

G-Cloud 15

Digital Footprint Intelligence Report



Atos

Table of contents

- 1. What is the Digital Footprint Intelligence Report Service 3
- 2. What does it deliver? 4
- 3. What technology does it use 5
- 4. What terms apply?7
- 5. Termination..... 8
- 6. How do I order? 9
- 7. Glossary.....10
- 8. Why Atos..... 11



1. What is the Digital Footprint Intelligence Report Service?

As reliance on digital technologies grows, Digital Footprint Intelligence assessments have become a critical component of robust cybersecurity strategies.

The Atos Digital Footprint Intelligence Report is a comprehensive solution designed to help public sector organisations navigate this complex landscape by identifying and mitigating risks associated with the digital footprint across the Open and Dark Web. These assessments provide a comprehensive view of the public sector's online presence, highlighting vulnerabilities, potential threats, and areas of concern.



2. What does it deliver?

The report goes beyond simple data collection and analysis. It provides a holistic view of your public sector organisation's online presence by amalgamating information from a wide range of intelligence resources across both the Open and Dark Web.

This includes data from network domains, user domains, organisation documentation, compromised email addresses, contact numbers, paste sites and social networks. By examining this data through the lens of potential threats, the report highlights vulnerabilities that malicious actors could exploit.

One of the key strengths of the Digital Footprint Intelligence Report is its ability to contextualise the gathered information. The report not only identifies potential risks but also explains how each piece of information could be used to harm the public sector organisation. For example, it may highlight how a leaked document could expose sensitive organisation information or how a compromised email address could be used in a phishing attack. This level of detail allows the organisation to prioritise its security efforts and allocate resources effectively.



3. What technology does it use?

The report is created by a team of dedicated security specialists who combine cutting-edge technology with expert analysis. They use a blend of commercial software and open source intelligence (OSINT) methods to gather data from a wide range of sources. This approach ensures that no stone is left unturned in the search for potential threats to the public sector organisation.

Once the data has been collected, the security specialists analyse it to identify patterns, trends and areas of concern that could lead to a cyber-attack, security breach or damage to the public sector organisation and wider government brand and reputation.

They then present their findings in a clear, actionable format that enables the organisation to make informed decisions about the public sector organisation's security posture. The report is divided into five core sections, each focusing on a different aspect of your digital footprint:

1. **Network** – Highlights links between network domains, risks to user domains and similar public sector organisation domains.
2. **Documents** – Identifies organisation artefacts found online that can be used for exploitation.
3. **Users** – Lists the compromised emails, addresses and contact numbers.
4. **Organisation and User Data** – Identifying information on external site, how exploitable to the organisation.
5. **Social Networks** – Significant entries on collaboration networks by internal/external organisation resources, exposing an organisation to risk.

The report provides in-depth, technical information informing the public sector organisation of key issues requiring mitigating action, helping minimise threats and reducing the attack surface.

By acting on the recommendations provided in the Digital Footprint Intelligence Report, the organisation can significantly reduce the risk and blast radius of a damaging cybersecurity incident.

This proactive approach can help the public sector organisation, or possibly the UK Government, avoid the negative financial and reputational impacts of a data breach, which can be devastating for any organisation, government or country.

In addition to identifying immediate threats, the report also provides valuable insights into emerging trends and potential future risks. This forward-looking perspective allows the organisation to stay ahead of the curve and adapt its security strategies as the threat landscape evolves.

In conclusion, the Atos Digital Footprint Intelligence Report is an essential tool for any public sector organisation seeking to secure its online presence.

By providing a comprehensive, contextualised view of the organisation's digital footprint, it empowers the organisation to make informed decisions and implement effective security measures.



4. What terms apply?

To the fullest extent permitted under G-Cloud 15 Framework Agreement and the Call-Off Contract, Atos will provide the Services in accordance with the Atos Supplier Terms (which will include, but may not be limited to , the Supplier Acceptable Use Policy, Supplier Data Processing Agreement, Supplier Specific Shared Responsibility Model, Supplier SLAs and Supplier Licence Terms and any applicable Third-Party Terms outlined in this Service Description document and the Order Form) and this Service Description document.

For clarity:

- Atos Supplier Terms may be modified in accordance with the provisions of the Call-Off Contract, and remain effective except where expressly overridden.
- Hyperlinks included in the Atos Supplier Terms and Service Description document remain effective where they point to Atos' or the relevant Third-Party Terms or documents. Should a hyperlink cease to function, Atos will work with the client to update it through the agreed procedure.



5. Termination

Termination shall be in accordance with:

- The G-Cloud 15 Framework terms and conditions
- Any terms agreed within the Order Form of the relevant Call-Off Contract
- For this specific service, by default Atos ask for at least thirty (30) days prior written notice of termination without cause.

Atos commits to the continued provision of services for the duration of the Call-Off Contract subject to the terms and conditions of the G-Cloud 15 Framework Agreement, the Call-Off Contract, the Atos Supplier Terms and the applicable Third Party Agreements (as defined in the Atos Supplier Terms and indicated in the Order Form) related thereto.



6. How do I order?

Please contact our team at: gcloud@atos.net

- We will prepare a quotation for your review, including any applicable volume discounts.
- Once the quotation is agreed, we will issue the necessary documentation (as required by the G-Cloud Framework) and request a purchase order from you.
- Upon receipt of your purchase order, we will configure the services in line with the agreed requirements. Where applicable, you will also receive access to our self-service portal to begin provisioning services.
- If you are a new customer, you may need to complete additional 'new supplier' forms.
- Invoices will be issued to you and to Crown Commercial Service (CCS), quoting the purchase order number, for the services procured.
- We will also submit the required monthly management information reports to Government Procurement.



7. Glossary

Term	Definition
OSINT	Open Source Intelligence



8. Why Atos

Atos has been a trusted partner on every G-Cloud iteration since the framework began, helping public sector organisations modernise with confidence. We combine global expertise with deep UK experience, delivering secure, scalable cloud solutions that meet the highest government standards.

As Europe's leading provider of cloud and cybersecurity services, Atos offers end-to-end capabilities - from migration and hosting to SaaS and consultancy - supported by UK delivery centres and strategic partnerships with hyperscalers.

Our focus on innovation, sustainability, and social value ensures that customers not only achieve operational excellence but also contribute to a greener, fairer future. With Atos, you gain a proven partner committed to driving efficiency, resilience, and transformation across public service.



About Atos

Atos Group is a global leader in digital transformation with c. 67,000 employees and annual revenue of c. €10 billion, operating in 61 countries under two brands – Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE is listed on Euronext Paris.

The purpose of Atos Group is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Learn more at: atos.net