

# SALES BRIEFING: DOMAIN MONITORING SOLUTION

Not for direct distribution to your customers or prospects

## WHAT IS DOMAIN MONITORING?

Domain Monitoring combines **Typosquatting** detection with **DNS Monitoring** to reduce the risks from brand impersonation.

Typosquatting, or URL hijacking, is a technique used by scammers to exploit mistyped URLs or to create a domain that impersonates a legitimate business. They do this by registering domain names that are very similar to the website, but with small typos, misspellings or special characters. Domains may be registered but not used immediately. If this is the case, they can appear to pose no immediate threat, but should be monitored in case a website or mail server is added at a later date.

## WHY SHOULD YOUR CUSTOMERS CARE?

According to Google Search, it found around 40 billion web pages of spam and malicious content every day last year - a six-fold rise from 2021. Domain registration and hosting is low cost, quick and easy to set up. So, typosquatting attacks can be targeted at any business. Typosquatting domains can be used to create convincing websites, emails and links to fool customers. They can be used in a variety of scams and cyber threats, including:

- **Phishing & pharming**
- **Payment diversion**
- **Brand impersonation**
- **Extortion**
- **Spreading malware**
- **Traffic monetisation**

## WHAT ARE WE SELLING?

**Skurio Digital Risk Protection** is a subscription based SaaS solution that monitors the surface, deep and Dark Web to detect data breaches and cyber threats outside the network that are specific to a business. The platform includes two key features to address Domain Monitoring as well as Analyst Services to provide incident support.

**Typosquatting Monitoring** - Skurio scans daily domain registrations and alerts customers when their brand terms are used. With this, businesses get timely notification of potential threats that could impact their customers.

**DNS Monitoring** - detects changes to domain name system records for any domain under investigation, including the addition of a live site with IP Address (A or AAA) record or an email facility with the addition of a Mail Exchange record (MX).

**Analyst Services** - Skurio also provides in-app access to request threat analyst advice and request investigation and takedown services\*. Takedowns are possible if a domain proves to be malicious and there is sufficient justification.

## WHY SKURIO?

Skurio is an ideal Domain Monitoring solution to prevent typosquatting attacks:

- Cost-effective
- Easy to use and on-board
- Doesn't require specialist skills and needs minimal resource
- Has tools to optimise search terms to reduce false-positives
- Teams can monitor domains that don't pose a threat initially
- Backed up with specialist threat analyst services\*

## QUALIFYING QUESTIONS

- Do you check to see if anyone has registered similar domains to yours?
- As a supplier, are you confident your domain protection measures would satisfy a risk assessment?
- Did you know that if you're not monitoring your domains you are open to ransomware, phishing and business email compromise attacks?

## OBJECTION HANDLING

- ? We could simply register every permutation of our domain to avoid this
- ? We don't need a solution for this, there are free tools that we could use
- ? We don't have the time or resources to spend on a solution that generates more alerts
- ? We don't want to invest in a platform just for Domain Monitoring

## HOW TO RESPOND

- ☑ The possibilities are almost limitless, so this would be resource-intensive and expensive
- ☑ They would require regular review so this wouldn't be practical
- ☑ Alerts are highly personalised and can be optimised to reduce noise
- ☑ Skurio is not just for Domain Monitoring, it covers a lot more use cases

## OTHER RESOURCES

- You'll find the Domain Monitoring Campaign in a box and tailored email copy on the Partner Portal at [partners.skurio.com](https://partners.skurio.com)
- The Domain Monitoring Playbook provides a step-by-step guide to implementing this capability



\*Site takedowns are charged separately from subscription services