Selling Digital Risk Protection Solutions with Skurio

WHAT IS DIGITAL RISK PROTECTION?

DRP is an umbrella term for data breach detection and cyber threat intelligence; monitoring for data that has been breached on the surface, deep and Dark Web, then finding and investigating threats specific to the business.

- Organisations traditionally spend budget on network-centric solutions to protect the network and the data inside it i.e. firewalls/endpoint protection
- Most data breaches are due to human error and not malicious attacks (80% are human error!), so traditional security solutions are no longer enough
- The network perimeter is constantly evolving and changing, especially now with more employees working remotely. A company's data is its most valuable asset, they should be protecting it, wherever it lives

THE NEED FOR DIGITAL RISK PROTECTION

Four kinds of data	Stored in three places	Two types of breach	One Solution
Login Credentials	Inside your network	Malicious attack	**Skurio Digital Risk Protection** **D**etect **A**lert **T**ake action **A**nalyse & Address
Assets and Infrastructure	In your supply chain		
Personal data		Human error	
Business critical information	Outside of your network		

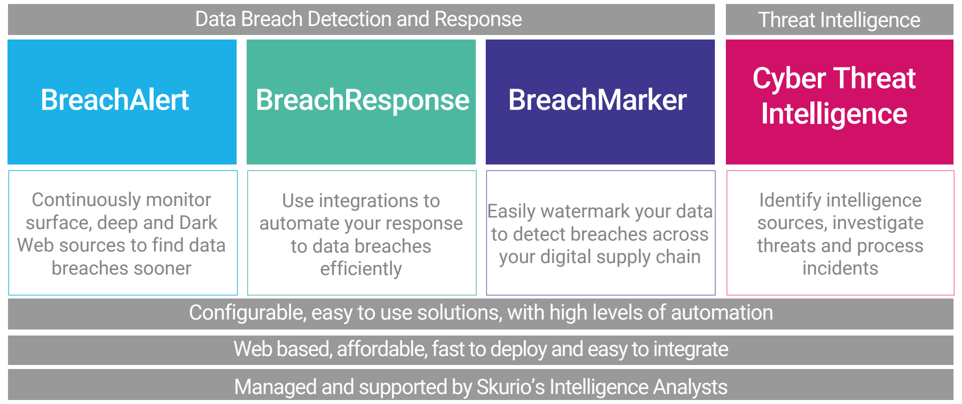
THE SKURIO SALE

The Skurio sale is driven by the desire to reduce the risk of data breaches and external threats. By understanding if business data or threats to the business appear outside of the firewall, the organisation can benefit from:

- Faster mitigation and remediation to reduce impact and further threats
- Reduced costs by minimizing operational impact and reputational harm
- Improved regulatory compliance and reducing financial penalties

SKURIO DIGITAL RISK PROTECTION SOLUTIONS

- We provide digital risk protection.
- We protect against data theft and cyber threats
- We minimise the impact of data breaches and cyber threats.
- We continuously monitor for data outside the firewall; on the surface, deep and Dark Web
- We provide instant alerts when company data appears where it shouldn't



Data Breach Detection and Response

Threat Intelligence

BreachAlert: Continuously monitor surface, deep and Dark Web sources to find data breaches sooner

BreachResponse: Use integrations to automate your response to data breaches efficiently

BreachMarker: Easily watermark your data to detect breaches across your digital supply chain

Cyber Threat Intelligence: Identify intelligence sources, investigate threats and process incidents

Configurable, easy to use solutions, with high levels of automation

Web based, affordable, fast to deploy and easy to integrate

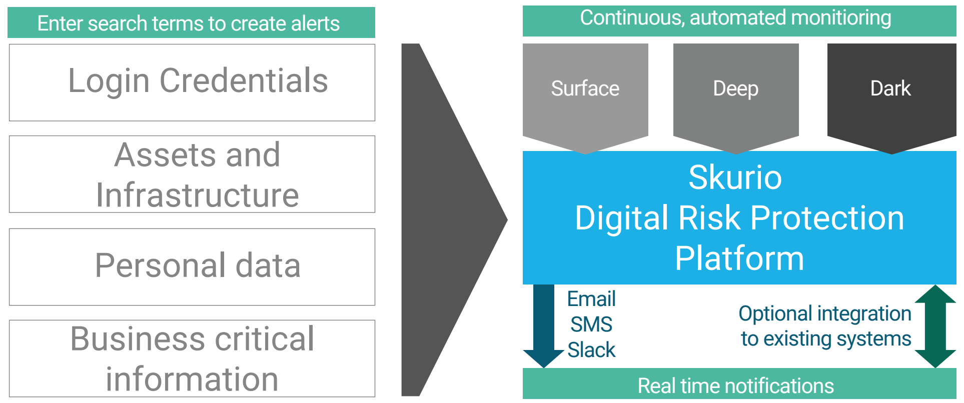
Managed and supported by Skurio's Intelligence Analysts

HOW DO WE DO IT?

