Digital Pathways

Your Data Security Specialists

Digital Pathways, over the last 20 years, has been working in the data protection and cyber security marketplace.

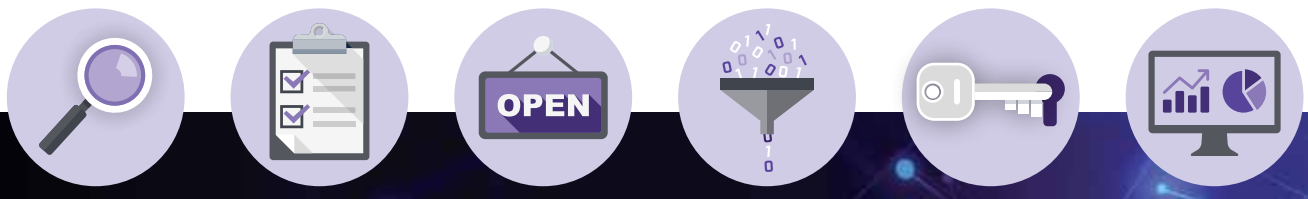
We have a range of solutions and expertise to meet today`s complex requirements for compliance and data privacy including GDPR.

Our success is based on our team of professionals, highly trained in data and cyber security, who have worked extensively in the commercial world and know how solutions work in practice. Theory is the starting block; practical, successful application is the end result.

Digital Pathways has a full range of data security solutions, some of which are also offered as a fully managed service, to match your business needs in a flexible, cost efficient manner.

AREAS WE COVER:

- Data Encryption
- Managed Security Services
- Secure Mobile Voice Recording
- Data Leakage
- Security Gap Analysis
- Smart Buildings and IoT
- Audit and Event Management
- Penetration Testing
- Protective Marking
- User and Session Recording
- Insider Threat Detection
- Incident Management Reporting



Secure Log Management and Reporting

Provides secure log storage and periodic reporting of access to your servers and devices regardless of location.

- Logs are monitored for integrity (the logs are not changed in any way)
- Logs are encrypted with AES256
- Logs are stored in a secure appliance
- Periodic reports are sent via email to nominated individuals detailing the activity specified in the reports
- Raw Logs can be made available at any time for audit or regulatory/law enforcement analysis

