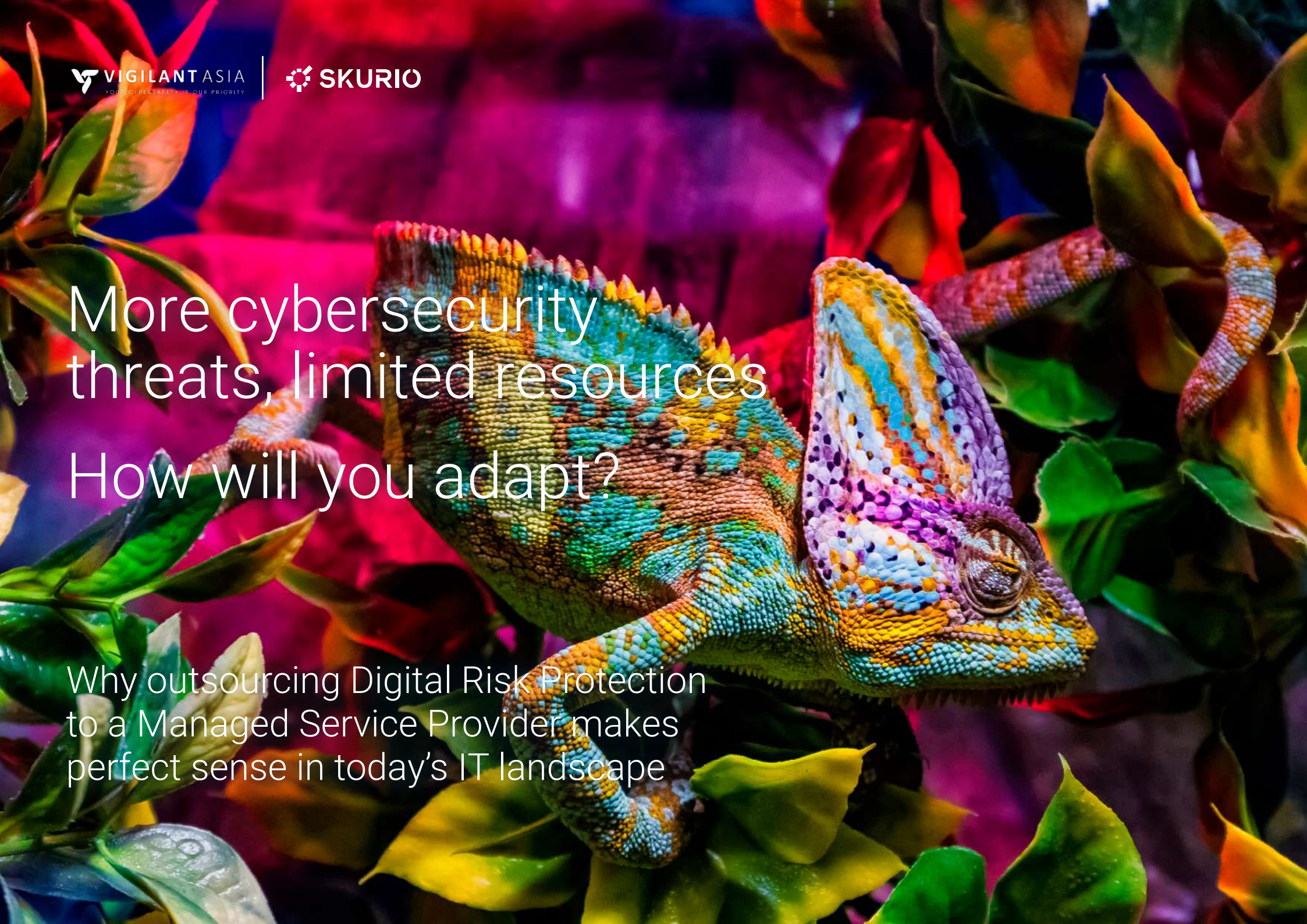

VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY
SKURIO
More cybersecurity threats, limited resources
How will you adapt?
Why outsourcing Digital Risk Protection to a Managed Service Provider makes perfect sense in today's IT landscape

The world has changed

Your cybersecurity service needs to change too

A growing number of businesses are changing their approach to cybersecurity, looking for ways to strengthen their security posture with limited resources. If that sounds familiar, outsourcing Digital Risk Protection (DRP) as a managed service is an excellent option to consider.

DRP involves monitoring for threats and data breaches beyond your network, so you can respond intelligently and focus your attention where it's needed most. It's a perfect fit for the new reality of IT, where much of your data is outside your control.

