The essential guide to Digital Risk Protection

skurio.com

SKURIO

Introduction

The need for Digital Risk Protection

The need for Digital Risk Protection

For many businesses, the last few years have changed the information security landscape significantly.

- New data privacy regulations require increased compliance and diligence, with significantly heavier penalties.
- Digital transformation and Cloud services have increased the complexity of IT infrastructure, making you reliant on multiple third parties to keep your data safe.
- The threat landscape has increased in breadth and depth with more attacks, more kinds of attacks and more targeted attacks.
- Consumers are increasingly aware of high profile data breaches, making privacy and security key to maintaining customer trust and brand loyalty

All this means that protecting your data within your network alone is no longer enough. You need to protect your data. Wherever it lives.

You have 4 key types of data to protect

To remain relevant and competitive, your business has digitally transformed and is data-driven in almost every aspect. Data is used to help define strategy, improve customer experience, accelerate research and development, drive recruitment and much more. If this data is leaked, stolen or given to competitors or criminals it can impact your business significantly. This data falls into four key types:

- Details about your infrastructure and software that can be used by bad actors to mount a cyber attack against you
- User credentials - login details and passwords for any systems used
- Personal information (PII) about your staff, customers or other individuals your organisation works with
- Business critical or commercially sensitive data which is used to provide services, run or organise your business

- IT infrastructure
- User credentials
- Personal information
- Business critical

Your data lives in 3 places

In the past, you knew precisely where your data was. Today, your data is everywhere and it lives in three types of locations.

- In your network – either on premise or Cloud hosted
- In your digital supply chain – with partners or on 3rd party apps
- Outside the business – on individual devices or surface, deep and Dark Web sites

Keeping control of on-premise data is straightforward enough. No doubt, you already have systems in place to manage data security inside the firewall. Cloud security adds additional process and complexity. But, when data leaves the business, things start to get tough. Requiring suppliers to conform to standards is a good first step; on-going enforcement is harder. Not least because your partners and suppliers will also be reliant on third party suppliers themselves; only increasing digital risk further. And to top it all, data could be stored on devices or shared on emails using insecure networks. All of this means that your data could end up in other locations without your permission, your knowledge or your protection. How do you keep up?

Inside your network

- On premise
- On private Cloud

Inside your supply chain

- Supply chain partners
- 3rd party apps

Outside your business

- Devices
- Shadow IT
- Surface, deep & Dark Web

There are 2 kinds of data breach

There are two main ways that data breaches can occur

The first is human error. Staff who work for you or your partners can accidentally lose data. A mis-addressed email or lost phone incident can happen to any business. Information incorrectly distributed or lost is the biggest cause of personal data breaches in the UK.

The second type of threat comes from a malicious attack. These can take many forms depending on the motivation for the attack, which could be to harm to your reputation, or operations or simply for financial gain. Bad actors could even include a former employee holding a grudge. Even if you have fantastic security and faultless processes, your business can still be at risk of attack through your supply chain.

Human error

- Wrong email address
- Lost device
- Data theft

Malicious attack

- Phishing
- Hacking
- Ransomware
- Ex-employee

There is one universal truth: Most businesses only focus on protecting data inside the network.

How do you know if your data is already out there?

Chances are you won't. That's because most businesses use one type of security solution. That is, security solutions that are focused on defending the network and data from external threats. And this is where Digital Risk Protection comes in – looking for your data and threats to your data outside the firewall, and beyond your network.

Digital Risk Protection focuses on protecting your data.

