Managed Security Service

Digital Pathways

Your Data Security Specialists

Exective Summary

The Digital Pathways Managed Security Service takes away many of the pain points, including interoperability associated with deploying a robust data protection and auditing system. Our service provides organisation's with reduced costs in terms of encryption deployment, maintenance and management and offers more effective controls through the provision of centralised monitoring, logging and reporting capabilities to ensure an organisation's digital assets remain secure and keeps the company compliant.

nCrypt nSIEM nLiten

Introduction

Managed cloud services such as Cloud Storage (CS), Infrastructure as a Service (IAAS) or Outsourced Server Management (OSM) provide organisations of all sizes with access to the technology services they need in a cost-effective way as opposed to performing these functions in-house.

Using a managed service, via a monthly or annual subscription, means that organisations can access the best technologies appropriate to their business and also means that investment in expensive hardware and software licences, in order to access that technology, becomes unnecessary.

GlobalAwareInternational
Intelligent Software Development & Security Solution Consultants

Global Aware International are market leaders in counter terrorist, security and intelligent software solutions and work for many of the world's 'Blue Chip' companies.

"As a highly regarded protection solutions provider to global companies we wanted to ensure that our own data, and that of all our clients, was robustly protected so that even if a 'hack' situation arose the data would continue to be secured.

"This requirement was not purely driven by best practice but also for the need for reputation and brand protection as well as a requirement of our ISO 2701 accreditation. We have been very impressed with the service, its reliability and the information on activities it is giving us.

"We definitely will be expanding our service with Digital Pathways and feel secure in being able to recommend them to our global client base."

Robin Rumsam
Finance Director, GAI

But these services can leave a company's data exposed to theft, tampering or even seizure by law enforcement agencies from many jurisdictions; exposing the data owner to large fines, bad press and possible business collapse.

The only way to protect the data is by encryption, which renders it unreadable to unauthorised people, allowing monitoring and reporting on who, or what, is accessing the data and when. Many organisations do not have the in-house expertise, the systems or the bandwidth to carry out these 'best practices' to ensure their business is protected against data theft or tampering. This is why many companies take a 'head in the sand' stance and think it won't happen to them, or, deploy a system but never have it optimised to meet their needs.

- EU Data Protection Act 2016 stipulates that all sensitive data must be encrypted with industry recognised coding that are robust and able to handle all formats of data
- PCI DSS standard for storing of credit card information requires all client data to be stored in a secure, encrypted environment, with all access to the data closely audited and monitored
- Company audits now often include elements of data access and compliance. To facilitate these audits companies are required to hold all log data in its raw format. Most organisations fail to store any logs thus fail an audit
- 62% of organisations fail to protect data which has been backed up and either stored in the cloud or within network attached storage servers
- It takes on average 5 minutes to hack a system and 7 months to detect due to the lack of monitoring of systems and data by the majority of organisations

Overview

Digital Pathways Managed Security Service offers functionality that can smooth out many of the problems involved with managing data security systems in-house, control on-going budgetary pressures and separate the duties between cloud service providers, data owners and data protection.

The Digital Pathways nCrypt solution can handle the full range of encryption needs both for data in transit and at rest, including full-data encryption of any server, and is transparent to the application or data structure (databases). This means that encryption and key management are provided as a unified service across all platforms. The Digital Pathways nCrypt solution provides a managed service where the Data Security Manager (DSM) security server appliances are located in a protected Network Operations Centre (NOC) where all encryption keys and security policies are stored. The encryption is enforced at the point of data access whether that is in the cloud or within clients' premises. This provides separation of duty between security policy and data access.

Once deployed the system provides extensive auditing of all access to data, both authorised and unauthorised, which can then be used to report to management on system activities, compliance reporting such as GPG13 and PCI or data breaches where detailed analysis is required across multiple systems to identify any weakness or rogue activity

All reports are generated through nSIEM in an easy to understand format and are emailed to designated contacts on an agreed schedule. All logs gathered not only from nCrypt but also servers, applications or proprietary systems, are stored securely in their raw format to meet auditing requirements but are also available to the client for use in wider reporting and management, internal audits or as evidence during an investigation.

The Digital Pathways Managed Security Service puts enterprise class data security services within the reach of organisations of any size. It allows them to improve their security posture and achieve governance or compliance objectives such as data protection without the need to install complex and expensive solutions nor take on additional staff skilled in the workings of cyber security.

SPECCOM

Specialist Communications offer a range of online trading and reporting solutions for the finance sector.

"A new service we launched was to secure all voice calls and needed a flexible, scalable solution to securely store all calls in a format that could be proven not to have been tampered with.

"We did not want to build our own system and so we turned to Digital Pathways to help build a system which encrypted all call files into a third party managed data store. This 'store' was locked down and only accessed by a registered client. These 'accesses' are logged and provide evidence of who accessed what and when. Given the data is encrypted there is no way an unauthorised person could view the data nor any of the operators within the third party data store.

"The major benefits we found were in transparency to our application, no increase in data volume due to encryption, performance and cost management."