Great network defences will always be necessary. But now, distributed supply chains, remote working, and cloud/SaaS are just part of the job; a lot of your attack surface is outside that traditional perimeter. It makes sense to be monitoring out there too.

DRP does that monitoring in a planned, consistent, automated way that you can tune to your organisation's specific needs. And at a time when **82% of companies are planning to use managed service providers*** to overcome IT challenges, outsourcing is an easy, intelligent way to maximise the benefits of this technology without putting extra demands on a stretched IT team.

If your IT or security managed service provider has recommended DRP – or if you're considering DRP but don't have the resources to manage it – this short guide is for you.

We'll outline what's changed in cybersecurity and how DRP addresses these issues head-on. Then we'll explain where it fits as part of a managed service and share some hints about finding the right balance for your business needs.

*Source: TechTarget March 2022

VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY

SKURIO

Your data has left the building So how do you protect it?

Lately, cybersecurity has changed in two crucial ways: more of your data is outside your network, and threats are too numerous and sophisticated to keep up with. DRP addresses both issues.

That's because DRP – monitoring for threats and breaches beyond your network – is a perfect fit for the new reality where cybercrime is a well-funded industry while much of your data is outside your control.

Where is the edge of your network?

Right now, your data is likely spread across hundreds or even thousands of systems, suppliers, and devices far from your perimeter. You could even say the perimeter is a thing of the past.

Remote working is one part of that. Users are accessing your resources from everywhere. And according to the UK's Department for Digital, Culture, Media & Sport, around half of all businesses now have employees using their own devices for work. Away from your advice and support, remote users can also be more prone to social engineering, lookalike apps, and failing to install software patches.

But more than that, IT itself has changed. Like any business, you probably rely on third-party cloud services, web applications, and SaaS solutions – before you even think about your users' productivity apps and other Shadow IT. And the chances are that at least some of your data gets shared with your suppliers, who are all facing the same challenges in turn.

Can you keep pace with a trillion-dollar industry?

As an IT professional, you don't need us to tell you cybercrime is no longer about bedroom hackers and badly-worded emails. It's an organised and well-funded industry with a turnover higher than the world's third-largest economy.

With money to invest, criminal gangs can develop more sophisticated attacks – and build automated approaches to carry them out on an industrial scale. This makes it profitable for them to move from hunting big enterprises to targeting smaller businesses and offering "Crime-as-a-Service" to enable new hackers.

Practically, this means one thing: you can expect a higher number of more severe cyber attacks. Already, 64% of companies worldwide have reported being attacked, and the number is growing every 39 seconds. In the UK, fast-rising digital fraud has contributed to fraud overall increasing by more than a third.

More cybersecurity threats; limited resources. How will you adapt? April 2022

VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY

SKURIO

New attacks evade traditional cybersecurity

Many of the fastest-growing cybercrime techniques happen outside the reach of traditional network security. For example:

- **Typosquatting** – Using a lookalike domain to send phishing emails or mimic your actual website
- **Social engineering** – Targeting individuals to obtain personal credentials or divert payments
- **Lookalike apps** – Exploiting confusion around new working practices to infiltrate users' devices
- **Form skimming** – Siphoning data from website forms before it reaches network monitoring

When a breach happens, how will you know?

With more data in more places and new kinds of attacks, a breach is more difficult to prevent and more challenging to detect. According to research by IBM and the Ponemon Institute, it now takes on average 287 days to identify and contain a data breach – and the delay is growing.

That's important because the financial and reputational damage from a breach increases by the day. The faster you can spot and rectify the problem, the more you can minimise its impact and cost – from compromised intellectual property to compensation and fines.

That means you need a way to identify leaked data quickly. You need to evaluate whether it's yours and pinpoint the source, wherever it is in your ecosystem of sites, users, or third party suppliers.

All these challenges are hard to solve using established cybersecurity practices. Great network defences are still important – but once you have those in place, it's time to go one step further and monitor the landscape outside your perimeter.

And that's precisely where DRP comes in.

VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY

SKURIO

Digital Risk Protection: a realistic response to a changing world

You don't control all your data all the time. You can't defend against every attack, and you need to know quickly if there's been a breach. But you can proactively monitor outside your organisation for breached data, as well as potential threats.

That's DRP.

DRP is an essential extension to your conventional network security. It gives your managed service provider the intelligence to prioritise your cyber defences where they're needed most, address vulnerabilities before they're exploited, and respond quickly to limit damage when your data is breached – whether it's from your organisation or via a third party.

VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY

SKURIO

DRP makes your cybersecurity service faster and more complete

For example, your managed service provider can:

Gain tip-offs before attacks happen. Monitoring the surface, deep, and Dark Web can reveal chatter about your organisation and infrastructure – giving time to make patches, reconfigure defences, and fix vulnerabilities before they're exploited.

Spot suspicious domain registrations, websites, and mail servers, such as misspellings of your organisation's name and brands. This lets you counteract potential typosquatting and URL hijacking attacks before they happen.

See when employees' credentials are exposed and respond quickly to limit damage and revoke access. You can also see repeat offenders and train them on good practice and password hygiene.

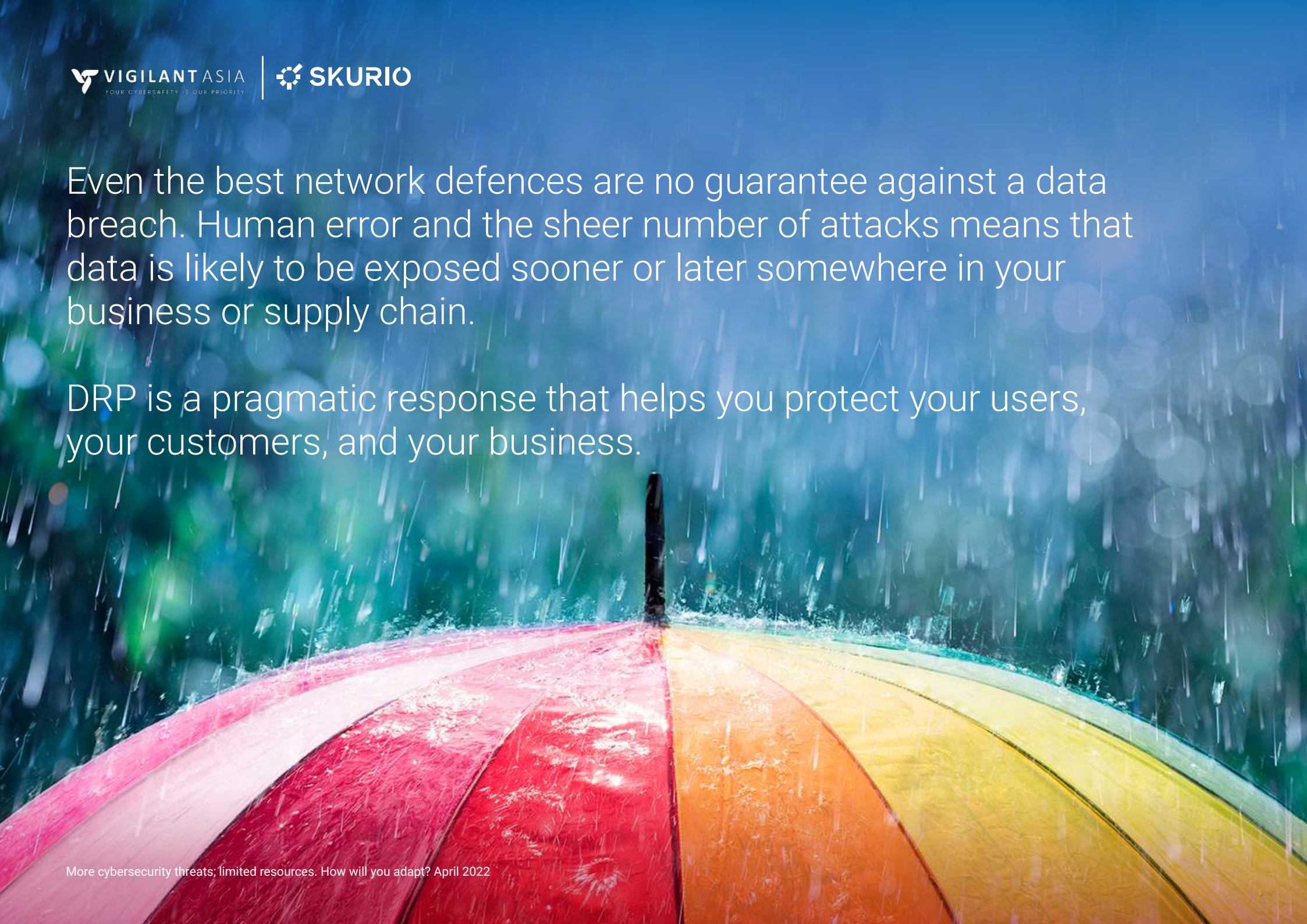
Protect high-risk account users like senior executives, finance colleagues, and IT administrators. In particular, your service provider can prioritise a fast response for the most damaging leaks by monitoring for their credentials.