- Skurio is like a security searchlight. If business data moves, we illuminate the potential danger
- We focus on protecting data: user credentials, assets and infrastructure details, personal information and business critical data
- We detect breaches of this data with automatic and continuous surface, deep and Dark Web monitoring.
- We provide alerts via SMS, email or API so remedy action can be taken

HOW IT WORKS

- Traditional approach: protecting assets within the network
- Our approach: a SaaS solution checking for data leaks, with automated crawlers and scrapers looking for business data outside the network
- Set up a list of important keywords and search terms based on what is important for the organisation to create monitoring alerts
- Carry out historical searches to investigate incidents



Enter search terms to create alerts

Login Credentials

Assets and Infrastructure

Personal data

Business critical information

Continuous, automated monitoring

Surface

Deep

Dark

Skurio Digital Risk Protection Platform

Email
SMS
Slack

Optional integration to existing systems

Real time notifications

	CUSTOMER CONCERN	RESPONSE
Scepticism	We haven't found any threats during our trial and our footprint report was clean.	Even if your network is safe at the moment, threats could occur at any time. Human error is involved in 80% of data breaches with common examples including poor password management, mis-addressed emails, phishing attacks and mis-configured devices. More importantly, breaches can originate from a partner or 3rd party service in your digital ecosystem, or from online services your staff have signed up for which you no nothing about. Footprint reports only look for breaches of emails for your own domain - our full service supports important use cases like customer data monitoring.
	We are too small to be a target	SME's are suffering from Ransomware and Phishing attacks because they are seen as relatively easy targets with less sophisticated defences and less staff awareness than large enterprises.
	We don't have anything valuable enough to make us a target	Most Ransomware attackers aren't aware of your company profile, simply attack an easy target. They are more likely to disrupt access to systems and data then attempt to steal data. What would be the business impact if you lost access to your systems (CRM, Accounts, e-commerce, self-serve portal, production control) or you lost the systems' data?
	We don't want to report data breaches	If you ignore a data breach and the information is sold or shared, you will need to consider to reputational damage as well as the possibility of increased regulatory fines because you didn't take steps to protect your data.
	If I don't know about a breach, then I won't be fined for it.	Robust data breach detection is a fundamental component of GDPR. The big fines get levied on companies who don't take privacy and security seriously. As more companies adopt Digital Risk Protection solutions like Skurio's, it's going to become an expected part of your defence – and being proactive will certainly help you reduce the impact of any breach by detecting it quickly and fixing it.
	I have been breached - if I can't work out where and how I've been breached, what good is this to me?	By alerting you in real-time, you can start to investigate the incident and stem the cause. You can use our intelligence analysts, or a third-party incident response partner, to investigate and try and identify the source of the leak It's often possible to identify the site that this data might have come from with a simple bit of analysis. Skurio's tools provide as much context as possible, including the full text of the breach where that's available. By being proactive, you'll be demonstrating that you're taking things seriously, which can definitely help mitigate your position if you end up facing a GDPR fine.
	Leaked credentials are not important to us and we use 2FA, so the service is not relevant.	That's great – although bear in mind that even if your own core network is very well secured, your staff may well be re-using those same passwords on other systems you can't control – hackers are increasingly using SIM Swap methods to bypass 2FA. What could be the consequence if someone got into your corporate (or CEO's) social media or LinkedIn accounts using those passwords? Skurio's platform provides protection of all your digital assets, including, Source Code, IT Infrastructure, Employee PII, Customer PII & Financial PII, Databases, Intellectual Property and more.