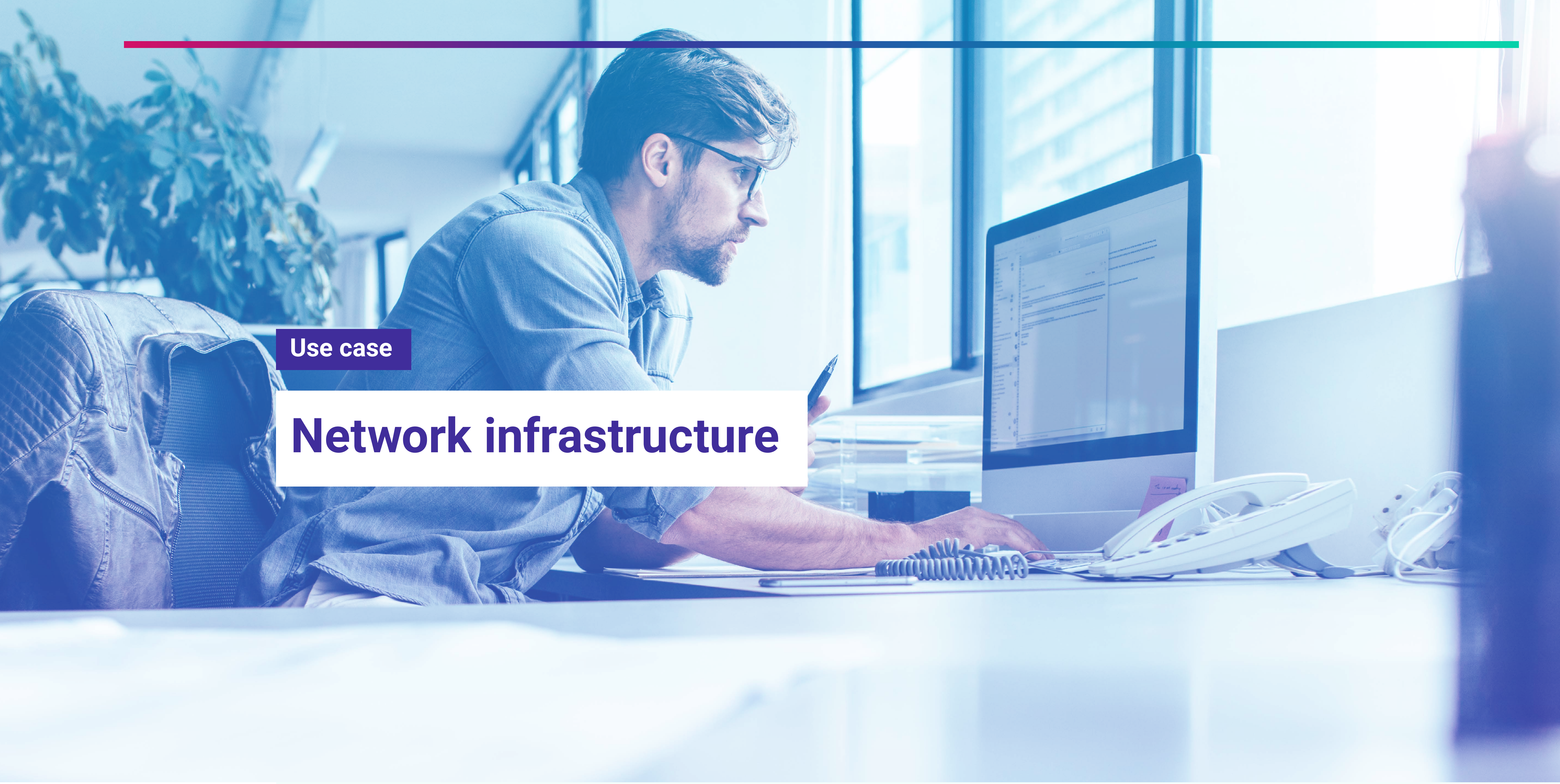
Wherever it lives.

The value of Digital Risk Protection

Looking at the four main types of data you need to protect, this eBook shows the business case for Digital Risk Protection and explains:

- What kind of information bad actors are looking for
- How this can be used against you
- How these threats increase your digital risk

But it's not all doom and gloom – we show you how Digital Risk Protection can help, how you can reduce your digital risk, and share thoughts from information security professionals who are already doing it.



Use case

Network infrastructure

Stop the next network attack before it happens

Did you know…

Bad actors and criminals could be targeting your organisation already. By collaborating and using techniques like port scans and reverse DNS look-ups, they can get hold of valuable information about your network infrastructure, vulnerabilities and the software you use.

Worse still, this information may have been shared by one of your own team.

Stop the next network attack before it happens

3 things bad actors look for

- Domains, subdomains and IP addresses
- Vulnerabilities in operating systems, hardware and software used
- Credentials for privileged system users

3 ways they can use them against you

- Denial of Service, either at a critical point (DoS) or distributed (DDoS)
- Accessing systems you use by exploiting vulnerabilities
- Targeted attacks (account takeover, spear phishing, extortion) on privileged users

3 ways this increases digital risk

- Reputational – inability to provide service or capture new customers
- Operational – availability, confidentiality & integrity impacts on your systems
- Revenue – payment diversion, extortion or ransom could impact your bottom line

Stop the next network attack before it happens

It’s not all bad news

In order to plan attacks on your business, bad actors and criminals need to get hold of this information. To do this, they may access the Dark Web to buy, sell or share details about your infrastructure. They may discuss or collaborate on attack planning using hacktivist forums. And, when they do, they leave a digital footprint. Which can act as an early warning of an imminent attack.

Stop the next network attack before it happens

Automated early warning

- Automated Dark Web monitoring can check if your information is being discussed or circulated and it works around the clock
- Instant alerts give you crucial hours, days or even months to take mitigating measures

3 easy ways to reduce risk

- Prioritise patch application and other measures to protect against exploitation of vulnerabilities being discussed
- Deploy web application firewalls
- Request takedown of posts

Our customers agree

"If we didn't have this type of threat intelligence capability, we would be under attack before we even knew that we were under attack."

