ARQIT

Encryption Intelligence

Arqit Encryption Intelligence provides detailed insights into the use of encryption across your organisation, so you can fix encryption weaknesses today and prepare for the coming PQC Migration challenge.

Arqitgroup.com

Encryption Intelligence

Arqit Encryption Intelligence provides detailed insights into the use of encryption across your organisation, so you can identify and fix encryption weaknesses today and prepare for the coming quantum computer threat.

Encryption Intelligence provides the insights you need to develop an effective post quantum cryptography migration plan in line with guidance from the National Cyber Security Centre. It provides encryption discovery, planning and implementation support for Cloud, IoT and applications.

For more information, visit **arqitgroup.com**

Assured Service Provider

National Cyber Security Centre

Consultancy: Post-Quantum Cryptography (Discovery and Migration Planning)

Introduction

The importance of encryption

Cyber security breaches continue to grow in number and severity across all industries and all types of organisations. The business risk of cyber security attack grows constantly and can pose an existential threat to any organisation.

At the same time, the sophistication of attacks is constantly increasing, with multi-national 'professional' threat actors (including those backed by nation states) growing and ramping up their activities. The risk that organisation data could be stolen or compromised is very real and the impact is likely to be catastrophic.

Encryption of data is at the core of most protection strategies – effective encryption of communications prevents threat actors from eavesdropping data or impersonating a legitimate business contact; and data which is encrypted properly will be safe even if the underlying system or communications path is otherwise compromised.

In recent years, many enterprise applications have shifted out of the office and into public Cloud infrastructure, either running in Virtual Private Cloud under control of the organisation, or delivered from public Cloud as Software-as-a-Service (SaaS).

With Cloud, the issues of data protection become even more important, as large amounts of potentially critical sensitive data flow out of the logical perimeter of the organisation and into the control of the application vendor. It becomes necessary to understand and assess the security posture of every SaaS vendor and Cloud platform, since they have become part of the supply chain and extended operations of the organisation. Identifying and approving all vendors in the supply chain is a critical element of Information Security certification such as ISO 27001.

Those who **start early will be the ones who maintain trust**, resilience and competitive advantage. Those who delay will face a **rushed, expensive and highly disruptive upgrade.**

The quantum threat to encryption

It is now well-established that quantum computers represent a fundamental threat to the most prevalent encryption schemes in use today.

As quantum computers continue to advance rapidly, they will become capable of breaking encryption, rendering encrypted data vulnerable to eavesdropping and misuse. The public-private key encryption schemes used by everything from mobile phones to web servers (including SaaS applications) to connected IoT devices and Operational Technology (OT) will be vulnerable.

Although publicly-announced quantum computers have not yet attained a level of capability that would allow state-of-the-art encryption to be attacked successfully, the rate of advancement is rapid. Encryption schemes being deployed today must be assessed for future security given that systems may be in use for many years. Government security agencies around the world, including in the US,UK and EU have warned that sophisticated threat actors are likely to be storing encrypted data now in order to decrypt it later when more capable quantum computers become available (so-called 'Harvest Now, Decrypt Later' attacks). To address these risks, governments around the world have mandated migration to quantum-secure encryption through post-quantum cryptography (PQC). The migration to PQC will be one of the largest and most complex technology transitions of the coming decade. Those who start early will be the ones who maintain trust, resilience and competitive advantage. Those who delay will face a rushed, expensive and highly disruptive upgrade.

Cryptographic Inventory

Given the importance of encryption to overall security, it is vital that every organisation understands how and where encryption is used within its business. Each organisation must actively investigate all potentially sensitive network communications and make a determination about the level of risk involved.

The UK's National Cyber Security Centre (NCSC) has set out guidance for Post Quantum Migration planning (**Read more**): By 2028 organisations should have carried out a full discovery exercise and built an initial plan for migration of systems to Post-Quantum Cryptography.

