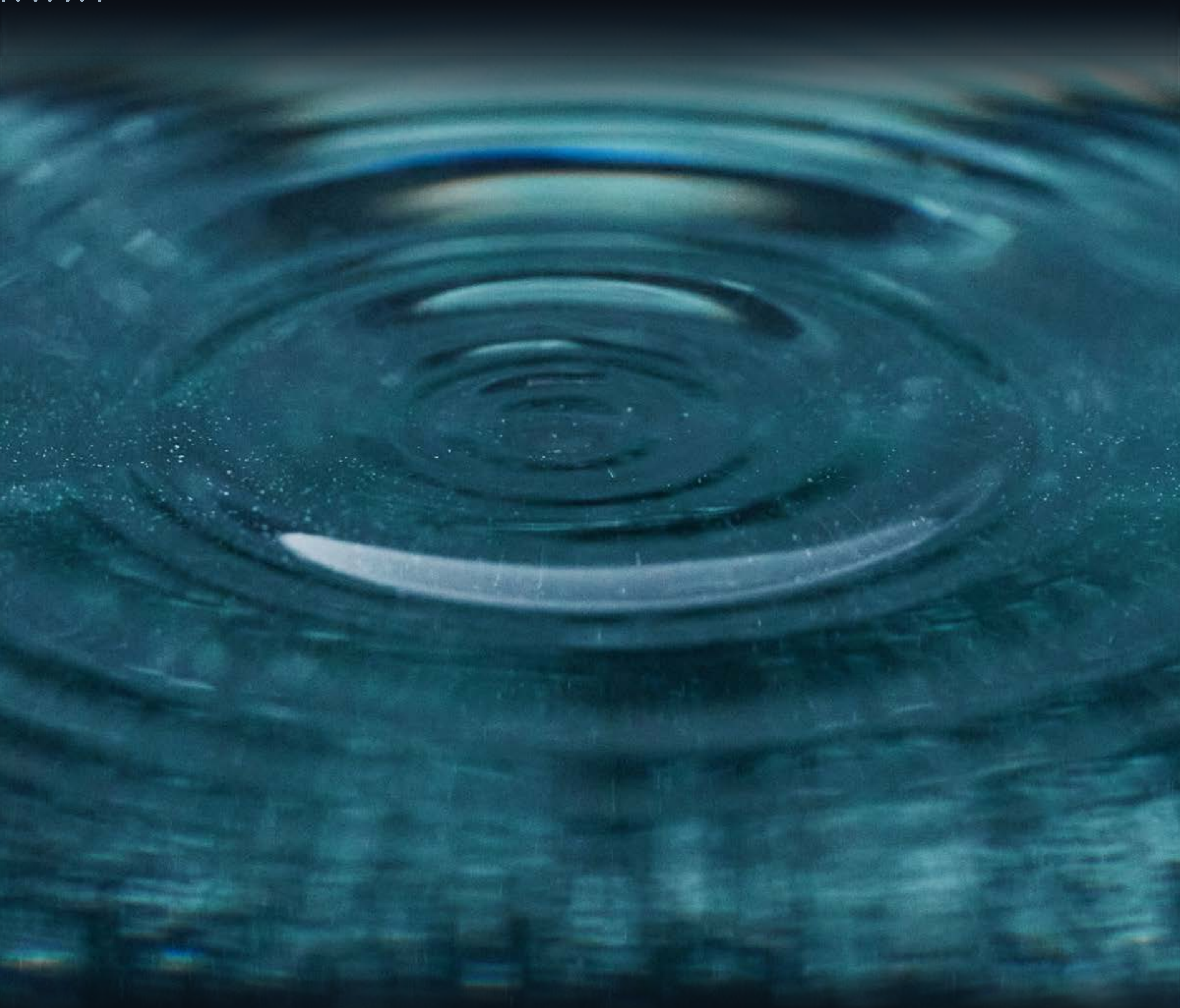
The Evolving Attack Surface



edgescan™

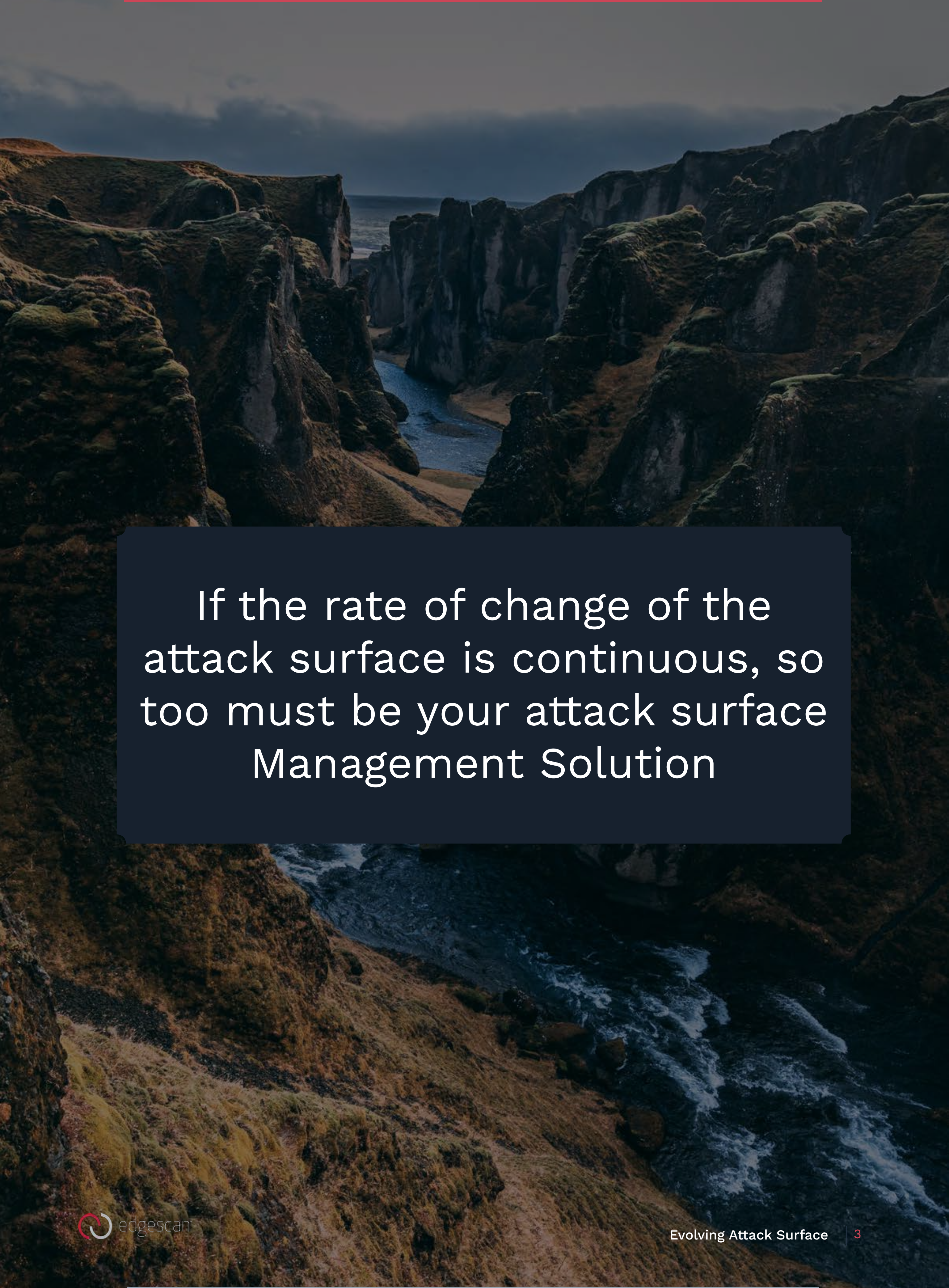
Adapting to an Evolving Threat

While it’s a constant challenge to anticipate the next wave of creative techniques deployed by cyber hackers - it’s all the more daunting when the very avenue of attack itself is in constant flux. It almost sounds like a strange science fiction plot - where the bad guys have some special powers to arrive on the scene at any time in any fashion they desire. But this is the reality an enterprise faces as they constantly try to detect when the attack surface changes and whether preventative measures need to be taken. This is the challenge of Attack Surface Management (ASM).

Change is Constant