— CISO, travel and tourism sector

Example: Infrastructure details breach

Input search terms

IP Address (range) search ("185.90.35.150")

Dark web monitoring result

IP Address discovered

Context provided

How your data is exposed

Port scans

Domain whois

Reverse DNS lookup

Insider threat

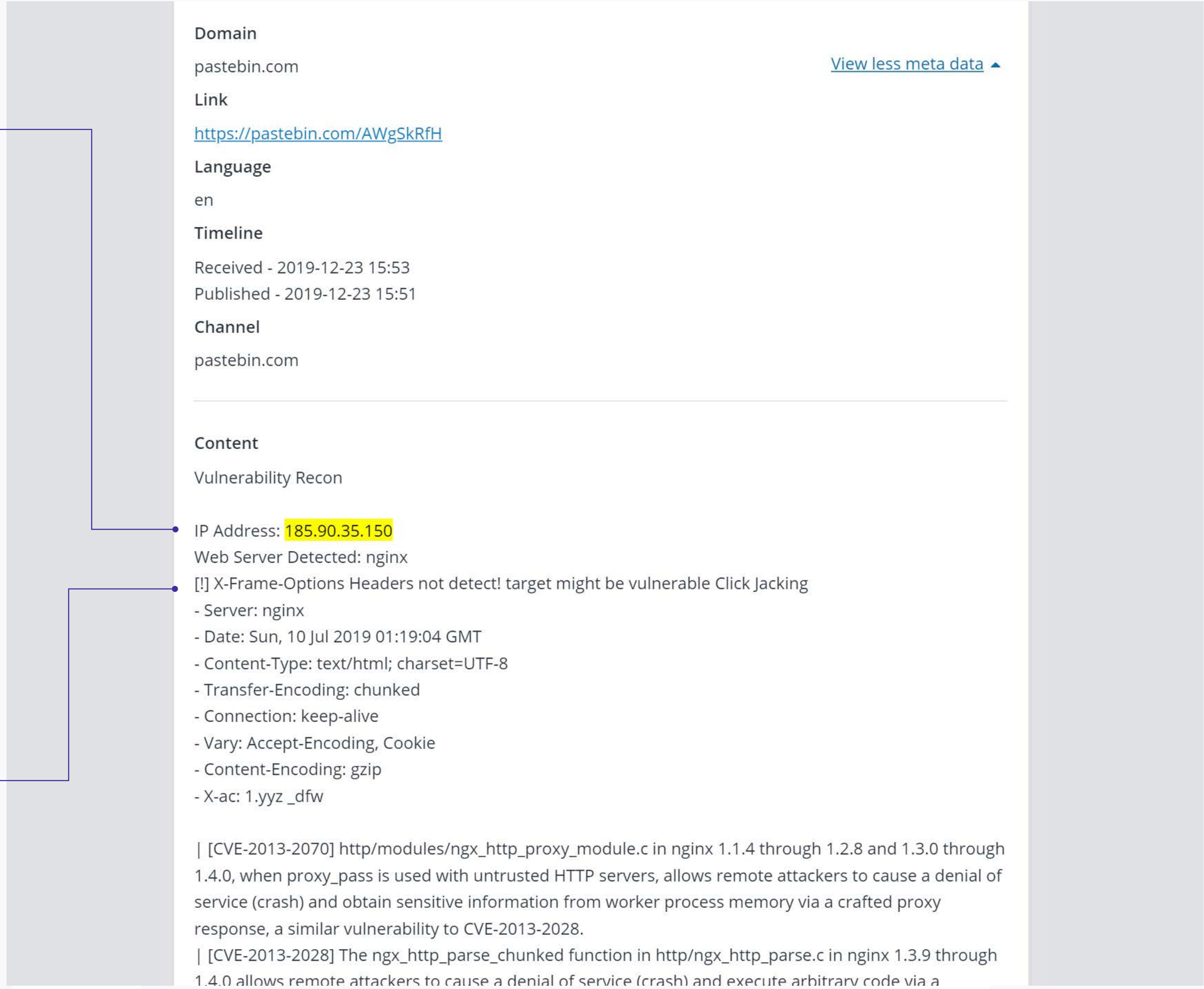
Data shared & traded

Domains, subdomains, IP addresses

Vulnerabilities

Privileged user credentials

Operating systems, hardware and software



Domain

pastebin.com

Link

https://pastebin.com/AWgSkRfH

Language

en

Timeline

Received - 2019-12-23 15:53
Published - 2019-12-23 15:51

Channel

pastebin.com

Content

Vulnerability Recon

```
IP Address: 185.90.35.150
Web Server Detected: nginx
[!] X-Frame-Options Headers not detect! target might be vulnerable Click Jacking
- Server: nginx
- Date: Sun, 10 Jul 2019 01:19:04 GMT
- Content-Type: text/html; charset=UTF-8
- Transfer-Encoding: chunked
- Connection: keep-alive
- Vary: Accept-Encoding, Cookie
- Content-Encoding: gzip
- X-ac: 1.yyz _dfw

| [CVE-2013-2070] http/modules/ngx_http_proxy_module.c in nginx 1.1.4 through 1.2.8 and 1.3.0 through
1.4.0, when proxy_pass is used with untrusted HTTP servers, allows remote attackers to cause a denial of
service (crash) and obtain sensitive information from worker process memory via a crafted proxy
response, a similar vulnerability to CVE-2013-2028.
| [CVE-2013-2028] The ngx_http_parse_chunked function in http/ngx_http_parse.c in nginx 1.3.9 through
1.4.0 allows remote attackers to cause a denial of service (crash) and execute arbitrary code via a
```

Priority response examples

Prioritise protecting against exploitation of highlighted vulnerabilities.

Deploy web application firewall

Inform mentioned users of potential phishing/extortion attacks

Request takedown of post

Types of threat

DoS / DDoS

Vulnerability exploitation

Spear phishing

Extortion

Use case

User credentials

A credential breach is bad news — you can stop it from becoming a disaster

Did you know...