	CUSTOMER CONCERN	RESPONSE
Resource constraints	We are upgrading our network and end point defences and will look at this later	Do you believe you will be better protected once that’s completed? Whilst you carry out the work you have an even greater exposure and need for Skurio, as you are even more likely to be breached now than when you finish your upgrades.
	The price is too high	Recovery from an attack can be considerable. Moreover - GDPR fines can be mitigated if Dark-Web monitoring has been deployed and built into your incident recovery processes. Starting with a basic package can help you keep cost down while proving the value of the service.
	We don’t have the staff to respond to the alerts.	We can provide a managed service which takes the pressure away from your IT Department. We will receive your alerts, triage to eliminate false positives, alert you, provide advice on degree of urgency and suggest remedial actions . With ‘Ask An Analyst’ and Take-Down services now included can support departments with limited resources.
Competition / Alternative approach	I can get this free of charge from HIBP.	HIBP is a great service, which is why we include it alongside our own data – we also make it much more convenient for you to consume. The HIBP service only works for reported credential breaches and doesn’t provide additional context -for example, the password which was exposed in the breach. HIBP represents a few hundred data breaches. We have more than 2.2 billion records in our index, and collect around 10 million new documents a month from the surface, deep and dark web, any of which could contain information relevant to you. Skurio provides protection of all your digital assets, including, Source Code, IT Infrastructure, Employee PII, Customer PII & Financial PII, Databases, Intellectual Property and more.
	We use a competitor	Great to hear. Let me ask you, do they provide automated monitoring? Can they track any data or do they focus on basic use cases? Our platform also gives access to analyst resources - is this included with your current solution?
	There are products from vendors like Dark Trace and Acronis which can prevent sensitive data from being leaked from the network like credit card details. So why do we need your service?	Data Loss Prevention systems are great, but they can’t catch everything, and much of your data is probably outside the perimeter of your DLP. For example, if data leaks from one of your supply chain partners, or a cloud app which has legitimate access to that information. Vulnerabilities like Magecart or typosquatting attacks using fake sites can also mean you’re your customer data gets ‘skimmed off’ before it even hits your systems, with no evidence of data leaving your systems. That’s what happened to British Airways – no amount of DLP would have helped there. There is also plenty of old data circulating online which could prove damaging to you if it starts being leaked or sold online – for example the recent incident with Foxtons.

	CUSTOMER CONCERN	RESPONSE
Trust	Can you guarantee to detect all data breaches?	The cyber-threat landscape is continually changing, so no individual supplier could make this claim. We continually update our sources through customer suggestions as well as our own research.
	Do Skurio cover all of the Dark Web?	No, but we don't need to. We focus on monitoring the core sites where data is monetised and shared.
	What examples can you show me about success stories around how the information Skurio has provided has helped customers to remediate.	Breast Cancer Now had suffered a previous breach through unauthorised access to a staff email account. Skurio's platform showed them that the same password had already been exposed in a previous breach – if they had been running it at the time, they could have avoided the incident. One of Skurio's banking customers is regularly targeted by hacktivist groups, who carried out a successful DDOS attack in 2018 which took their systems out of action for 2 days. Since deploying the Skurio service, we have detected chatter in hacktivist forums planning these attacks, allowing the customer to temporarily increase Web Application Firewall levels to survive the period of the attack.
	Why would I buy a tool which tells me I've been breached but doesn't prevent me from being breached?	Skurio can stop you being breached by identifying external threats which could be used to get into your systems or steal your data – for example, vulnerabilities in your apps and systems being discussed on a hacker forum, or staff credentials leaked from a third party site. Many breaches only emerge months or years after the security incident which caused them. With the introduction of our new typosquatting services, Skurio can provide additional, pre-attack intelligence to help you business and your customers from being targeted.

WHO ARE OUR CUSTOMERS?

Users -	Threat Analyst | Security Operations | Data Privacy
Buyers -	CISO | CIO | CEO | CRISKO | CFO
	IT Managers and Directors
Customers-	Breast Cancer Now | BearingPoint
	The Gym Group | Cifas | Rubix

GET IN TOUCH

email:	partner@skurio.com
phone:	+44 28 9082 6226
web:	skurio.com

WHAT SETS SKURIO APART?