For just as a business adapts on the fly to new market conditions, so too does its internal and client-facing IT services. It is constantly changing. The way the attack surface changes is wide and varied – and the chance of human error with every new exposure is equally mixed.

A exposures could be the result of deploying new systems and servers and the control measures are not set up properly or a key service is inadvertently exposed▯it could be something at the administration level, like not configuring the services securely or it could simply be human error, exposing unintended services involved with new and rapidly expanding cloud service deployments.



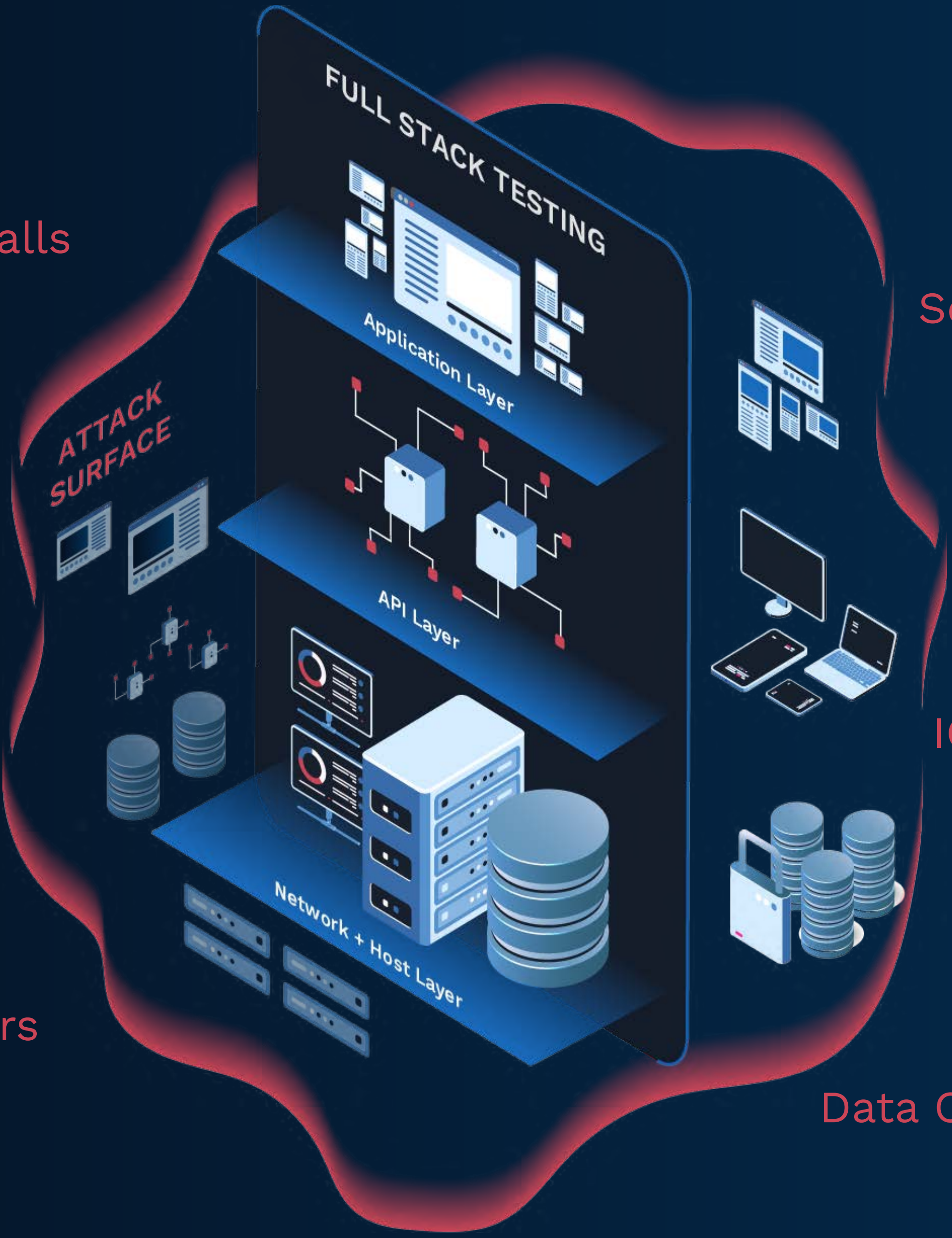
If the rate of change of the attack surface is continuous, so too must be your attack surface Management Solution