A credential breach from any one of the Cloud applications your business uses can pose a serious threat to your systems. Last year, 60% of email system hacks were made possible by breaches of credentials from 3rd party apps.

But these incidents could have been prevented or stopped.

A credential breach is bad news — you can stop it from becoming a disaster

3 things bad actors look for

- Credential breaches from apps including plain text passwords
- Passwords which have been reused multiple times or slightly modified
- Corporate social media account details

3 ways they can use them against you

- Direct or brute force access to critical business systems
- Impersonation by hijacking your email or social media accounts
- Data exfiltration, stealing business critical information via email or payment diversion

3 ways this increases digital risk

- Operational – preventing access to commercial or back office systems
- Reputational – spreading harmful or fake information about your brand
- Resource – doxing your senior execs or trade secrets theft

A credential breach is bad news — you can stop it from becoming a disaster

Stop fall out before it starts

The sooner you know a credential breach has occurred, the sooner you can act. But, with reposting of credential breaches so wide-spread it can be difficult to eliminate false alarms. Integrating information from your employee directory can help you spot active account compromise quickly and easily.

A credential breach is bad news — you can stop it from becoming a disaster

Own your playbook

- Optimise breach response by integrating credential breach alerts into your SOC systems.
- Understand breach sources and compare alerts to previous breaches to understand who's affected and the level of risk.

4 easy ways to reduce risk

- Use insights to educate users with bad password habits
- Send alerts to compromised accounts to change passwords
- Deploy multi-factor authentication to prevent external access
- Update external service use policy

Our customers agree

"Peace of mind is probably one of the key things. The simplicity of the interface is really good. It's clear and obvious how things work, and there's flexibility in how you set it up."