Arqit is proud to have been selected to join NCSC's Post-Quantum Cryptography pilot. This is an assured consultancy scheme aimed at supporting the UK's national migration to PQC by ensuring that organizations have access to the advice and tools they will need to help them along their migration journey. By choosing an NCSC-assured provider such as Arqit, you can be certain that the advice you receive will be of high quality and will meet NCSC's standards for PQC readiness.

Key Use Cases

Build a comprehensive Cryptographic Inventory

Uncover the hidden encryption tech in applications, services, and devices that your employees and customers use.

Uncover encryption vulnerabilities

Identify obsolete or weak encryption schemes and highlight exposures to known exploits.

Prepare for migration to quantum-safe encryption

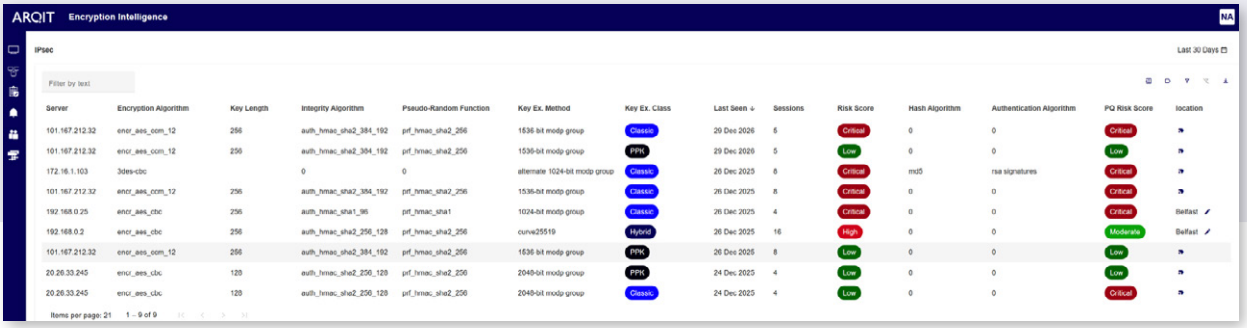
Prioritise systems, applications and devices so your most critical assets can be protected from quantum attack.

Continuous encryption monitoring

Monitor your entire encryption landscape continuously and securely, so you can detect and correct threats immediately.

Validate vendor PQC compliance

Test new vendor hardware and software to verify correct use of post-quantum cryptography before deployment, reducing supply-chain risk.



The Need for Encryption Intelligence

Encryption is the invisible shield that protects every aspect of modern life, but it carries hidden risks

Every organisation has critical data that must be kept confidential to retain the trust of customers, employees and the public.

Encryption is the bedrock of data protection, but it is being put at risk by outdated technology that is vulnerable to attack. Unless you understand the encryption used by every device and application, you cannot address the risk of data loss.

Quantum Threat to Encryption

Quantum computers are increasing in capability at an exponential rate, and it is certain that they will soon be capable of decrypting currently 'unbreakable' encryption. We are facing an imminent need to upgrade all encryption, which will be a massive task.

The PQC Migration challenge will affect every organisation for years to come. Without good knowledge of where and how encryption is used within the organisation, you cannot build an effective plan.

Data moving across networks and the Cloud is at risk

The risk of data interception is greatest when your data moves and transits across a network. With increasing use of Cloud and scale-up data centres, more of your critical data is transiting outside your physical control and crossing insecure public networks.

Satellite, radio, fibre optic communications are all open to interception. Only good cryptography keeps your data safe, so you must be able to assess encryption risk.