So What Exactly is an Attack Surface?

While the frequency of change is fast and continuous there are a finite types of attack surface that one must manage:

This includes anything facing public internets including the following:

Cloud



Firewalls

Services

API’s

IOT Devices

Servers

Data Centers

So What Exactly is an Attack Surface?

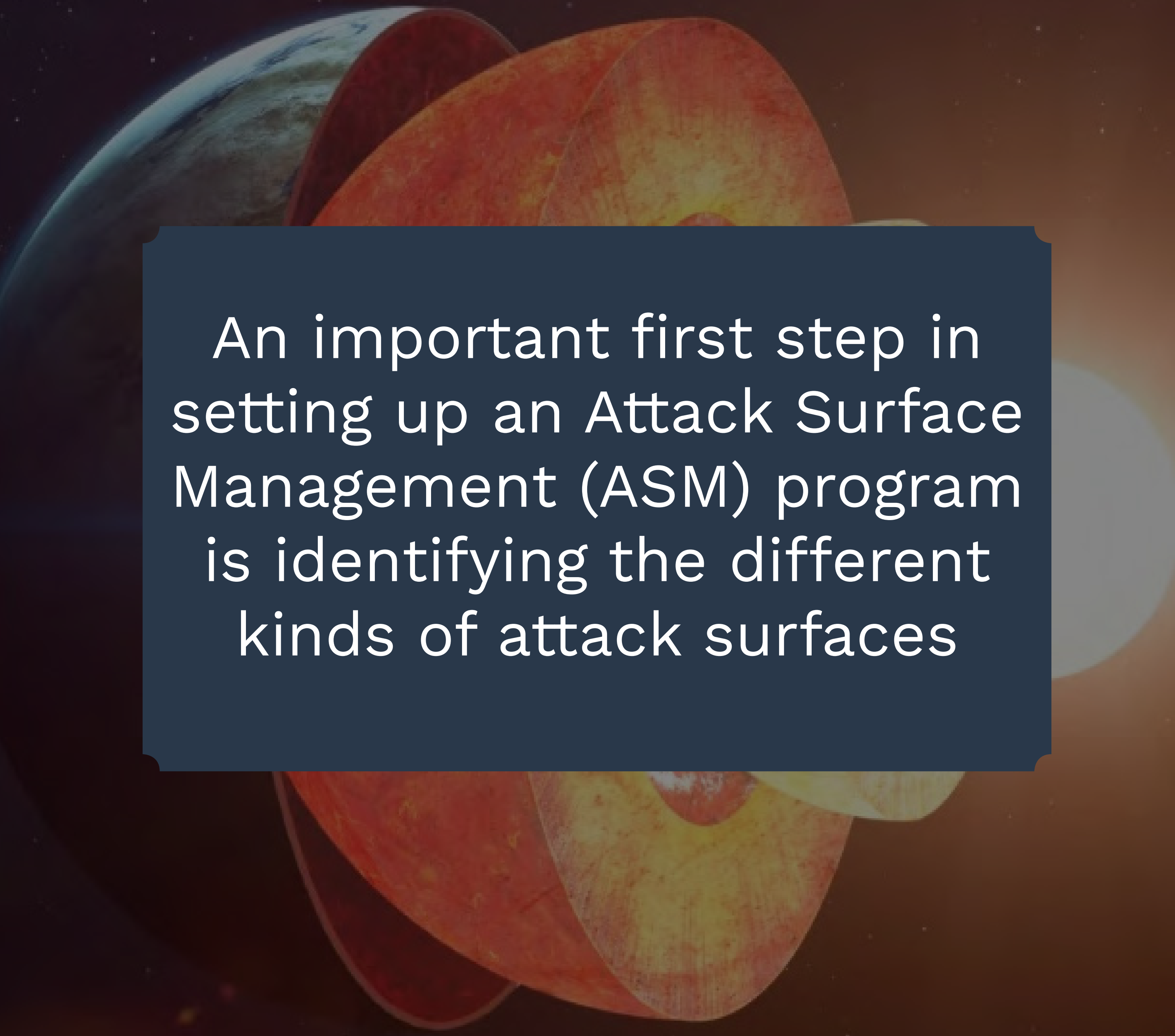
Any endpoint exposed to the public Internet is attackable, hence Attack Surface Management (ASM).

