SKURIO MSP GUIDE 2023

SKURIO

Guide to Managed Digital Risk Protection services

Create managed DRP service offerings with Dark Web Monitoring, Data Breach Detection and Threat Intelligence solutions.

Create new cybersecurity services with Skurio

Protecting data inside the network perimeter is essential. But these days, your customers use mobile devices, third-party cloud-based applications and distributed supply chains, so their data lives outside of their network more than ever before. So, traditional cybersecurity approaches like endpoint protection, intrusion detection, and network traffic analysis are no longer enough to defend an organisation against data loss or targeted threats, particularly if one of their supply chain partners is hit.

Skurio can help you mitigate your customers' risk from cyberattacks wherever their data lives.

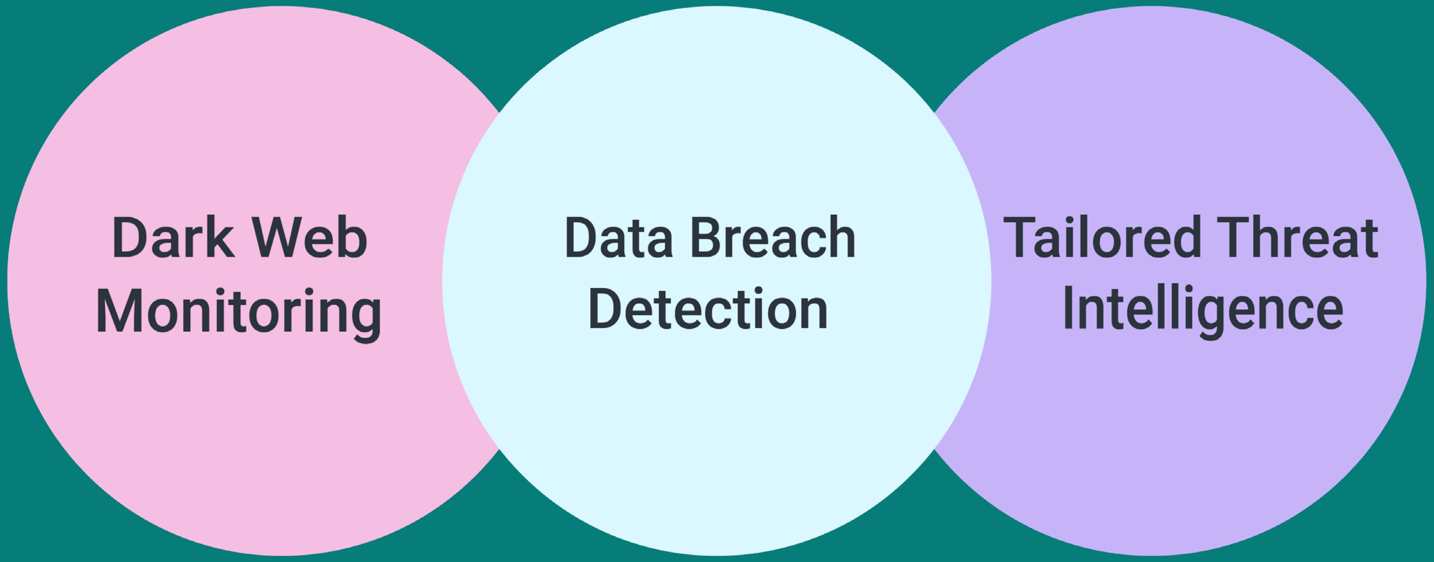
Managed Digital Risk Protection (DRP) services is an exciting new security category that is easy to sell into your existing customer base, increasing monthly recurring revenue (MRR), retention and customer satisfaction. According to Future Market Insights, the global DRP market was worth $1.3 billion in 2022.

Skurio's multi-tenant SaaS platform brings this advanced capability to organisations of all sizes in partnership with Managed Service Providers (MSPs).

What is Skurio Digital Risk Protection?

DRP helps protect an organisation from cyber threats. It does this by monitoring for cyber threats and exposed data on the surface, deep and Dark Web. When breaches and threats are detected sooner, remediation is faster, reducing the risk of further data breaches and cyberattacks.