Discover when sensitive or business-critical information has leaked by monitoring for specific identifiers in your confidential documents, transaction records, or software code.

React quickly when breached customer data is revealed online, helping you reduce reputational damage and costs. You can also report proactively to authorities, potentially limiting fines.

Identify your data, and prove the source of any leaks by digitally watermarking your datasets with dummy records. If cybercriminals use the data for phishing, this method can reveal a leak even before records are shared online.

More cybersecurity threats; limited resources. How will you adapt? April 2022


VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY
SKURIO
Even the best network defences are no guarantee against a data breach. Human error and the sheer number of attacks means that data is likely to be exposed sooner or later somewhere in your business or supply chain.
DRP is a pragmatic response that helps you protect your users, your customers, and your business.
More cybersecurity threats; limited resources. How will you adapt? April 2022

VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY

SKURIO

A perfect fit for outsourcing

For many companies, it makes excellent sense to outsource DRP as a managed cybersecurity service. It's a great way to meet today's cybersecurity challenges without putting pressure on your IT resources. It's also quick and easy – and maximises the benefit from the DRP data.

Outsourcing is not the only way to deploy DRP. With an automated platform, it's perfectly possible to carry out the monitoring in house, with minimal additional training or specialist skills.

But often, a managed DRP service can be a perfect fit. It gives fast, integrated results with minimum disruption to your core IT work – and because it doesn't impact your day-to-day operations, it's quick and easy to implement. If you haven't outsourced cybersecurity before, it's an ideal place to start.

The main reasons companies outsource DRP fall into three overlapping areas: expertise and resourcing, service availability, and the quality of response.

VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY
SKURIO

Minimum impact on IT resources and skills

There is a growing trend for businesses in the Asia Pacific region to outsource their cybersecurity. Often, this is driven by pressures on IT headcount, skills, and costs – and some businesses outsource DRP for the same reasons.

Cybersecurity is famously suffering from a global skills shortage, with millions of roles unfilled. So it's understandable if your IT and security resources are stretched or if you're finding it challenging to hire the people you need.

DRP doesn't take specialist knowledge, but evaluating risk intelligence and responding to alerts does take time. And if you have a limited number of skilled people, outsourcing lets them focus their efforts on other priorities.

You might also find that outsourcing makes budget management more straightforward, with no need to meet a DRP platform's annual subscription costs.

High service availability, sustainable for the long term

With a managed service contract, your supplier is accountable for the reliability and availability of your DRP function. You get the peace of mind of letting them worry about keeping things running smoothly, allowing you to concentrate on what you do best.

As part of your contract, you can negotiate service level agreements (SLAs) to suit your business priorities and provide levels of cover that would be hard to match with a cross-functional in-house team. For example, you could specify a specific response time or obtain 24/7 coverage if you feel it's needed.

Your managed service provider also takes on the planning burden of delivering that service sustainably. It's their job to ensure redundancy for staff availability, sickness, and holidays to give you the cover you need. And recruiting and retaining the correct number of specialists to cover future demand becomes their problem too.

Likewise, outsourcing to a specialist team gives you the best chance of keeping abreast of new trends, threats, and techniques in the fast-moving cybersecurity landscape.

Fast, integrated response

DRP intelligence is only valuable when you can act on it. Often, this involves taking cybersecurity or IT-related action, for example, patching software to address a vulnerability you've seen discussed on the Dark Web, reconfiguring your firewall, or revoking access from a compromised account.

If a managed service provider handles many of these functions for you, integrating DRP into that service will give you a fast, joined-up response.

It's also helpful to view DRP intelligence in the context of the bigger cybersecurity picture. With experience, data signals from your cybersecurity point solutions can give you a better understanding of what's happening and where the actual issues lie.

So it makes sense to have your DRP managed alongside other complementary measures like penetration testing, training, web firewalls, email security, managed threat detection, and endpoint detection and response.

And if the person interpreting the intelligence is a full-time cybersecurity specialist, they'll likely be able to assess potential threats accurately on the spot. If they don't need to wait to talk to an expert, your response will be faster still.

Where your data is a valuable asset, but your IT and security resources are limited, outsourcing gives the opportunity to maximise the benefit of DRP without overstretching your team.

VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY

SKURIO

How to outsource DRP successfully

DRP intelligence can be used in many ways, and no two businesses have the same digital risk profile. Getting the most from your DRP service will depend on choosing a partner – and a service level – that's a good fit for your needs.