Attack Surface Checklist

And against each of these layers one should have a solution that is:

1. Fast ☑
2. Customizable ☑
3. Maintains historic records ☑
4. Supports IOT detection ☑
5. Delivers API discovery ☑
6. Scalable ☑
7. Real-time ☑
8. Accurate and Useful!! ☑

DEVICES
DATA
NETWORK
ATTACK SURFACE
API
APP



An important first step in setting up an Attack Surface Management (ASM) program is identifying the different kinds of attack surfaces

Managing Risk - Attack Surface Demarcation

There are basically two layers of concern from opposite ends of the spectrum. On one side, there are internal avenues that should never be exposed to the public internet and then on the other side, there are external client-facing services that must be managed.

Shut it Down

There are the cases when internal assets are exposed to the public internet and they should not be– an administration console, a remote desktop/access type service, a database or file share/S3 bucket is exposed, a new internal deployment etc.

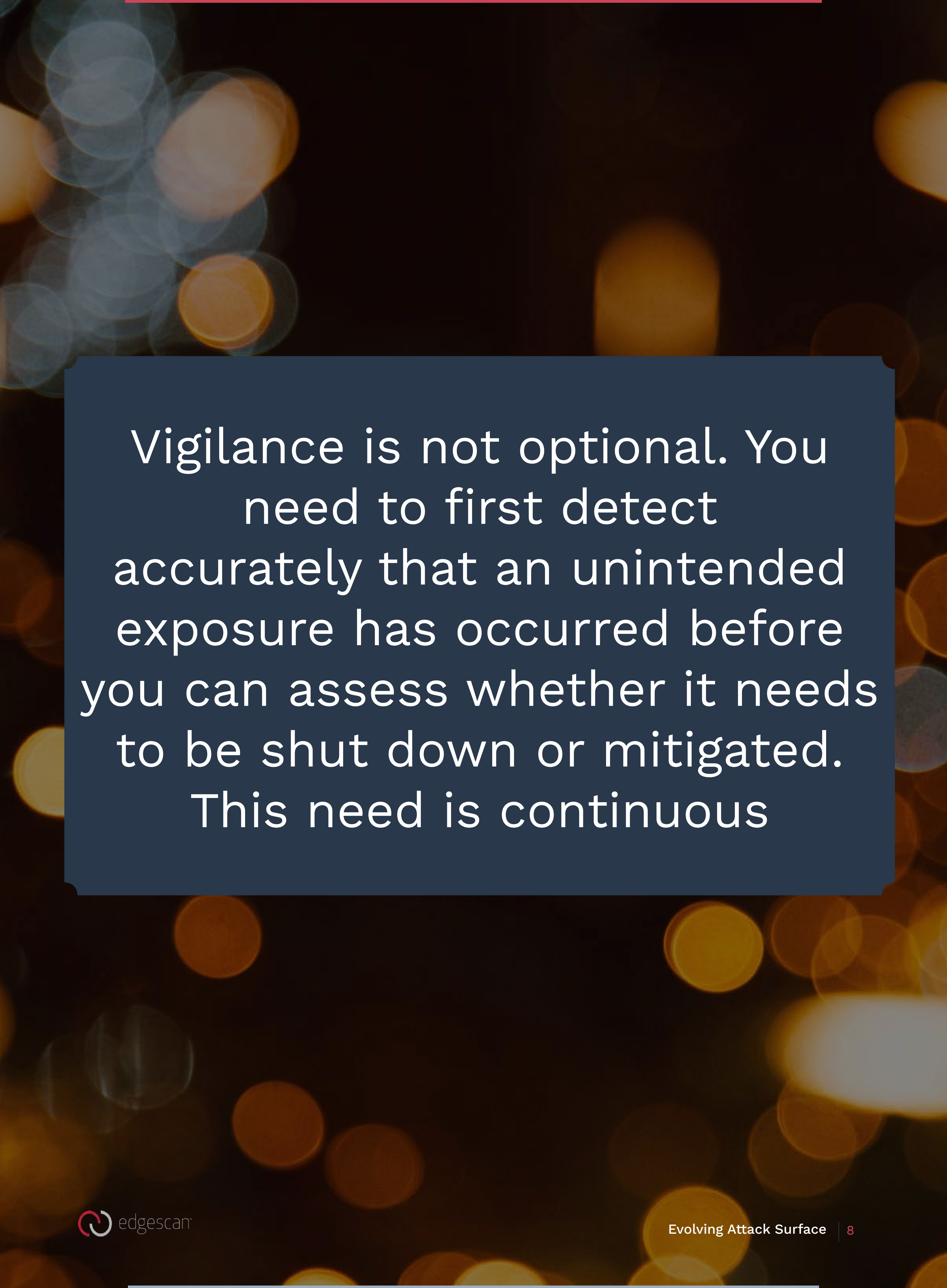
And while human error can lead to a lot of these kinds of exposures – there is no uncertainty whether exposure is necessary or not – they simply should not be exposed and they should be shut down immediately.