The Skurio DRP platform combines Dark Web Monitoring, Data Breach Detection and Tailored Threat Intelligence



Skurio automatically monitors for exposed data and cyber threats and supports many use cases. Some suggested service offerings, such as Core Managed DRP services, use fully automated monitoring of domains, emails, and IP address information to cover essential use cases like leaked credentials and brand impersonation. An Advanced Managed DRP service adds powerful keyword searches, specialist data sources and analyst services to maximise risk reduction. As an MSP, you can select and bundle use cases to meet the specific needs of your customers, or to integrate with or enhance your existing services.

Why partner with Skurio?

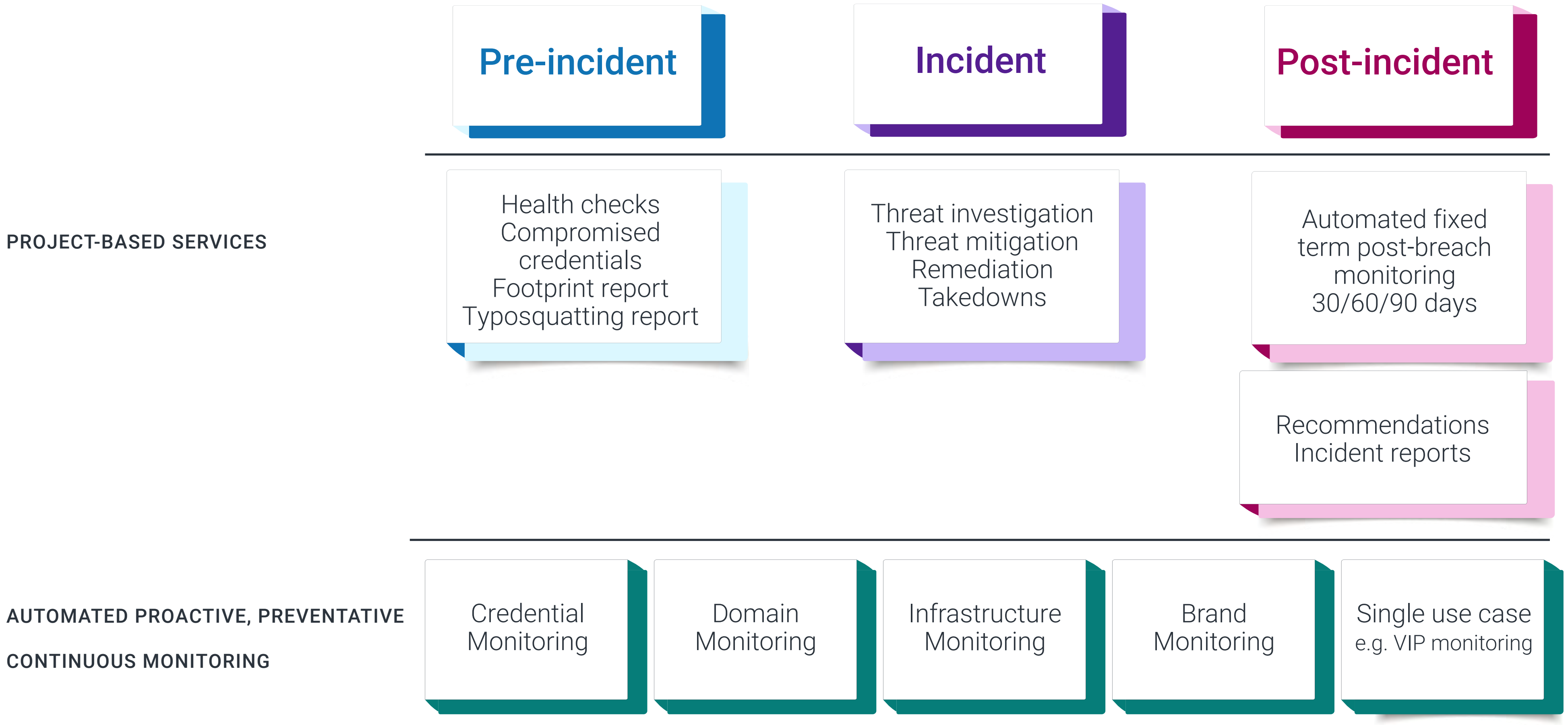
Skurio has been at the forefront of threat intelligence for 12 years, providing specialist tools for automated data monitoring across the surface, deep and Dark Web. The Skurio DRP platform helps MSPs to implement new services quickly and offers many advantages. You can:

- Respond to growing customer demand for Dark Web Monitoring services
- Expand your services portfolio to enhance customer satisfaction and build trusted advisor status
- Deliver affordable services to any size of end-user, from SMBs to large enterprises and public sector
- Create highly profitable revenue streams from one-off project work or ongoing monthly monitoring services

The Skurio platform is easy to use and highly automated. It's operationally very efficient, and you don't need specialist resources to set it up.