Jonathan Clark
Director at Speccom

Managed Security Services

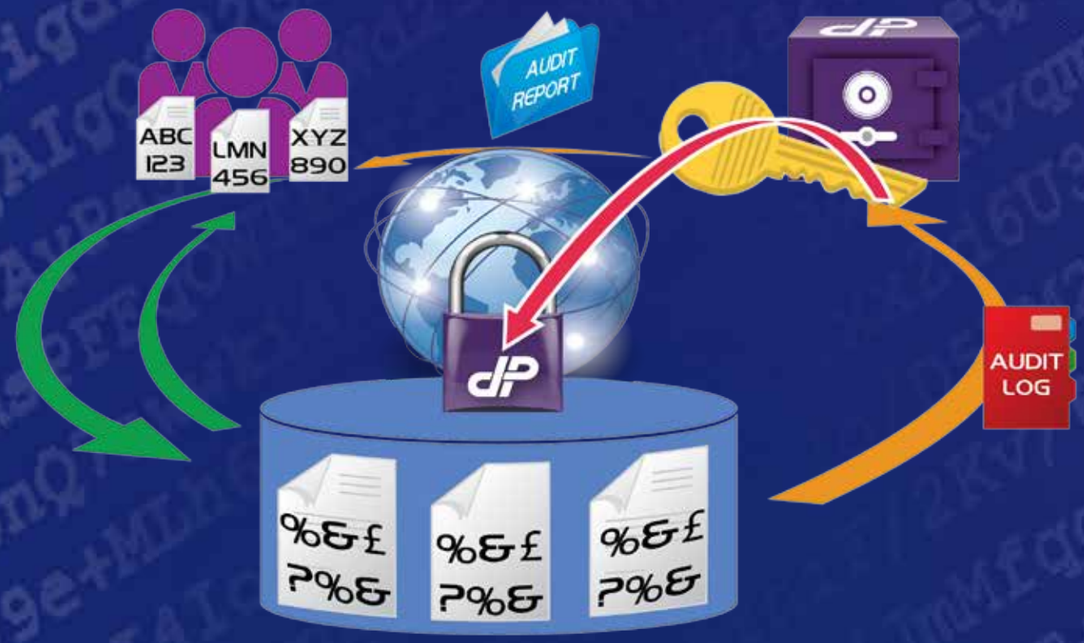
Our Managed Encryption solution, nCrypt, allows your IT administrators to focus on delivering their applications without having to worry about managing their encryption keys, designing security policies or having to go through the pain of modifications to network infrastructures to facilitate a secure operation.

The Managed Encryption solution uses fault tolerant key management appliances held in a secure location on dedicated hardware, communicating securely using mutually authenticated TLS sessions over the internet to an encryption server, which provides the mechanism to perform the encryption and decryption of data at the point of storage.

Our service protects data wherever it is stored. This means that if your data is held within your data centre, in the cloud, third party contractors or even a mixture we can strongly protect the data at rest, allowing you to decide on how each user can access the data and what they can see or do with it.

The service has five modules:

- Transparent data encryption for flat files and databases
- Application level encryption
- Tokenisation or data masking within applications
- Secure key management and storage
- Secure gateway services for Box, Amazon and proprietary NAS/SAN storage



Key Benefits

- **Reduced costs/controlled budgets**
- **'Virtual' In-house security experts**
- **Effective controls**
- **Full reporting and intrusion alerts**
- **Transparent to applications**
- **Compliant**
- **Scales to your needs**
- **Compliance level auditing**
- **Cloud based or on-site data protection**

Future Proof

Over time your encryption needs might mean that you wish to take over control of the security policies for your data or even build your own system. The nCrypt solution easily accommodates this either by:

1. The creation of a secure domain within our system which allows you to manage the security policies and reporting leaving us to simply manage the platform with no access to your security policies or procedures.

2. We can install your own system, train and support you in its operation but transfer all your existing policies from the managed platform onto your own. This minimises the 'down time' involved in bringing up your own system and defining new policies.

nCrypt

Audit & Event Management

Understanding what is going on in a network is very important not only for capacity planning but also to detect unusual behaviour and produce reports to ensure good governance or compliance to the myriad of rules and regulations which face every type of business.

The complexity of diverse logs and the sheer volume of data that is produced often swamps an organisation and makes detection very difficult and therefore frequently ignored. Also logs need to be stored to be used as evidence should the organisation face an audit either by internal divisions, external clients or law enforcement or financial agencies. This storage of raw logs needs to be kept 'untouched' rather than what is termed 'normalised' and should be protected to ensure they cannot be tampered with.

nSIEM is based on industry standard log management controls with Digital Pathways gathering and storing the logs from any server, application or proprietary system in our secure data vaults and encrypted using the nCrypt system. The raw logs are made available to each client, or, pre-defined reports are emailed at set times to selected members within the organisation. All logs can be processed by a rules-driven analysis and anomaly detection engine. This allows for tailored and extensible analytic rules which allow 'questionable' events to be tagged and written to a database for further review and possible alerting. This is achieved through a 'Google' type search on item, providing rapid and effective interactive understanding of any incident. Knowledge gained in this way can provide input to the generation of new automated policies for data access and reports.