Managing Risk

And then there are the types of exposure – IP's and Web Applications for example – that are intended to be exposed to the internet. This is specifically what they are used for - public access.

Of course a business like eCommerce requires online purchases for their revenue goals – out of the gate a comprehensive Attack Surface Management solution is required. However, traditional business like financial services, travel and health services are rapidly rolling out digital transformative offerings to become competitive. This means they continue to expose more services to the internet. In this case, the enterprise is specifically moving to the public internet to access new streams of business and while this is a calculated decision to allow new public access – now an additional layer of managing attack surface exposure is introduced.

And again our friend – human error – can wreak havoc – including issues like the simple lack of knowledge that something was deployed, a firewall was configured incorrectly, a system is without a critical patch etc. All of these require immediate detection and an immediate business assessment that such instances represent an issue or is aligned with intended business goals.



Vigilance is not optional. You need to first detect accurately that an unintended exposure has occurred before you can assess whether it needs to be shut down or mitigated. This need is continuous

Archiving Surface Management

Is it acceptable to let things die on the vine?

Resembling outer space where various countries have allowed satellites to simply float around after their active service engagement has expired – the proverbial space junk – enterprises, almost as standard practice, also allow a service to simply stick around just in case some legacy processes might need to use it in the future. Management believes they are simply playing it safe – but are they?

Festering Vulnerability

While there is not a consistent pattern or explanation, it turns out that legacy services and their related exposed surfaces become more vulnerable over time. Allowing old services to persist is not playing it safe – it is introducing your organization to a larger window of exposure and in most cases completely unnecessary risk. Sometimes it's not possible to replace a legacy service, so then countermeasures need to be deployed. If we are not aware that this is the case, we may not protect a critical asset adequately.

Your Options

The most obvious option of course is if the service is truly no longer needed, then decommission it. But also provide a re-introduction request option for when the business so requires. The second option – if true business need currently persists – knowingly allow the service to be exposed but simply agree on a timeline when that decision can be revisited. So then it can be effectively shut down when it makes business sense and risk is effectively managed while it remains in service.

Visibility is of paramount importance in cyber security.
We cannot secure what we cannot see.

Attack Surface Management Law

–

The longer a business allows old services to continue, the larger the window of exposure.

API’s – A Special Challenge

Not to be dismissive – Web and IP are more easily dealt with by just using standard scanning tools. Exposures related to things like the Administrator Console or Internal Databases in the context of Attack Surface Management are relatively straightforward to handle and there are mature solutions to deal with them. However, API’s are a special breed of problem.

API’s – Can We Talk?

So why can we not just use the same scanning technology for the network and application layers for API’s? Well the principle challenge is that one needs to “talk” to an API. One cannot detect with port scanning-only type solutions – it requires a multi-layer probing approach. API’s can “hide” behind regular web ports without being found by typical port scanning technologies.

The Solution – A Phased Approach

In order to talk to an API for detection purposes, a full stack probing technology needs to be deployed where it looks for API’s across the web application and network stack. For example, the API may be sitting on a server that you simply do not know about.

To provide total visibility – a three-phased approach is recommended:

Phase 1 Passive

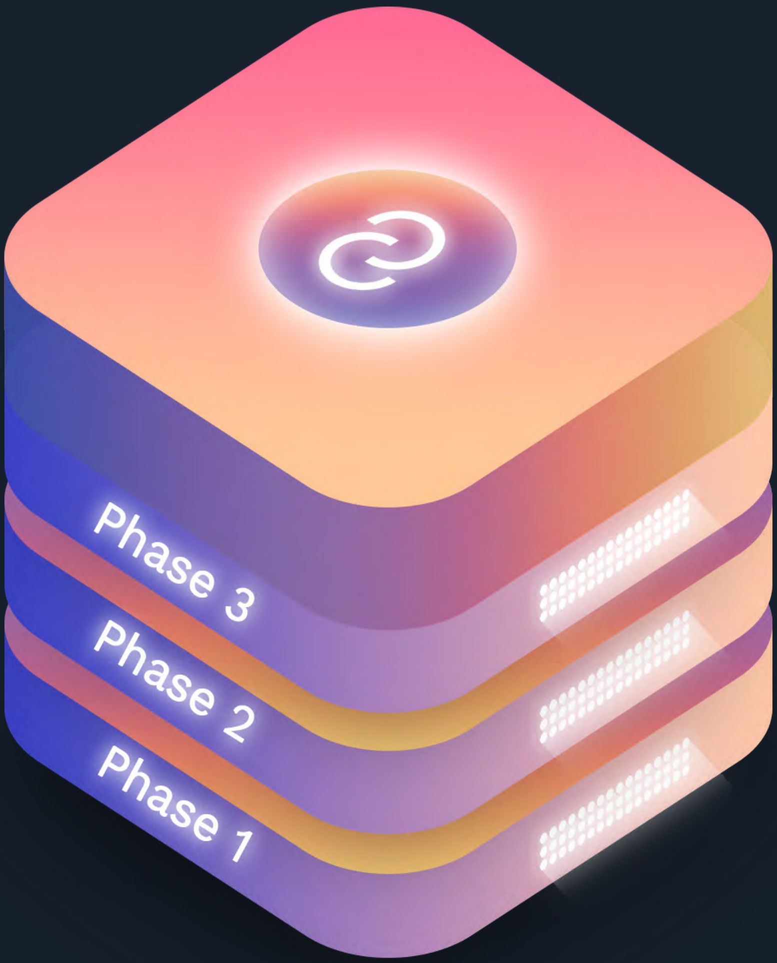
Analyze the estate looking for indicators of APIs