— IT Manager, High St and On-line Travel Agent

Example: Employee credential breach

Input search terms

- Email domain: webnightsec
- Staff list: email addresses: admin@webnightsec

Dark web monitoring result

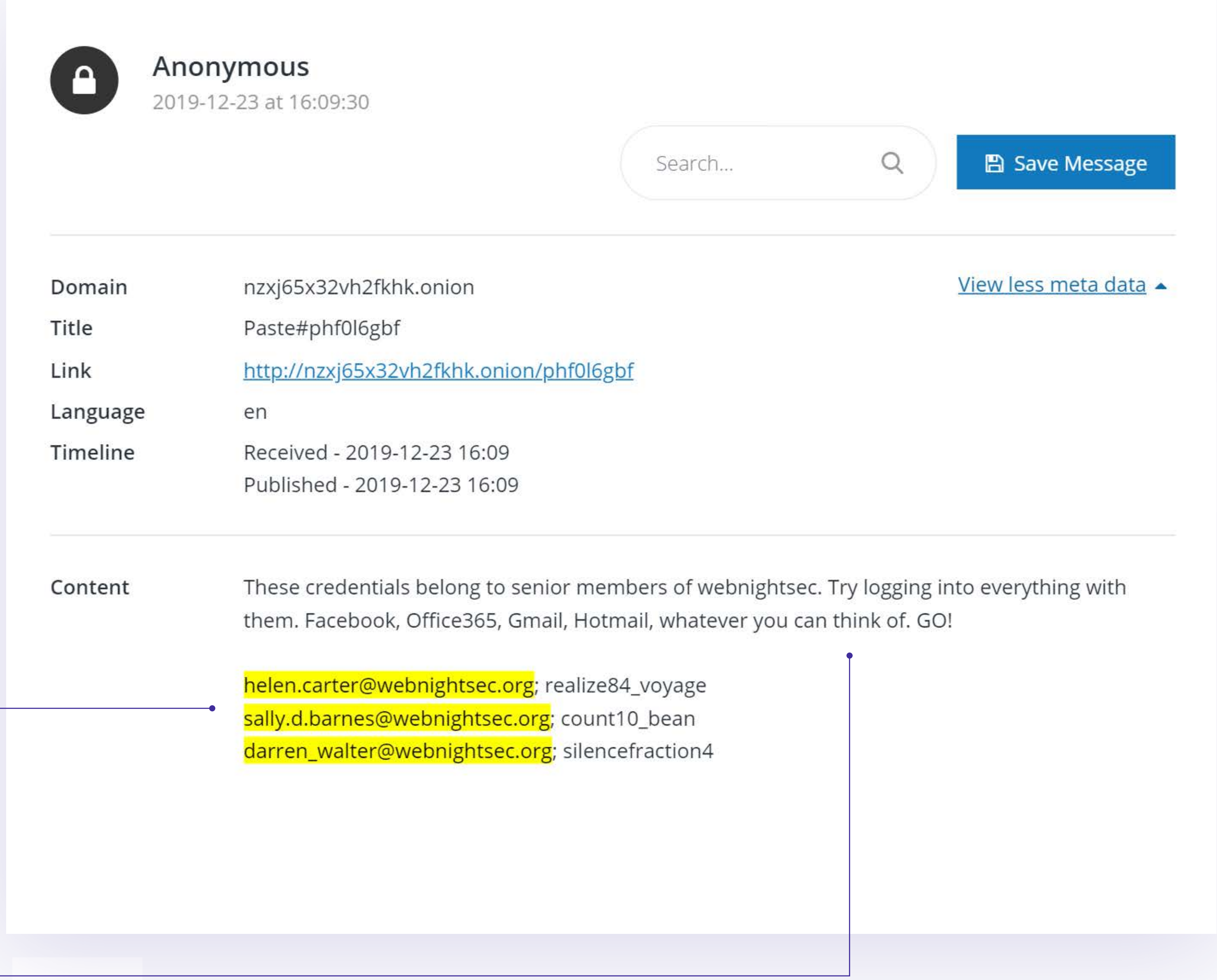
- Matching email address discovered
- Plain text password dumps highlighted
- User, website and URL

How your data is exposed

- Insider threat
- 3rd Party app data breach
- Shared password

Data shared & traded

- Email address lists
- Credential lists
- Operating systems, hardware and software



Anonymous
2019-12-23 at 16:09:30

Domain	nzxj65x32vh2fkhk.onion
Title	Paste#phf0l6gbf
Link	http://nzxj65x32vh2fkhk.onion/phf0l6gbf
Language	en
Timeline	Received - 2019-12-23 16:09 Published - 2019-12-23 16:09
Content	These credentials belong to senior members of webnightsec. Try logging into everything with them. Facebook, Office365, Gmail, Hotmail, whatever you can think of. GO! helen.carter@webnightsec.org; realize84_voyage sally.d.barnes@webnightsec.org; count10_bean darren_walter@webnightsec.org; silencefraction4

Priority response examples

- Inform mentioned users of potential phishing/extortion attacks
- Request takedown of post
- Enforce password rotation
- Implement password manager and multi-factor authentication to prevent future attacks
- Provide awareness and training for repeat offenders

Types of threat

- Spam / Phishing
- 3rd party system access
- Brute force
- Attack planning
- Extortion

Use case

Customer data

Digital trust is the new frontier — give customers confidence in your services

Did you know...

Customer trust is a bedrock for loyalty and business growth. One recent IBM survey reported an average 3.9% higher churn rate for businesses that had suffered a customer data breach.

According to RSA, 35% of consumers use false details when creating accounts - becuase they don’t trust brands to keep their data safe.

Digital trust is the new frontier — give customers confidence in your services

3 things bad actors look for

- Unprotected databases exposed on Cloud infrastructure
- Opportunities to inject code into web plugins including payment or chat applications
- Staff or supply chain partners who are willing to leak or sell customer details

4 ways they can use them against you

- Customer data, including PII is shared or sold via the Dark Web
- Email lists are used for spam, phishing or payment diversion
- Attackers threaten to post a database if a ransom is not paid
- Skimming customer payment details by form-jacking

3 ways this increases digital risk

- Reputational – customers lose trust and turn to competitors
- Operational – downtime of service, loss of access to critical data
- Financial – loss of revenue, ransom payments, compensation and regulatory fines

Digital trust is the new frontier — give customers confidence in your services

Protect your data. Wherever it lives.

Customer data doesn't just live inside your network. Cloud storage and apps, 3rd party services and partners can still lose data, no matter how good your own network defences are. Watermarking your data and continuously monitoring for leaks or misuse will help you minimise the potential fallout and damage of a data breach.

Digital trust is the new frontier — give customers confidence in your services

Best practice is key

- Data privacy is important to your customers. Have a clear policy and stick to it.
- Make sure your partners take data security seriously too.
- Use Digital Risk Protection techniques to protect data beyond your network.

