

Factsheet

Next Generation Digital Risk Protection as a Service

Enable, drive and protect
your business.

As digital threats against brands and data grow, a proactive protection stance is key

Proactive protection for brands & data: identify risks and mount a targeted defence against digital threats.

At a time when brand reputation, customer data and companies' digital presences face an onslaught of attacks such as phishing and fraud, a proactive approach to threat identification and mitigation is more important than ever and key to ensuring confidence and security in the digital world. The discovery of confidential information on public or closed

networks poses a significant threat to security. Traditional security solutions are unable to identify risks such as a loss of data, phishing or website spoofing. Next Generation Digital Risk Protection as a Service (ngDRPaaS) collects and analyses relevant company data, including the external attack surface and inventory of Internet-exposed assets (asset library), to transparently identify these risks. Potential security incidents are escalated and recommendations for action provided.



Identification of digital risks

Unwanted threats on the public Internet and in closed networks are identified so that you are kept informed of the current threat situation.



Recommended actions

You decide on the measures to be taken on the basis of the recommendations for action suggested.



Managed Takedown

Direct submission of deletion requests for illegally hosted content to third parties, including transparent reporting.



External Attack Surface Management


Intelligence methods to record and analyse your digital attack surface, including inventories of Internet-exposed assets.

How ngDRPaaS works




Domain
Brand
IP Ranges
...

Define
assets



Deep Web
Open Web
Social Media
Dark Web

Find threats
to assets




Human &
Technology

Analyse and
identify risks



Exposed Password
Phishing Website
...

Risk list with
recommended actions



Change Password
Take down
...

Implement
measures

Facts & Figures

Basic services

Brand and Domain Protection:

The ngDRP platform is provided as a managed service to secure the online brand and detect malicious domains set up to spoof or launch attacks from customer domains. The service automatically scans the surface web, deep web, dark web and social media for potential threats.

Optional services

External Attack Surface Management:

The solution records Internet-exposed assets and creates an asset library that is regularly compared against risk databases, such as CVSS and CVE.

Managed Takedown:

A complete takedown service with integrated workflow to target specific malicious content.

On-Demand Investigations:

Combat complex threats with the support of our threat intelligence team. We provide customised threat analysis, strategic decision reporting and red teaming services for realistic security audits.

Additional services

Security Analytics as a Service (SAaaS):

As security and big data experts, we offer proven security analytics. Connect log sources and monitor security incidents from the dashboard. The analysis and response is in your hands.

SOC as a Service (SOCaaS):

This dashboard provides an overview of potential and confirmed security incidents from your company's defined log data as well as analyses with specific recommendations for action.

You can find more information and our expert's contact details at <https://swisscom.ch/drps>