Skurio MSSP packages are commercially attractive whether you have one customer or hundreds. You can start small, and you can pay-as-you-grow.

The DRP services lifecycle



Pre-incident

Incident

Post-incident

PROJECT-BASED SERVICES

Health checks
Compromised credentials
Footprint report
Typosquatting report

Threat investigation
Threat mitigation
Remediation
Takedowns

Automated fixed term post-breach monitoring 30/60/90 days

Recommendations
Incident reports

AUTOMATED PROACTIVE, PREVENTATIVE CONTINUOUS MONITORING

Credential Monitoring

Domain Monitoring

Infrastructure Monitoring

Brand Monitoring

Single use case
e.g. VIP monitoring

Cybersecurity incidents often trigger the need for project-based services to investigate and remediate threats. Once an incident has been dealt with, there's also an opportunity to create monthly recurring revenue with managed DRP services that monitor for and proactively identifies data breaches. And, being aware of and responding to data breaches in near real-time should prevent further, more sophisticated cyber-attacks from happening in the future.

Project-based services

You may already be providing your customers with pre, during or post-project-based services, but if not, here are some project-based services you can add to grow your business with DRP.

Pre-incident project-based services

Health check

Understanding the digital exposure of your customers is the first step to reducing their digital risk and preventing bad actors from using exposed details to mount an attack. For example, your team could conduct research to show potential threats and essential data that could be used against them if hackers target their organisation.

Typosquatting reports

Criminals impersonating customer brands can make web links and emails look genuine with a domain that closely resembles the customer's domain. Investigation and takedown services can remove threats and generate demand for ongoing typosquatting monitoring.

Compromised credentials

A credential breach from any Cloud application your customers use can pose a significant threat to their systems. For example, 60% of email system hacks* are made possible by breaches of credentials from 3rd party apps. If their corporate emails are included in a breach, you can investigate the alert notifications and provide an analyst assessment with advice on mitigation.

Footprint reports

Our digital footprint reports let you provide your customers with historical data breach information for their corporate email domain(s) to help you prospect and sell.

* https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/

Incident response project-based services

Your analysts can carry out threat remediation using the Skurio platform to identify and resolve threats to your customers' IT systems. You'll provide a customised statement of work based on their needs, including an agreed estimate of hours and costs upfront.

