boring tasks of daily, vulnerability management – the donkey work – almost unanimously they will say getting rid of the noise – removing the false positives. For if you want a truly ineffective VM program, let all your prized cyber security staff act on every incident alert that arises. Instead the hybrid model takes a team of experienced security engineers who act as a filter ruling out the false positives so when your VM team receives actual verified alerts – they know they are real.

Can the Hyrbid Approach Scale?

Of course we should remind ourselves that the entire point of these smart automated scanning tools was to scale. If integrate human experts into the equation then does not our ability to scale suffer. Sure we want to the human discernment but not if it means we cannot scale with a rate at which incidents occur. And the answer is to pick a hybrid solution that offers an integrated team of experts in sufficient quantity that it can in effect handle the scale.

Human Experts Equipped with Smart Tools

And more important than the capacity of the human touch side of the hybrid model, is the fact that they themselves use integrated, automated tools to handle the volume issue and provide the human interpretation layer only when needed. That's the key to scaling.

The Complete Smart VM Solution

The smartest feature of Smart VM is the integration of expert certified security analysts augmented with smart technology to ensure that every discovered vulnerability is real, accurate and risk rated correctly. This smart approach delivers accurate insight where it matters and timely remediation for resolution.

Conclusion

A Paradigm Change

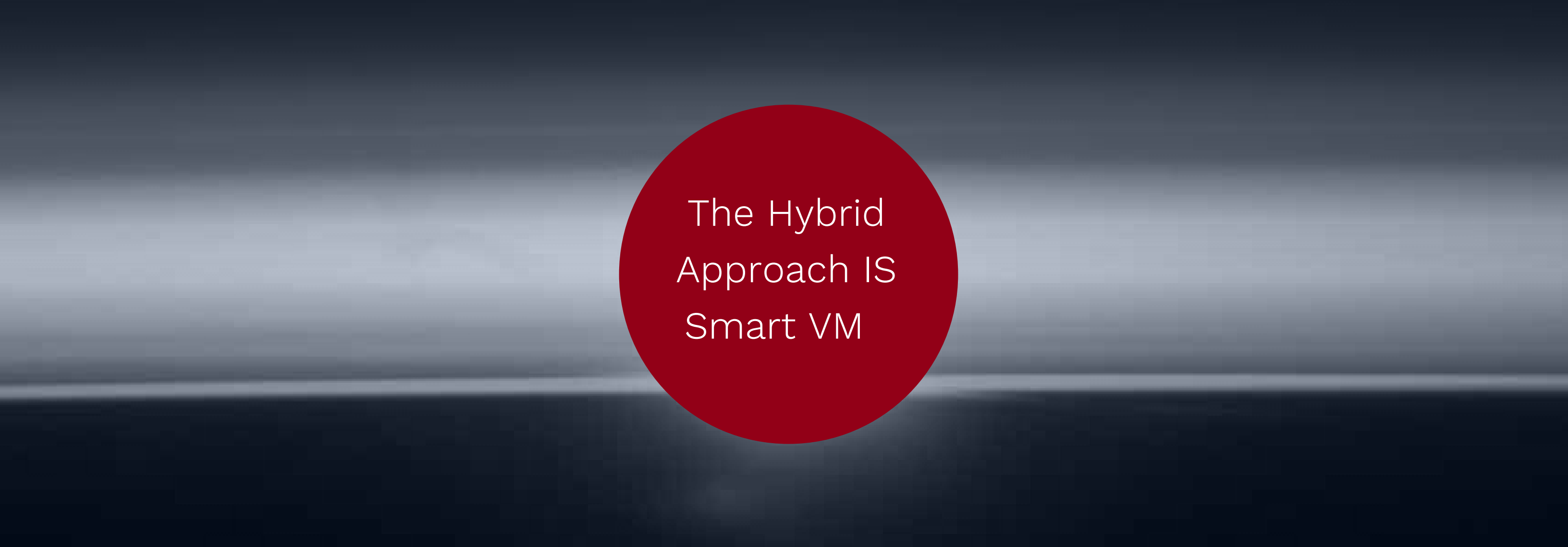
So in the end it turns out that far from being a hackneyed marketing phrase, Smart Vulnerability Management represents an approach that fundamentally turns traditional vulnerability management on its head. Rather than thinking about only adding a bunch of automated scanning tools to your program, the Smart VM approach actually starts with expert security analysts and then integrates a complete VM platform that does the bulk work of automated detection across the entire stack. And the whole approach does not lead to smart devices as the end game, but rather leads to the smart analyst who takes the torrent of noise and refines it into smart intelligence and smart remediation with no false positives to lead one astray.

Human Expertise Delivers Smartness

Smart VM actually is a hybrid approach – the marriage of smart automation with smart human intelligence across the entire stack. A bit of irony perhaps – but the consumer analogy that led this paper – an analogy which stresses the proliferation of smart devices to advance the concept of the smart home really is broken with Enterprise Smart VM. For it’s the old school craft of the Security Engineer who through training, certification and years and years of experience delivers the final “smartness”.

Point Solutions are the Enemy of Smart

And unfortunately in the year 2021, the enterprise is still chasing point solution tools (aka smart devices) when this traditional VM model is broken. To be truly Smart VM, the hybrid model must be adopted.



The Hybrid Approach IS Smart VM