User Monitoring and Analytics

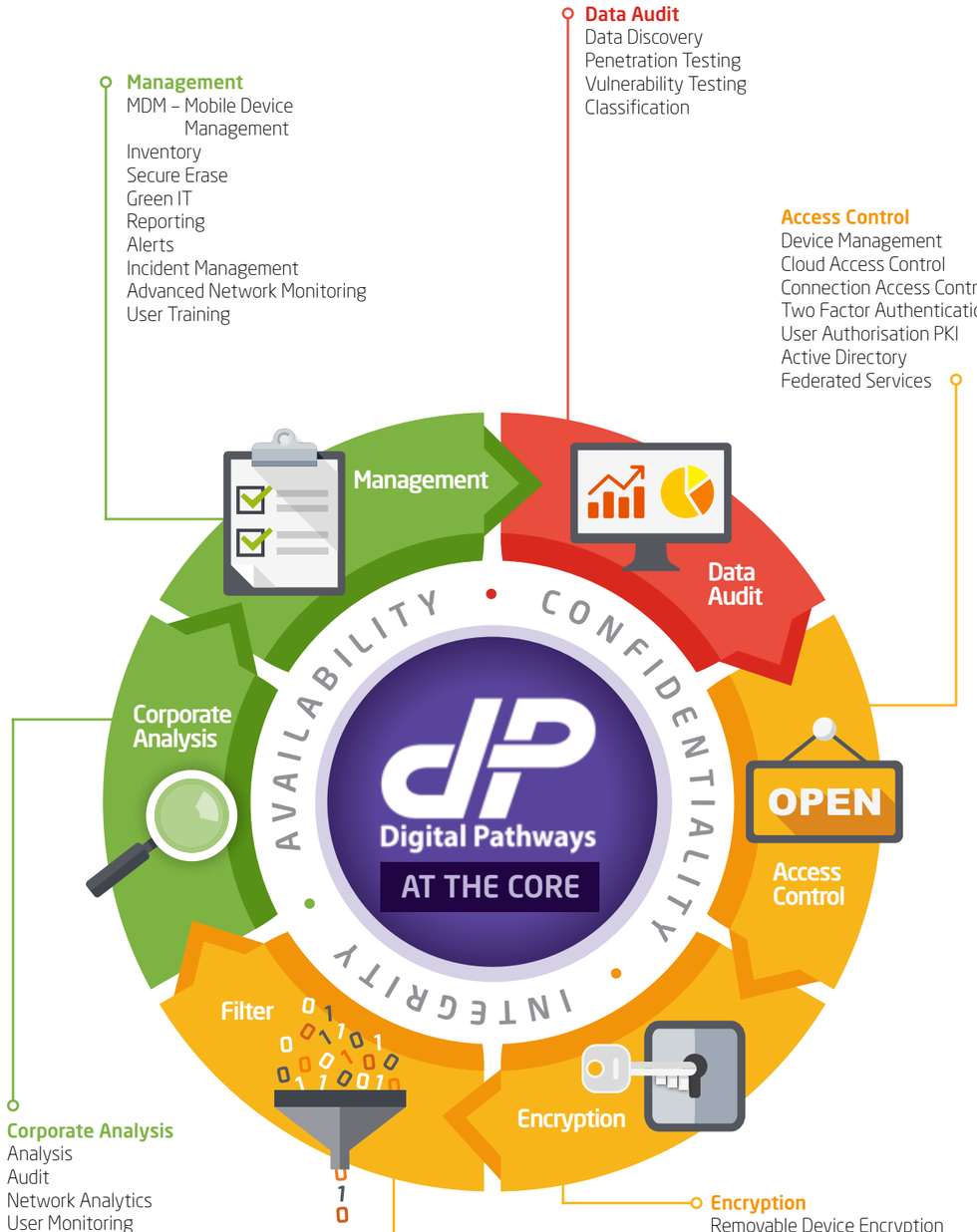
We can enable your organisation to monitor your administrators, third party developers and users in their daily access to corporate resources, and provide instant training on best practice to the individuals via on screen messages. Any session can be recorded if an individual performs an unapproved action. All these statistics are stored and used to provide analytics on a user behaviour, which can be used to trigger an alert to unusual working patterns and prevent a breach before it happens.

- Low impact recording and monitoring
- Clear concise analytics via an informative dashboard
- Customisable messages to improve user understanding of company policies
- Improves user awareness of data security
- Reduces the Insider Threat

Transparent Data Encryption

All formats of data can be protected using our transparent data encryption services for any sensitive information residing on your servers, cloud based, laptops, removable media, smartphones or within your local network environment, without any changes to the server operation or modification to the application.

- Provides cryptographically strong key storage within FIPs certified appliances
- Robust access controls to protected data
- Completely transparent to existing applications
- Very low impact to services and performance
- Strongly protected encryption keys residing within the European Union
- Invisible to authorised users of the data and no training required to use the system
- Database or application level encryption to comply with PCI



Management
MDM – Mobile Device Management
Inventory
Secure Erase
Green IT
Reporting
Alerts
Incident Management
Advanced Network Monitoring
User Training

Data Audit
Data Discovery
Penetration Testing
Vulnerability Testing
Classification

Access Control
Device Management
Cloud Access Control
Connection Access Control
Two Factor Authentication
User Authorisation PKI
Active Directory
Federated Services

Corporate Analysis
Analysis
Audit
Network Analytics
User Monitoring
Penetration Testing
Vulnerability Testing
Intrusion Detection System
SIEM

Filter
Content
Analysis & Filter
Anti-virus
Application Control
Sandbox
DLP – Data Leakage Prevention
Honey Pot

Encryption
Removable Device Encryption
Full Disk Encryption
Pre Boot Authentication
Folder Encryption
Network Encryption
Cloud Encryption
Android Encryption
IOS Encryption
Mail Encryption
Application Encryption
Masking
Pseudonymisation
Tokenisation
Key Management
Data at Rest Encryption
Database Encryption
Key Management

Oracle and Microsoft SQL Server Encryption

We can offer secure Oracle Wallet or MSCAPI secure automated key storage for your cryptographic key material relating to your Oracle or Microsoft SQL servers regardless of its location.