Threat investigation

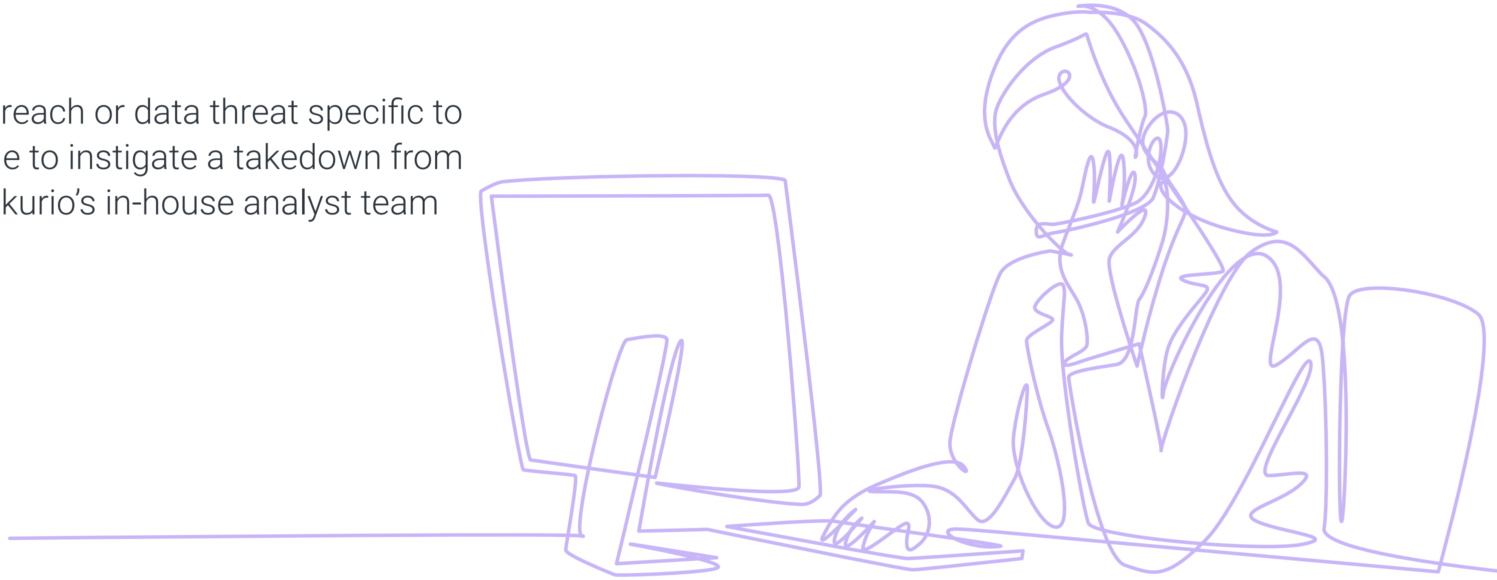
If the Skurio platform detects exposed data or potential cyber threats, your team will be there to help. You'll provide a customised statement of work based on their needs, including an agreed estimate of hours and costs upfront.

Remediation

Your analysts can carry out threat remediation using the platform to identify and resolve threats to your customers' IT systems. Again, you'll provide a customised statement of work based on their needs, including an agreed estimate of hours

Takedowns

Where possible, once you've identified a breach or data threat specific to your customer's business, you may be able to instigate a takedown from paste bins or social media, for example. Skurio's in-house analyst team are also available to help here.



Post-incident project-based services

Your analysts can carry out post-incident reporting and recommendations using the Skurio platform to ensure that lessons are learnt and any security gaps are addressed. Again, you'll provide a customised statement of work based on their needs, including an agreed estimate of hours and costs upfront.

Incident reports
Whether a data breach or cyber threat has been detected, your analysts can provide an expert view of that incident. Concise details of precisely what happened, when and who or what was involved is the starting point for any investigation.

Recommendations
Once an incident has been investigated and remediated, your analysts can provide recommendations for customers to implement in the short and medium term to prevent an attack of the same type from happening again.

Fixed period monitoring
Give your customers piece of mind post an incident investigation and remediation. Offer them fixed-day monitoring packages for 30/60/90 days.

SKURIO

Automated Credential Monitoring Managed Service

Our Credential Monitoring Managed Service provides proactive monitoring and reassurance for small to midsize organisations looking to improve their cybersecurity posture. This service continuously monitors the Dark Web, hacker forums, paste and bin sites looking for company credentials information using your customer's domain names. Our automated software platform combines continuous, 24/7 monitoring with real-time alert notifications. This ensures your security team is quickly alerted to any new data breach - minimising the impact of any incident.

Service features:

- Detect new credential leaks specific to your customer's organisation being posted on the surface, deep and Dark Web forums
- Prevent account takeover of corporate, cloud or shadow IT systems used by your customer's staff by detecting leaked corporate credentials and trigerring remedial actions

Time to onboard
1-2 hours

Management per month
1-4 hours

Managed services elements

Initial alert configuration

Initial report to include historical searches and credentials reports

Ongoing monitoring

Monthly/quarterly reporting

Incident response & investigation

Remediation and recommendations

Monitoring for:

- Corporate email domains

Automated Core Managed DRP Service

Our Core Managed DRP Service provides your customers with all the service elements of our Credentials Monitoring service. You will incrementally have the additional service coverage listed below.