AFFORDABLE	Low entry point and generous search volumes. Great packages and no hidden extras.	EFFICIENT	Skurio data collection is highly automated and is easily configured to remove unnecessary noise.	SOURCES	Comprehensive monitoring of surface, deep and Dark Web with swift onboarding of new feeds.
EASY TO USE	Skurio is quick to deploy and easy to use. No need for prior experience or skills.	USE CASES	Skurio offers an unbeatable range of use cases includng brand and customer data monitoring.	SUPPORT	In-app ‘Ask-an-Analyst’ and Takedown requests. Expert intelligence analyst service packages.

SKURIO

- Channel focused
- Cost effective
- Use case flexibility
- Specialist use cases
- Customer focused analysts

DIGITAL SHADOWS

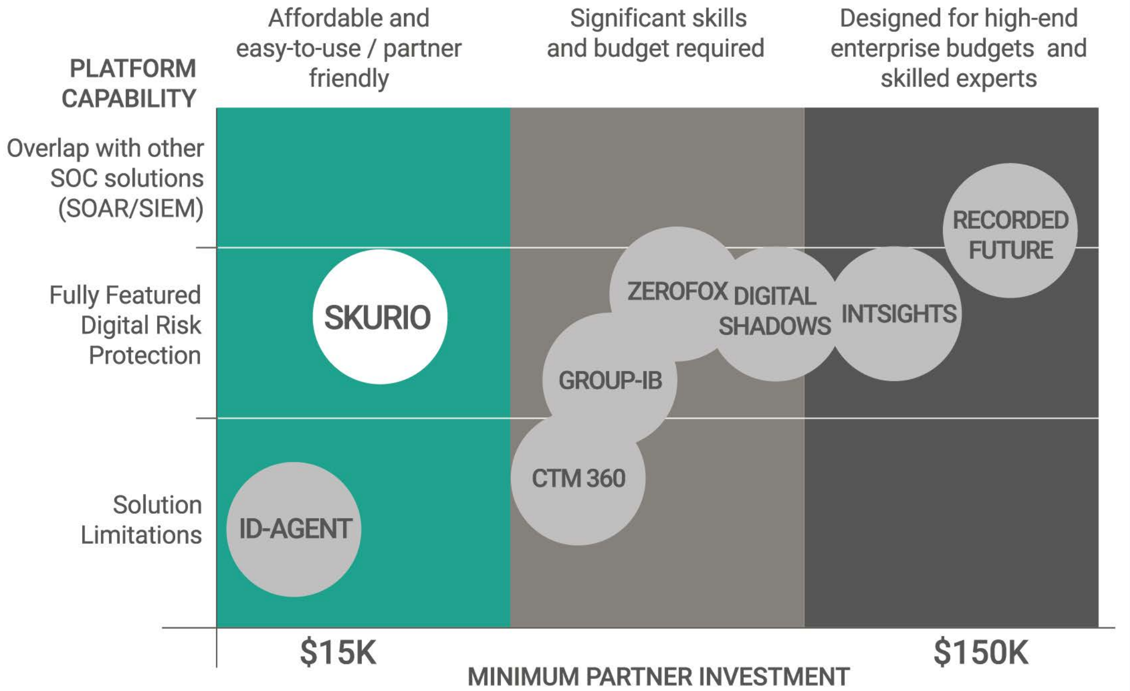
- Variable customer service
- Reliance on manual intelligence curation
- Inefficient use of skills
- Analysts focus on threat types not customer needs

SKURIO

- Fast, simple onboarding
- Cost effective
- Responsive data collection
- Complimentary to other SOC solutions
- Analytics/dashboards

INTSIGHTS

- Poor high-level dashboard
- Slow to bring new feeds and functions on board
- Complicated onboarding
- Buyers pay for capability they have in SOAR etc.



SKURIO

- Cost effective packaging
- Easy to use but full DRP
- Use case flexibility
- Specialist use cases
- Commercial flexibility

ID-AGENT

- Not GDPR compliant
- Low entry price but hidden costs for extras
- Very limited CTI features
- Compulsory multi-year contracts

SKURIO

- Better alerting
- Cost effective
- Use case flexibility
- Specialist use cases
- Channel focused

RECORDED FUTURE

- Highest sector pricing
- Requires specialist skills
- Prioritise direct business over channel
- Extensive feed coverage generates too much noise

SKURIO

- Single solution
- Cost effective
- Use case flexibility
- Specialist use cases
- Customer focused analysts

ZEROFOX

- Expensive to scale: costs for searches and feeds
- Lots of false positives
- Rely on junior analysts
- Manual intelligence
- Multiple systems