It's easy to see why outsourcing cybersecurity is so popular: IT resources are under pressure, experts are difficult to recruit, and just keeping your knowledge up to date can be a full-time job.

DRP is easy to deploy as a standalone, outsourced service – but it can supercharge a managed cybersecurity service. It can help your provider focus and strengthen your defences while their specialists bring the awareness and knowledge to interpret the findings. Centralising your solutions makes it easy to respond to alerts quickly and in a joined-up way.

VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY

SKURIO

Assess your digital risk

The service you get needs to match the reality your business faces. And the trick is working with a partner that can give you the right level of support and protection for your risk level. Factors to consider include:

- **The sector you work in** – Are cyber attacks common in your market, and do you work in an area where a breach would be especially damaging?
- **Your user base and supply chain** – Who could potentially make a mistake that exposes your data? How many are there, where are they and, frankly, how much do you trust them?
- **The quantity of data you hold** – Most commonly, it might be you store data for a large customer base. But it could also be detailed records for each one.
- **The value of your data** – Whether to cybercriminals, to your customers, or you. Criminals might seek records with a high monetary value, but leaking personal details might be more damaging to your customers. Also, consider the importance of critical business information like confidential documents, intellectual property, digital assets and software code.

Find a service that fits

Having taken an honest view of your risk level and how important digital risk protection is to your organisation, it's essential to find a service level to match. Things you might consider when outsourcing DRP include:

- **A broad range of services and SLAs** – Some aspects might be necessary to you, others less so. For example, if it's crucial to show customers and regulators a rapid, proactive response to any breach, you might want to look for 24/7 monitoring. Be sure to devolve authority to rectify an issue when it's spotted.

- **Flexible monitoring that matches your needs** – Ask what types of assets your provider's monitoring can protect beyond the standard user credentials and customer data. For example, you might want to protect confidential business documents, infrastructure, or software code or keep a watch for details about specific high-risk VIPs.

- **A strong understanding of your sector and business** – Ideally, look for a proven track record in your sector. This will help your provider keep an eye on the right threat vectors and respond proportionately to DRP alerts as they arise.

- **Appropriate skill sets and cyber certifications** – The sector you work in might have specific regulatory requirements, or your business could look for particular accreditations. If so, this is a critical part of your selection process.

- **A joined-up approach** – Is the provider well equipped to quickly harness complementary services and solutions when there's a DRP alert? Look for assurance that the vendor can see data in context and respond coherently.

- **Software alliances and integrations** – If your managed service provider can unify multiple data sources to understand an alert or automate some of the resulting actions, it will help them make sense of what's happening and respond fast when needed.

- **A Security Operations Centre (SOC)** – A specialist SOC can enable a service partner to centralise and analyse data feeds through a "single pane of glass", helping security specialists to understand the nature and importance of a threat or leak, and how they can best respond.

However they achieve it, your managed service provider must have a clear plan for how they'll understand your DRP intelligence and take joined-up action when needed.

VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY

SKURIO

DRP is an intelligent answer to a changing world

Outsourcing is a sensible way to deploy it

If you have limited time, resources, or skills in your IT or cybersecurity team, outsourcing Digital Risk Protection is a wise choice. It can help you keep pace with the changing nature of cyber threats without overstretching your team.

Traditional network defences are like locking your building's windows and doors at night or installing an alarm on your premises; they're fundamental to your security. But DRP gives you an extra dimension: a police officer patrolling the beat looking for anything suspicious.

You need that watchful eye on the world outside your perimeter because, increasingly, that's where your data lives.

For many businesses – especially those in the mid-market – a strong relationship with an outsourced IT or security service provider makes DRP more attainable and easier to manage. And if you do it well, it can also maximise the benefit of the intelligence you receive by ensuring any alerts get a fast, coordinated, expert response.

VIGILANT ASIA
YOUR CYBERSAFETY IS OUR PRIORITY

SKURIO

If you'd like to know more about how DRP works, our essential guide to DRP is packed with valuable use cases to help you understand this important new technology

Or, if you'd like to find out how it could benefit your business in particular, we'd love to discuss it with you

Call us today on **+60 (3) 58702252** or email **info@vigilantasia.com.my**

vigilantasia.com.my

Vigilant Asia (M) Sdn Bhd
No 3 Jalan Astaka U8/82 | Bukit
Jelutong 40150 | Shah Alam | Selangor
Malaysia

Vigilant Asia Cybersecurity Pte Ltd
24 Peck Seah Street
#02-08 Nehsons Building
Singapore 079314