Service features:

- Detect and monitor newly registered 'spoof' domains impersonating their organisation and brands, minimising the risk from phishing and fraud
- Help your customers protect their staff by protecting them from phishing attacks from typosquatting domains

Time to onboard
2-8 hours

Management per month
4-12 hours

Managed services elements

Initial alert configuration

Initial report to include historical searches and reports; credentials and typosquatting domains

Ongoing monitoring

Monthly/quarterly reporting

Incident response & investigation

Remediation and recommendations

Monitoring for:

- Corporate email domains
- Web & applications domains
- Typosquatting
- Public IPs

Automated Advanced Managed DRP Service

Our Advanced Managed DRP Service provides your customers with all the service elements of our Core DRP service. As well as the Core services, you will have the additional service features listed below.

Service features:

- Discover attempts to use your customer's brand fraudulently, reducing the risk to their reputation and margins
- Allow for early detection of threats to their VIPs - i.e., protect level plans, personal information of the VIP and possibly close relatives' personal information
- Uncover breaches of critical data through supply chain leaks
- Find fingerprints of sensitive corporate data - commercially sensitive documents, datasheets or pricelists

Time to onboard
2-5 days

Management per month
8-16 hours

Managed services elements

Initial alert configuration

Initial report to include historical searches and reports; credentials and typosquatting domains

Ongoing monitoring

Monthly/quarterly reporting

Incident response & investigation

Remediation and recommendations

Additional monitoring for:

Brand and VIP

- Company
- Threat intel
- Partner logins
- High-risk account

Business critical information

- Sensitive data
- Fake/grey market
- Fraud

Data breach detection

- Databases
- Customer emails

Key benefits of partnering with Skurio

Skurio realises that one size doesn't fit all. We can work with partners of all sizes and levels of security maturity. The table below illustrates just some examples of partner types and how a relationship with Skurio would benefit them.

MSPs

Currently offering migration to Cloud services, IT support, or IT helpdesk

What Skurio offers:

Low cost, entry-level monitoring, with a highly automated solution that doesn't need skilled staff to set up or operate

MSSPs

Project-based security specialists offering pen testing, vulnerability assessments or incident response

What Skurio offers:

Ability to add SaaS-based monthly recurring revenue into the mix

Automation boosts the efficiency and effectiveness of your existing staff

MSSPs offering XDR

Already providing EDR, MDR or XDR services and familiar with the concept of monitoring and incident response

What Skurio offers:

Quick and easy integration into cybersecurity stacks to extend the attack surface coverage offered to your customers

Be more proactive with DRP, detecting threats before they hit enterprise security points

MSSPs offering DRP

Already selling Dark Web Monitoring, Cyber Threat Intelligence, or both to enterprise customers

What Skurio offers:

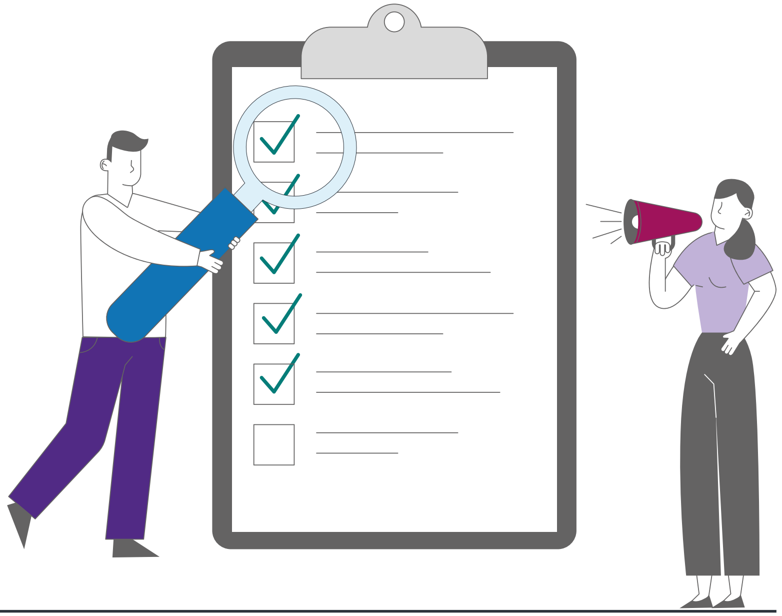
Automated data collection so your analysts focus on investigation and remediation