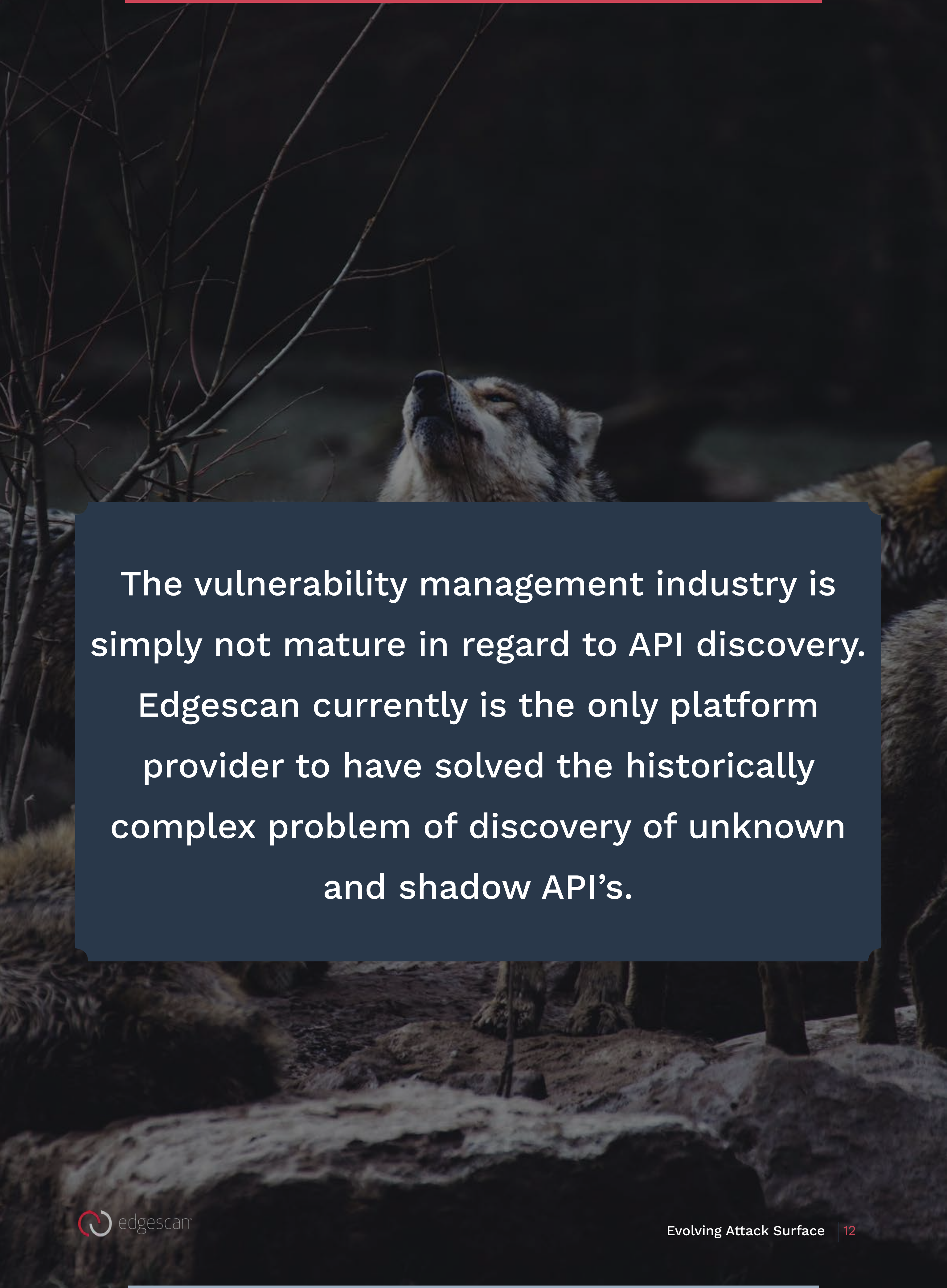
Phase 2 Interaction

Continuous asset profiling run against all available external addresses integrated with multilayered checks applied to all live services, resulting in discovery of unknown and shadow API’s.

Phase 3 Assessment and Enumeration

After API discovery has been completed, run custom API security assessments against all live services. These are specific API security checks to determine the security posture of the discovered API’s.





The vulnerability management industry is simply not mature in regard to API discovery. Edgescan currently is the only platform provider to have solved the historically complex problem of discovery of unknown and shadow API’s.

Integrating ASM with Vulnerability Management (VM)

Advancing a Vulnerability Management Program (VM) first with a sound Attack Surface Management (ASM) approach makes sense. It is simply irresponsible not to proactively manage and have visibility of potential avenues of attack before a hacker takes advantage of them. Sure a comprehensive VM solution can detect vulnerabilities but why would one not visibility of the avenues of attack – the exposed endpoints - in the first place?

Continuous Really Means Continuous

While it would be desirable in one herculean move to rid oneself of vulnerable and exposed systems altogether (reducing the attack surface) - the reality as we have seen is that human error coupled with patching cadence and more and more rapid new deployments - especially with the migration to the Cloud - is really a recipe for continuous and new potential avenues of attack. The monster never sleeps.