4 easy ways to reduce risk

- Watermark your data with unique synthetic identities to spot leaks
- Deploy multi-factor authentication for customer access to your services
- Monitor for your customer data on the surface, deep and Dark Web
- Report breaches without delay

Our customers agree

"As a leader in our industry, maintaining our brand reputation and the trust of our customers is vital. Skurio's BreachAlert provides us peace of mind with minimal day-to-day effort."

— Network Security Manager, Industrial manufacturing

Example: Customer data breach

Input search terms

- Email domain: webnightsec
- List: customer emails
- Breachmarker: email address

Dark web monitoring result

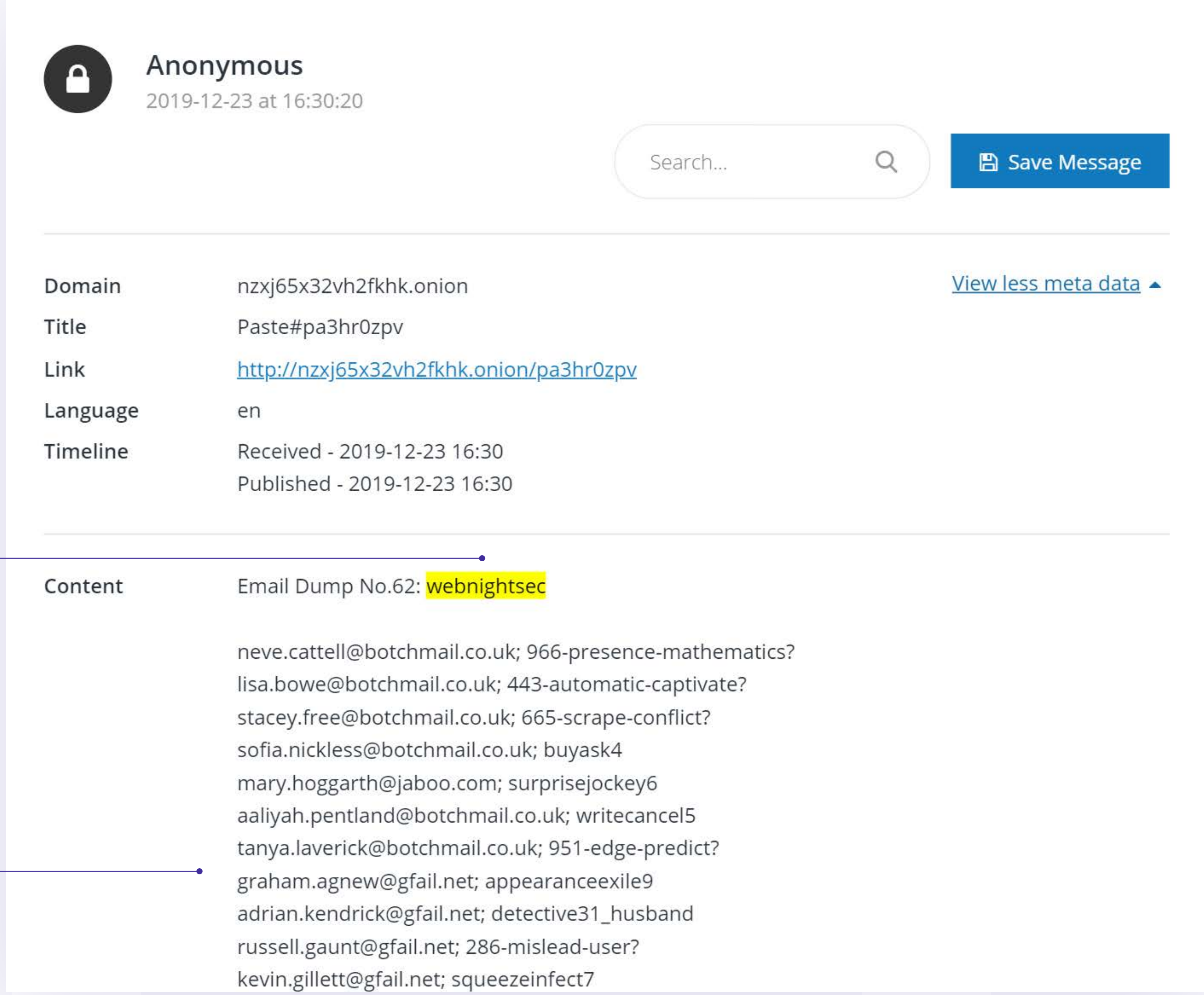
- Email addresses and password combinations included in a post which mentions the company domain
- Source and URL for post

How your data is exposed

- Insider threat
- Supply chain partner breach
- Shared password
- Unauthorised database access