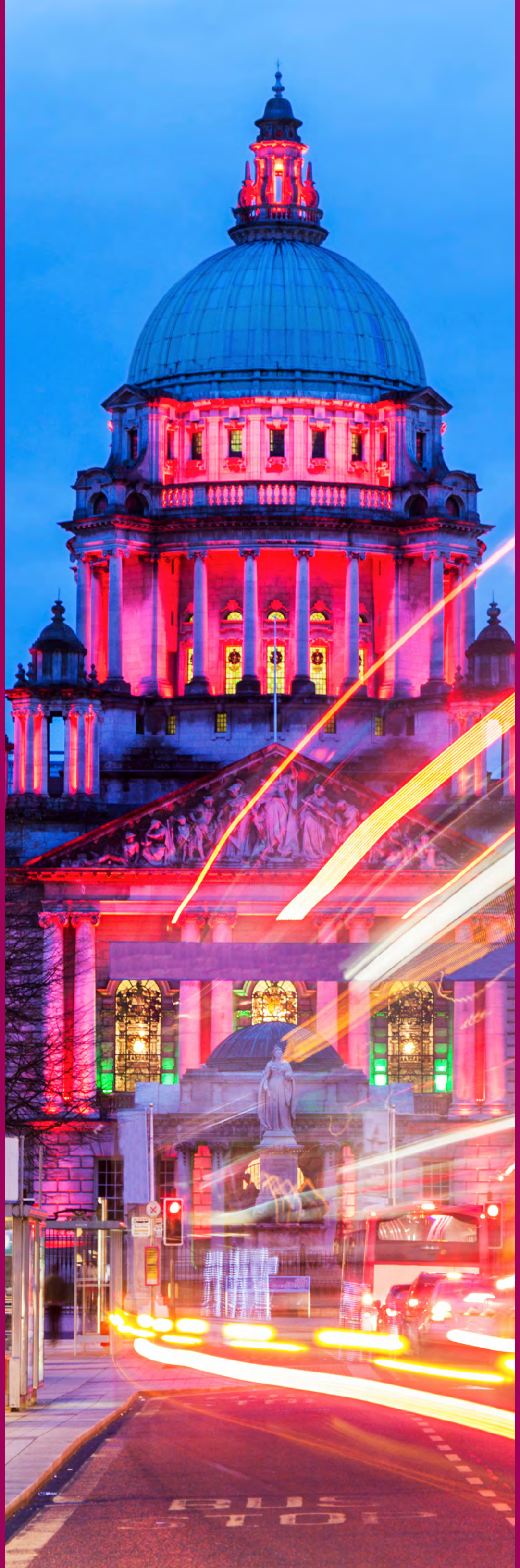
Multiple use cases with just one platform

Skurio's flexible commercials can make sense with just one key customer

Partner programme elements

- ☑ Assistance with demonstrations and RFPs
- ☑ Support with opportunity development
- ☑ Marketing campaigns in a box
- ☑ Choice of subscription periods
- ☑ Flexible, pay-as-you-grow based commercials
- ☑ Service creation tailored to your customers
- ☑ Maximum ROI from your subscription
- ☑ Sales enablement materials
- ☑ Pre-sales reports with historical data breach information
- ☑ End user demand generation
- ☑ Sales and technical training curriculum
- ☑ REST APIs for your SIEM, SOAR, ITSM
- ☑ Deal registration





SKURIO

About Skurio

Skurio, the innovative cybersecurity software company, helps organisations protect themselves from digital risks. Our Digital Risk Protection platform combines automated, round-the-clock monitoring of the surface, deep and Dark Web with powerful analytics capabilities for cyber threat intelligence.

Founded in 2011, Skurio is headquartered in the UK with an international partner network. Skurio's highly skilled team of security analysts work at the leading edge of business threat intelligence and digital risk protection, providing organisations with the support they need to extend their in-house expertise. Our partner and distribution network serves hundreds of customers in 33 countries.

Book a session to find out how the Skurio DRP platform can help you grow your business.

Contact partner@skurio.com or visit our website.

SKURIO LTD | ARTHUR HOUSE | 41 ARTHUR STREET | BELFAST | BT4 1GB +44 28 9082 6226

www.skurio.com info@skurio.com