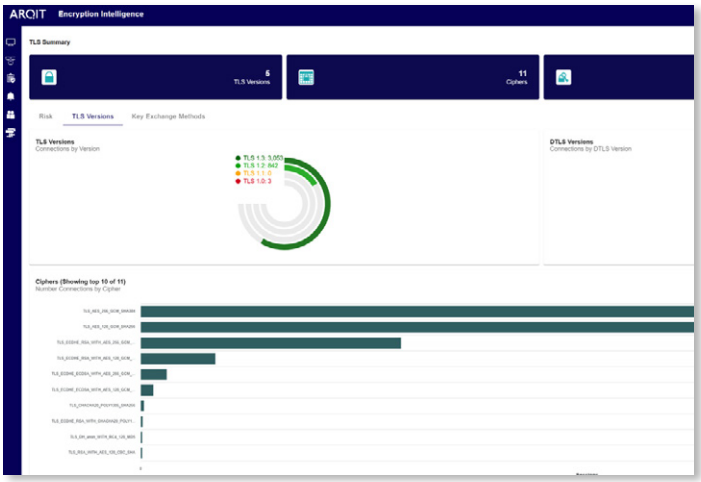
Arqit Encryption Intelligence

Every time one of your people uses a Cloud application, or an IoT device reports a data measurement, they depend on encryption. Arqit Encryption Intelligence gives you confidence that weak encryption cannot put your people and data at risk.

Encryption Discovery

Your organisation uses encryption millions of times every day, so finding encryption security threats requires efficient discovery at scale.

Arqit Encryption Intelligence processes network communications at gigabit scale to find every use of encryption, classifying and risk assessing in real time.



Encryption Inventory

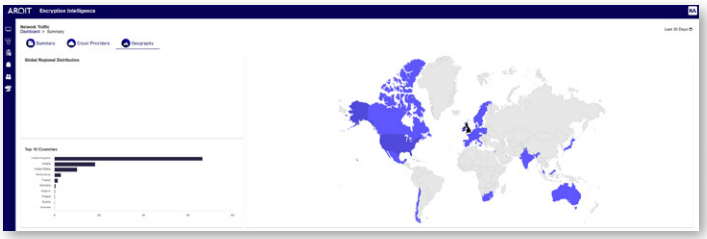
True Encryption Intelligence needs much more than a list of encryption schemes. Arqit's platform uses AI automation to probe and scan every use of encryption to add context, and help you answer key questions such as:

- **How effective is the encryption technology?**
- **What data is being protected?**
- **Who in your organisation created the data?**
- **What is the sensitivity lifetime of the data?**

Encryption Monitoring

Your individual encryption landscape changes all the time, so Arqit Encryption Intelligence monitors continuously, searching for new ciphers, new protocols and new vulnerabilities.

Encryption Intelligence sends alerts to your existing security monitoring tools, so your cyber defenders can get complete visibility of encryption threats and respond immediately.



Simple cloud deployment, fast results

Arqit Encryption Intelligence can be installed and analysing your encryption in minutes

Encryption usage information is gathered from across the organisation infrastructure, analysed in-place on locally-installed probes, and the results are collated in the Encryption Intelligence platform (available in cloud or on-premises) for deeper analysis.

Data collection flexibility

Arqit data collection probes can be deployed to suit the needs and infrastructure of your organisation. Probes are packaged as virtual appliances which can be deployed locally on-site, in Cloud infrastructure (public or private) or installed on dedicated hardware appliances.

Secure data collection and analysis

Arqit network probes are read-only and operate against a mirror copy of your network data. The contents of your communications are never observed and never leave your infrastructure - only the metadata related to encryption setup is analysed, and only summarised information is sent to our ISO27001-compliant Encryption Intelligence platform.