Data shared & traded

- Email address lists
- Credential lists
- PII
- Payment details



Anonymous
2019-12-23 at 16:30:20

Domain nzxj65x32vh2fkhk.onion
Title Paste#pa3hr0zpv
Link http://nzxj65x32vh2fkhk.onion/pa3hr0zpv
Language en
Timeline Received - 2019-12-23 16:30
Published - 2019-12-23 16:30

Content Email Dump No.62: webnightsec

neve.cattell@botchmail.co.uk; 966-presence-mathematics?
lisa.bowe@botchmail.co.uk; 443-automatic-captivate?
stacey.free@botchmail.co.uk; 665-scrape-conflict?
sofia.nickless@botchmail.co.uk; buyask4
mary.hoggarth@jaboo.com; surprisejockey6
aaliyah.pentland@botchmail.co.uk; writecancel5
tanya.laverick@botchmail.co.uk; 951-edge-predict?
graham.agnew@gfail.net; appearanceexile9
adrian.kendrick@gfail.net; detective31_husband
russell.gaunt@gfail.net; 286-mislead-user?
kevin.gillett@gfail.net; squeezeinfect7

Priority response examples

- Inform customers to anticipate phishing attempts and force password change
- Inform regulatory authority (e.g. ICO) of data breach to minimise GDPR fine
- Watermark data to establish breach origination
- Identify the scope and impact of the breach on your organisation
- Where possible, attempt removal of information from the site
- Identify method of breach and mitigate against future risk

Types of threat

- Spam
- Phishing
- Payment diversion
- Forced regulatory compliance failure

Use case

Business critical information

All businesses are data driven — stop your best asset being used against you

Did you know…

Almost every aspect of your business relies on data in one way or another. Theft of intellectual property or strategic, confidential information are two of the biggest digital risks to your business. According to Verizon, over 70% of workers admit to taking intellectual property with them when they resign.

All businesses are data driven — stop your best asset being used against you

3 things bad actors look for

- Previously breached staff credentials
- Vulnerabilities via supply chain partners
- Whistleblowers or aggrieved staff willing to sell or leak data

3 ways they can use them against you

- Disclosure of breached data to press, authorities or competitors
- Facilitate counterfeiting of your goods and services
- Financial fraud or extortion activities

3 ways this increases digital risk

- Operational – jeopardised business strategy
- Reputational –unwanted media coverage
- Financial – reduced ability to compete, diverted payments

All businesses are data driven — stop your best asset being used against you

Monitor for business critical data outside your network

You might not be able to stop all theft of business critical data, especially if it has taken place in your digital supply chain. But, if you can detect it, you can identify the cause and prevent further leaks or theft. More importantly, early detection will allow you to take measures which will mitigate further issues. Proactively using techniques like digital watermarking can help you pinpoint breaches even sooner.

All businesses are data driven —
stop your best asset being used against you

Go beyond credential monitoring

- Use Digital Risk Protection to safeguard VIPs, intellectual property, brand misuse and more
- Add digital watermarks to verify if data found definitely belongs to you, and reduce false positives

4 easy ways to reduce risk

- Use security permissions to stop staff from downloading data
- Use unique digital watermarks to track any movement of intellectual property
- Consider requesting takedown of publicly pasted data
- Identify source to prevent further loss

Our customers agree

"It's been an enormous success story. We've been able to open up a whole avenue of intelligence that people were not looking at before."