So for a typical organization with say 100,000 end points – to give oneself 24 X 7 continuous coverage we would typically expect a frequency cycling every four hours to update and provide an accurate picture of your entire attack surface.

Integrating ASM with Vulnerability Management (VM)

Extending ASM with VM – A Three-Layered Approach

But of course no matter how accurate and continuous your ASM program is – one still has to manage risk by accurately identifying vulnerabilities as they occur across the full technology stack and assessing their impact and resolving them in a timely manner. So just as we suggested a three-step approach to API discovery, we also suggest layering in three basic approaches with VM:

Layer 1 – ASM – continuously and accurately detect and assess your attack surface including the challenging case of API's. What can be potentially hacked?

Layer 2 – Vulnerability Management – continuously and accurately detect all vulnerabilities and exposures across the full stack to rank business concerns and tightly integrate with support operations for timely remediation. What weaknesses to we have?

Layer 3 – Penetration Testing – armed with ASM and VM intelligence, perform laser-focused resilience tests on areas of concern, or complex areas not suitable for automation such as business logic, to determine the validity of any potential issues and take the extra step of breaking the business logic of applications for 100% validation. What can a skilled attacker do?

Setting Up Alerts

Of course every business has its own nuances and will need to set up alerts to capture "quirks" within their own digital estate. But it is important to realize that there are solutions that provide customized, multiple-format, automated alerts that let one continuously know that there are new attack surface exposures that need to be assessed. If your current solution does not provide such capability, you should consider a new solution.

Proactive Alerting & real-time visibility

One simply needs to be informed when it happens – rather than look in a portal to source a new potential exposure, one requires a proactive solution. For example, perhaps a service popped-up in Korea. Perhaps in this case, we already knew that. But the next alert from Brazil, suggests a new service started that you did not know about and it carries huge risk – you need to mitigate the issue quickly. In either case, your smart ASM solution should alert you and allow you to make that decision. And the system should detect so-called benign exposures – say in the case where you did allow an old system to die by the vine in a safe fashion.

Take Advantage of New Advancements in Contextual Alerting

More progressive ASM solutions offer contextualized alert logic. Again every business has its own quirks. So for example, a gaming company might provide access to 100,000 end points and only allow access through ports 80 and 443. So in this case, you can create an alert so that any time a port that is not 80 and 443, one is notified. While a different enterprise might offer service globally hosted with say the exception of clouds in Canada and Egypt. So anytime a service is detected from an IP space in Egypt or Canada, alerts are triggered. And so one should configure their alerts to what matters to them – whether its geography, a URL or URL's, a business unit, etc. This will also help with Attack Surface alerting "fatigue" – only triggering alerts where it matters to your business.

Choose Your Communication Avenues

And just as you contextualize what triggers the alerts for your business, you should also take advantage of solutions that can customize how you communicate those alerts. In some cases, it could be a help desk email,▯other case it could be an Instant Message or through Slack or it could trigger an API web hook As we have discussed – especially with the proliferation of cloud based services – changes can occur quickly and one should communicate attack surface changes in a format that produces the desired response within your audience's particular workflow.

Customized, Intelligent Automated Alerts are Key to Attack Surface Management

Does is Really Matter?

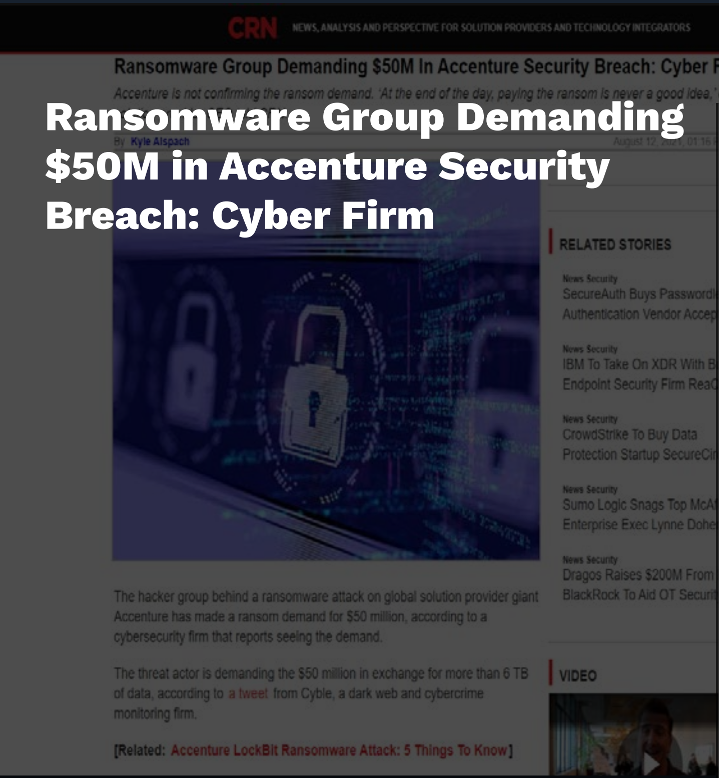
Of course, even if conceptually it does not seem a good idea to allow new attack surface avenues to propagate – one can still ask at the end of the day – does it have a significant downside? Are the big security disasters we read in the news simply the byproduct of poor Attack Surface Management?

