

# 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.

## 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.

ARQIT Encryption Intelligence															NA
IPsec															Last 30 Days
Server	Encryption Algorithm	Key Length	Integrity Algorithm	Pseudo-Random Function	Key Ex. Method	Key Ex. Class	Last Seen	Sessions	Risk Score	Hash Algorithm	Authentication Algorithm	PQ Risk Score	location		
101.167.212.32	encr_aes_com_12	256	auth_hmac_sha2_384_192	prf_hmac_sha2_256	1536-bit modp group	Critical	20 Dec 2026	5	Critical	0	0	Critical			
101.167.212.32	encr_aes_com_12	256	auth_hmac_sha2_384_192	prf_hmac_sha2_256	1536-bit modp group	PPK	29 Dec 2026	5	Low	0	0	Low			
172.16.1.103	3des-cbc	0	0	0	alternate 1024-bit modp group	Critical	20 Dec 2025	8	Critical	md5	rsa signatures	Critical			
101.167.212.32	encr_aes_com_12	256	auth_hmac_sha2_384_192	prf_hmac_sha2_256	1536-bit modp group	Critical	20 Dec 2025	8	Critical	0	0	Critical			
192.168.0.25	encr_aes_cbc	256	auth_hmac_sha2_256_192	prf_hmac_sha2_256	1024-bit modp group	Critical	20 Dec 2025	4	Critical	0	0	Critical			
192.168.0.2	encr_aes_cbc	256	auth_hmac_sha2_256_192	prf_hmac_sha2_256	curve25519	Hybrid	20 Dec 2025	16	High	0	0	Moderate	Belfast		
101.167.212.32	encr_aes_com_12	256	auth_hmac_sha2_384_192	prf_hmac_sha2_256	1536-bit modp group	PPK	20 Dec 2025	8	Low	0	0	Low			
20.26.33.245	encr_aes_cbc	128	auth_hmac_sha2_256_192	prf_hmac_sha2_256	2048-bit modp group	Critical	21 Dec 2025	4	Low	0	0	Low			
20.26.33.245	encr_aes_cbc	128	auth_hmac_sha2_256_192	prf_hmac_sha2_256	2048-bit modp group	Critical	24 Dec 2025	4	Low	0	0	Critical			

## 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.



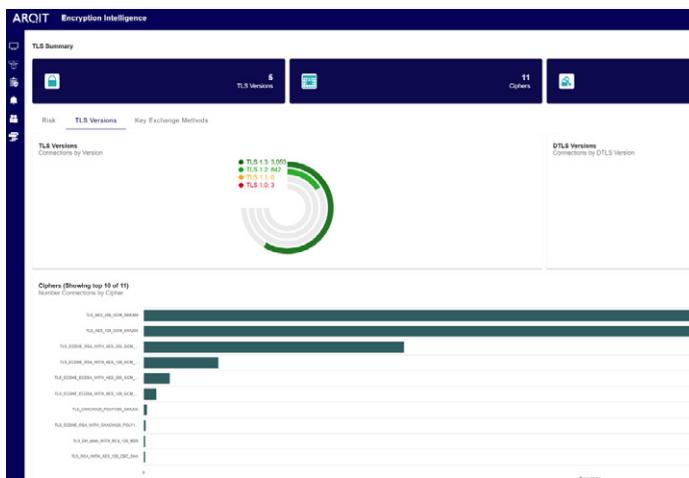
## Arqit Encryption Intelligence

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.



## 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.

### 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.



### Reporting and visualisation to aid decision-makers

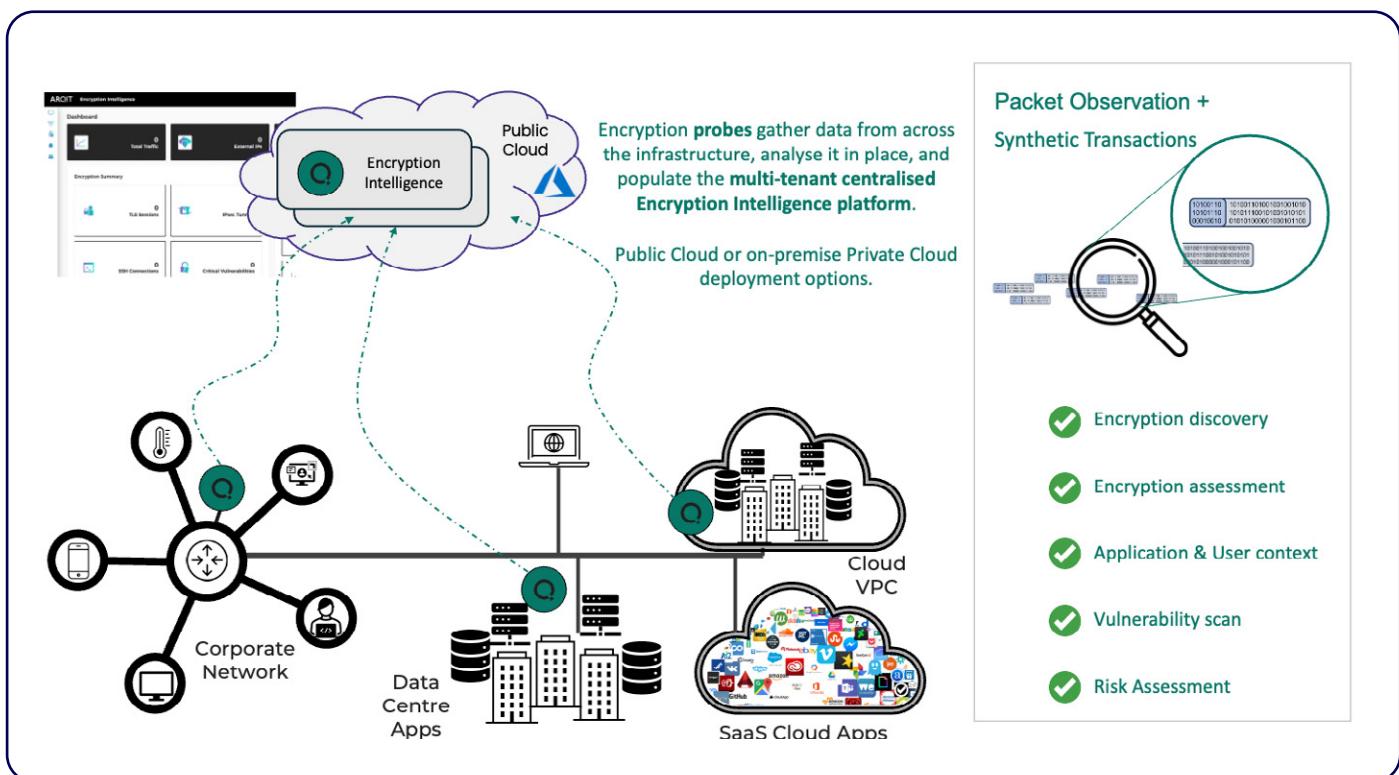
The Encryption Intelligence application has the dashboards and reports that you need to understand your encryption landscape in detail, build a business case to mitigate issues, and manage progress towards full encryption security.

### 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 range of additional services to help your organisation manage encryption risk and plan for the migration to post-quantum cryptography. Please contact us for further details

### Contact us



[Arqitgroup.com](http://Arqitgroup.com)



[consultancy@arqit.uk](mailto: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)