— Finance Operations Manager,
Communications sector

Example: Business data breach

Input search terms

- Keyword: brand/product/ project names
- Watermarker: Pattern matcher

Dark web monitoring result

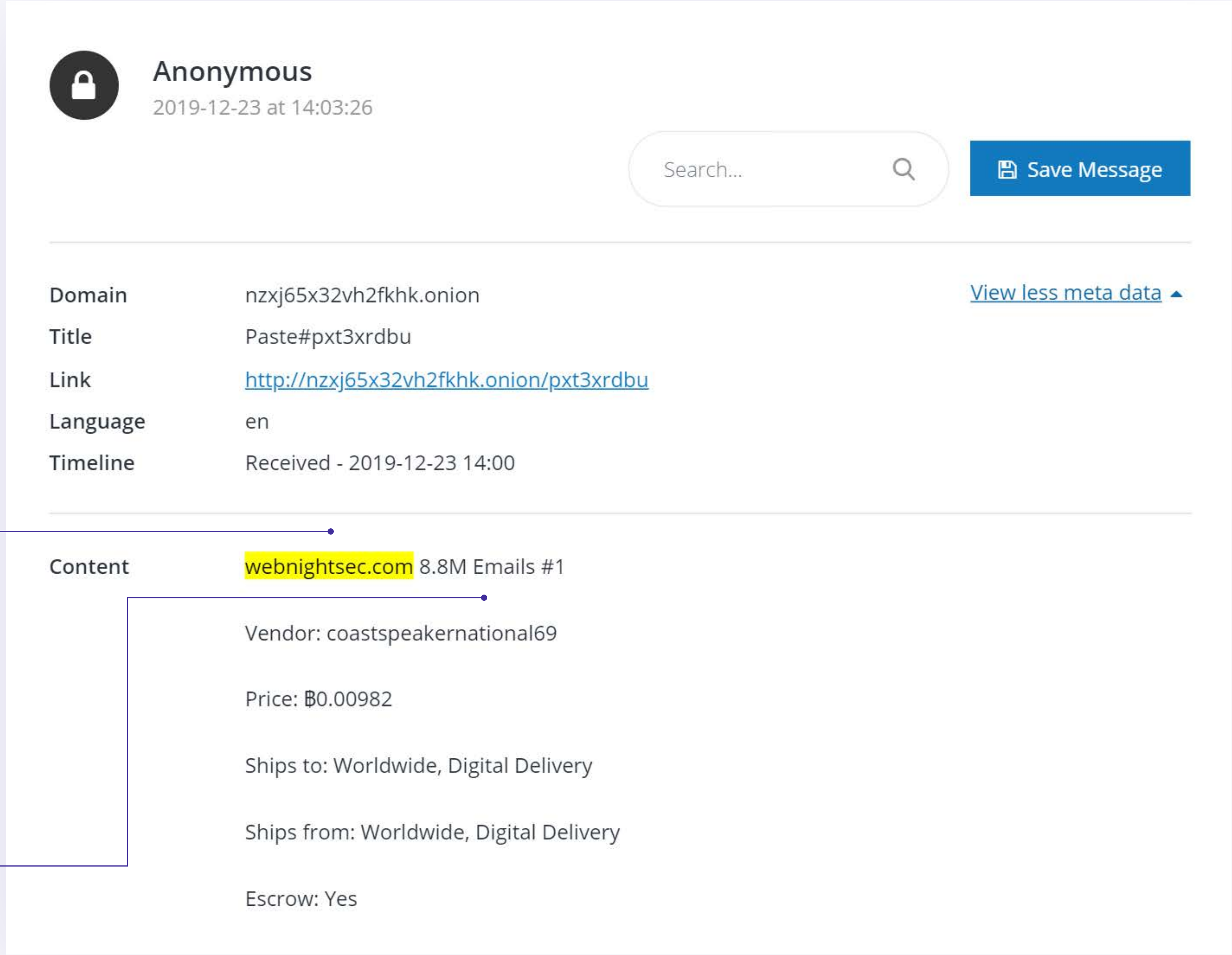
- Matching keyword
- Content
- Domain
- Poster (if known)

How data is exposed

- Insider threat
- Credential breach
- Supply chain attack

Data shared & traded

- Digital assets e.g. media / code
- Confidential email
- IPR
- Strategic plans / financial detals



Anonymous
2019-12-23 at 14:03:26

Domain	nzxj65x32vh2fkhk.onion
Title	Paste#pxt3xrdbu
Link	http://nzxj65x32vh2fkhk.onion/pxt3xrdbu
Language	en
Timeline	Received - 2019-12-23 14:00

Content webnightsec.com 8.8M Emails #1

Vendor: coastspeakernational69

Price: ฿0.00982

Ships to: Worldwide, Digital Delivery

Ships from: Worldwide, Digital Delivery

Escrow: Yes

Priority response examples

- Watermark data to establish breach origination
- Identify the scope and impact of the breach on your organisation
- Where possible, attempt removal of information from the site
- Identify method of breach and mitigate against future risk

Types of threat

- Extortion
- Disclosure
- Fraud

Skurio Digital Risk Protection

Dark Web Monitoring

- Monitor for staff, customer, infrastructure and critical business data 24x7
- Tailor searches on social, surface, deep and Dark Web sources
- Search years of historic data to obtain better insights

Data Breach Detection

- Get instant alerts if your data is found outside your network
- Automate your breach response playbooks with readymade integrations to SIEM and ITSM
- Instantly detect and verify the source of a breach with data watermarking

Cyber Threat Intelligence

- Combine curated content relevant to your business to speed investigations
- Use intuitive analytics to get usable insights faster
- Organise intelligence insights with simplicity and collaborate to improve resolution

Skurio Digital Risk Protection

The Skurio Digital Risk Protection platform provides you with the components necessary to adopt a data-centric approach to cybersecurity for your business. BreachAlert continuously monitors for your data on the surface, deep and Dark Web and instantly alerts you whenever it is found.

Skurio Cyber Threat Intelligence looks for cyber threats specific to your business, giving you a single view of all data protection incidents and threats outside your network.

BreachMarker and BreachResponse features help you protect your data across your supply chain and integrate valuable alerts into your response management systems.

To understand how Skurio can help protect what's important to your business and reduce your digital risk, please visit www.skurio.com

skurio.com | info@skurio.com

SKURIO