Poor ASM Results in Big Breaches

It turns out that large breaches are a result of not managing attack surface properly. Many recent high profile Ransomware attacks were a direct result of letting the guard down managing their attack surface. The June 2021 Colonial Pipeline attack where hackers who launched a cyber-attack against the company, disrupted fuel supplies to the U.S. Southeast. Again poor ASM was at the root of the problem. The vulnerability may have been mitigated if a high level of visibility was in situ via an ASM solution.

So How Does it Work?

How can detection of unwanted attack surface exposures prevent these type of massive, newsworthy hacks? Well it turns out that average age of the exploits used to breach is one to three years. So if they had a viable ASM solution – in other words if they had identified and closed the avenue of attack earlier – all of these hacks could have been avoided, assuming the issue could be mitigated in some way.



Ransomware Group Demanding $50M in Accenture Security Breach: Cyber Firm

CRN NEWS, ANALYSIS AND PERSPECTIVE FOR SOLUTION PROVIDERS AND TECHNOLOGY INTEGRATORS

Ransomware Group Demanding $50M In Accenture Security Breach: Cyber Firm

Accenture is not confirming the ransom demand. 'At the end of the day, paying the ransom is never a good idea,' one

By Kyle Alspach

August 12, 2021, 01:16

RELATED STORIES

News Security
SecureAuth Buys Passwordl
Authentication Vendor Accep

News Security
IBM To Take On XDR With B
Endpoint Security Firm ReaQ

News Security
CrowdStrike To Buy Data
Protection Startup SecureCir

News Security
Sumo Logic Snags Top McAf
Enterprise Exec Lynne Dohe

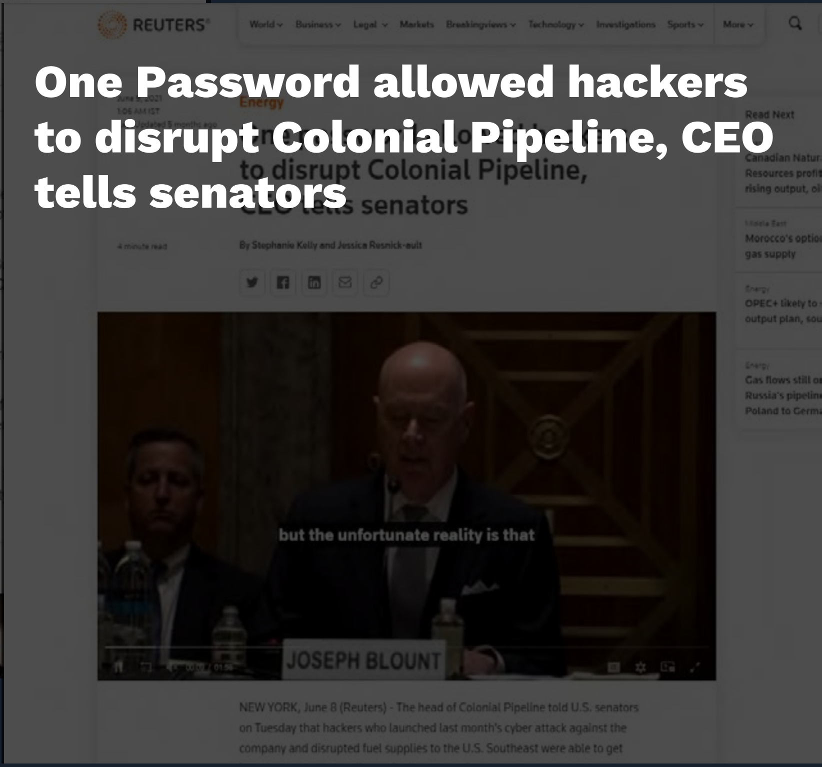
News Security
Dragos Raises $200M From
BlackRock To Aid OT Securit

VIDEO

The hacker group behind a ransomware attack on global solution provider giant Accenture has made a ransom demand for $50 million, according to a cybersecurity firm that reports seeing the demand.

The threat actor is demanding the $50 million in exchange for more than 6 TB of data, according to a tweet from Cyble, a dark web and cybercrime monitoring firm.

[Related: Accenture LockBit Ransomware Attack: 5 Things To Know]



One Password allowed hackers to disrupt Colonial Pipeline, CEO tells senators

REUTERS

June 9, 2021
1:06 AM IST
Updated 5 months ago

Energy

to disrupt Colonial Pipeline, CEO tells senators

4 minute read

By Stephanie Kelly and Jessica Resnick-ault

NEW YORK, June 8 (Reuters) - The head of Colonial Pipeline told U.S. senators on Tuesday that hackers who launched last month's cyber attack against the company and disrupted fuel supplies to the U.S. Southeast were able to get

Read Next

Canadian Natur
Resources profit
rising output, oi

Middle East
Morocco's optio
gas supply

Energy
OPEC+ likely to
output plan, sou

Energy
Gas flows still o
Russia's pipelin
Poland to Germ

What's Old is New Again – The Re-Introduction of ASM

One does not want to think of proper, robust Cyber Security approaches and tools to be just a part of a temporary fad. But it is sobering to think that Attack Surface Management (ASM) as an identifiable program or approach has only come up in the last year or two. This is a new departure. And its rumored that Gartner may come up with a new quadrant for ASM.

Its Only Logical

But despite the temptation of fixating on point scanning tools for one's Vulnerability Management (VM) solution - it does not take a huge conceptual leap to think it would be easier to effectively run a VM program if one detects and shuts down rogue attack surface exposures even before the incidents start to happen. Smart VM means having a Smart ASM.

For real precision and fidelity, ASM combined with full stack vulnerability coverage is required.