Reporting and visualisation to aid decision-makers

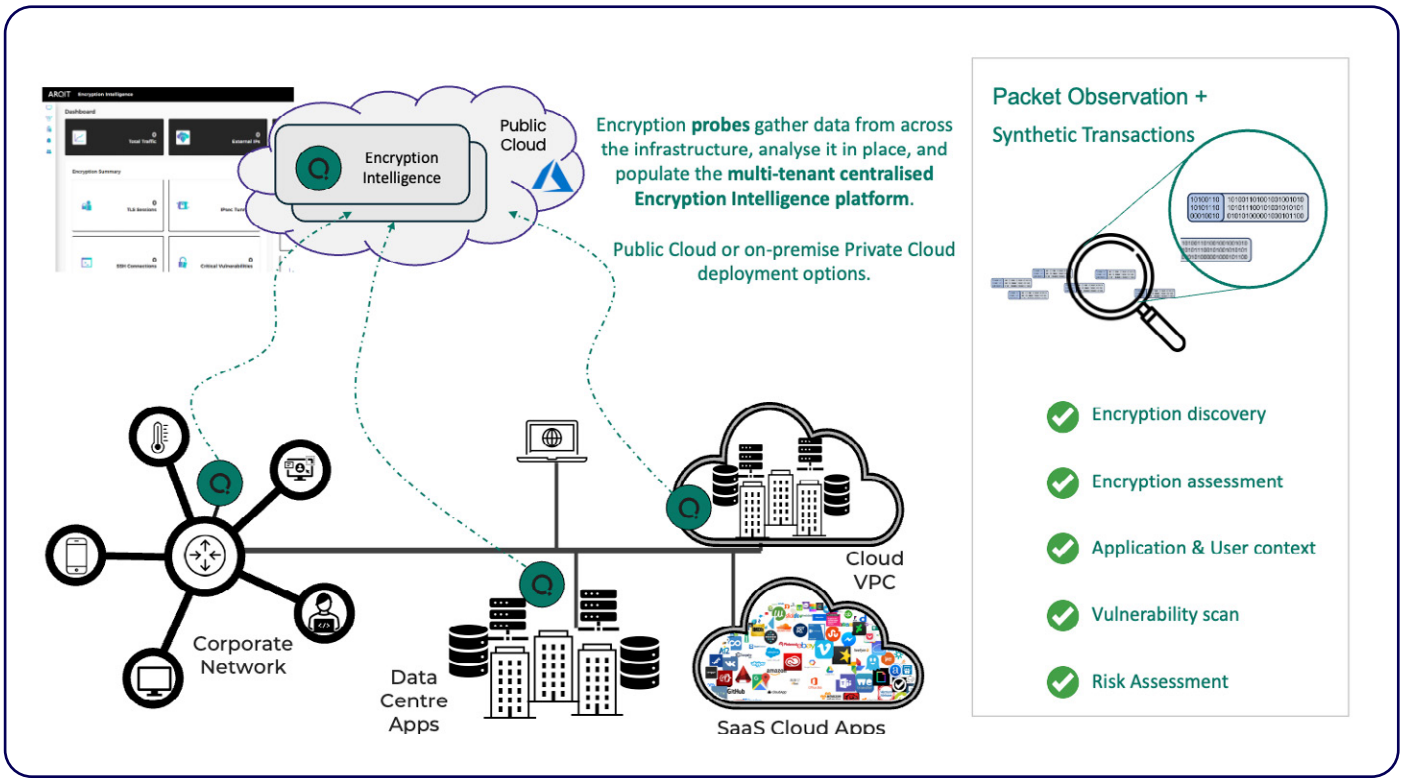
The Encryption Intelligence application has the dashboards and reports that you need to understand your encryption landscape in detail, build a business case to mitigate issues, and manage progress towards full encryption security.

Integration to support security infrastructure

Arqit Encryption Intelligence has the APIs and flexible integration points to integrate it with your existing security monitoring infrastructure via your SIEM and SOC.

Deployment Flexibility

Arqit's multi-tenant Encryption Intelligence platform is the fastest and most convenient way to deploy. However, if organisation security policies require a completely on-premise dedicated installation, this can be offered on private cloud or local infrastructure. Please contact Arqit for details and pricing.



Additional Services

Arqit and our partners can provide a series of additional services. Our consultants will be happy to discuss these with the buyer at an appropriate time.

Contact us

Arqitgroup.com

consultancy@arqit.uk

Arqit

These services include (for example):

1. Consultant-led Encryption Risk Advisory services.
2. Development of detailed encryption security strategies.
3. Development and implementation of post-quantum encryption mitigation plans.
4. Supply chain validation and advisory services.

Assured Service Provider

National Cyber Security Centre

Consultancy: Post-Quantum Cryptography (Discovery and Migration Planning)