- Secure key storage and management
- Keys not stored with the Database server
- Keys not available to the Database Administrator at any time
- TDE/wallet keys stored in multiple secure tamper proof appliances
- Data can be Tokenized or Masked dependent on the business or compliance requirements
- We have no access to your encryption keys at any time

Automated Server Compliance Auditing and Reporting

By working with you to develop a set of criteria your servers must achieve, we can then integrate this into our automated Auditor Tool to generate periodic compliance reports. This information enables you to track patch levels, software and domain policy, applications and trends across all your servers giving you and your auditor, visual and immediate information on your systems. This is then used to demonstrate your corporation's compliance with regulations, governance and best practice policies.

Managed Gateway and Endpoint Services

We can install, configure and manage your internet gateway, providing:

- Secure email encryption
- Country control (geographical region blocking)
- Gateway e-mail antivirus and spam scanning
- Desktop antivirus device control and encryption
- Web scanning and application control (Skype, Facebook etc.)
- Secured WiFi with guest privileges if required

Managed SIEM Services

By working together with your organisation`s infrastructure, server and network teams we can provide On or Offsite Security Incident and Event Management services, integrating and correlating logs and events from your equipment to provide actionable security intelligence relating to your servers, desktops, mobiles and network infrastructure, delivering periodic reporting and near real time alerting and enabling consistently reliable and effective oversight of your security posture.

Protective Marking of Documents and Emails

We can install and manage a flexible solution for protective marking of any document or email created within your organisation, providing:

- Multi-level options for document classification
- Detailed auditing of document control and violation
- Control of document leakage or inappropriate emailing of information
- Not limited to documents but can be applied to images, PDF`s and Web Outlook emails

Data Audit

Understanding what is going on within a network, or the organisation as a whole is vital for any security strategy. We have a range of services to address this area providing:

- Vulnerability and Gap analysis of the current network and business processes to identify areas of data security weakness
- Penetration Testing both external and internal to identify areas of potential exploit
- Data Discovery to locate sensitive or critical data to then apply appropriate controls to it or move into a secure location
- Classification of data to enable fine grain controls to be added to any type of data making tracing, rights management, ageing or deletion a simple process

Intelligence Management Platform

Given many systems within our networks and buildings are interlinked, with some operating even as an island, it is difficult to ensure all incidents or events are handled in a fashion which follows the company's operating procedures, meets the demands of compliance reporting and even Health and Safety regulations. Our platform, nLiten, ensures all parties report consistently and follow agreed procedures to ensure the business is protected and any incident, from a Cyber attack to a building evacuation, can be reviewed and evidence gained which can be used to report or action at any level in a forensically sound way.

- Ensures standard operating procedures are followed
- Allows for incident escalation and audit trail of decisions made and by whom
- Works with any syslog system, even those using proprietary protocols
- All data is secured and uniquely identified and once entered cannot be altered, ensuring non repudiation of data entry
- Store all forms of data within reports such as CCTV footage, photographs, scanned documents etc.
- Can store service reports to ensure third party service level agreements are maintained
- Provides consistent reporting by any employee or third party
- Reaches out to lone workers, remote guards, travelling employees or executives to enable them to send or receive critical information or alert to any distress

Digital Pathways

Tel: 0844 586 0040
Email: intouch@digitalpathways.co.uk
Web: www.digpath.co.uk

Digital Pathways
Harlow Enterprise Hub,
Edinburgh Way, Harlow, CM20 2NQ