Custom reports, real-time alerts, are sent via email to selected individuals and can be created either on the fly or ordered through the Digital Pathways support portal.

Logs are gathered wherever the data servers are located and either consolidated at a location by a locally installed software agent and then batch uploaded or direct streams are established to our nSIEM system. Both forms of transfer are digitally signed using a RSA/SHA256 digital signature which is calculated and the log digitally signed before transfer. Every transfer is authenticated and encrypted using TLS in transit to ensure the integrity of the data.

Once the data is stored within the nSIEM the collected logs are processed by a rules-driven analysis and anomaly detection engine. Flexible and extensible analysis rules allow 'interesting' events to be tagged and written to a database for further analysis and reporting.

nSIEM

Smart Building Reporting

Currently many building management and control room systems operate on proprietary protocols and reporting packages. To compound this, these systems are often on the back-bone network thus making them vulnerable points of entry to exploit not only the building systems but any other data sources on the network.

Other challenges are:

• Standard Operating Procedures (SOPs) are frequently paper based and not easily accessible by all

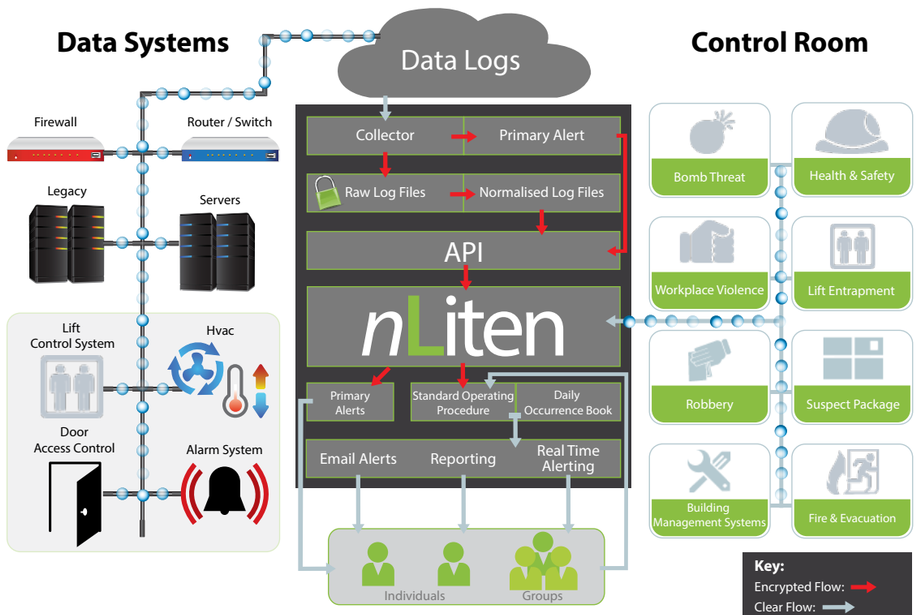
• Lack of reliable, forensically sound incident reporting.

These weaknesses in current building management systems (BMS) mean that ensuring data integrity, consistent incident reporting and following agreed procedures often fail leading to the quality and integrity of the data being challenged.

nLiten is designed to bring these systems, operating procedures and work flows into a unified security portal to enable better management and reporting of incidents and to task operators of systems to confirm integrity of devices or processes should an incident occur.

nLiten is accessed from a web enabled dashboard or via remote terminals to view or initiate daily tasks, access SOP's, escalate incidents such as lift entrapment or control evacuation procedures. All reports can be started during an incident so all decisions taken and the reasons why can be captured and securely stored.

All data collected is held within our secure data center, encrypted by nCrypt and held in client based repositories for retrieval at any time by the client.



nLiten

Service Overview

Technical Information

The Digital Pathways Managed Security Service allows our NOC staff, or yourselves, to create encryption keys (which are totally secure and not viewable by you, or us, under any circumstances) for your application and construct encryption policies allowing you to control which user is accessing the protected data, what applications you wish them to use and when they are allowed to perform these operations.

Once the system has been configured the encryption agent runs transparently in the background encrypting and decrypting data without the user being aware or you having to make any changes to your application.

Our managed encryption service gives you the ability to define how you want to use the service. You can allow our NOC staff the ability to manage your system on your behalf, or, you can assign your own administrators access based on their roles.

The roles available are as follows:

Reporting
The ability to access logs and run reports for their assigned hosts

Key administration
The ability to generate, annotate, retire and delete encryption keys

Security administration
Access to and creation or deletion of encryption policies and hosts

Key Features

- Transparent to all applications - no modifications to application code is required
- Encryption keys are not stored with the protected data
- Access to the data is controlled by user name and or application
- Scales from one to tens of thousands of processing cores real or virtual
- No limit on number of users or applications accessing the data
- Decouples data ownership to data management
- Full audit of access to protected data
- Compliance reporting

Managed encryption keys used

128/256 bit AES
Transport encryption
Mutually authenticated TLS

OS/Infrastructure Requirements

SLES Linux from v11
Redhat enterprise Linux from v5 (not oracle Linux)
Centos from v5
MS Windows server

Filesystems supported

EXT2/3/4
NFSv3
NTFS
Vxfs (on centos/redhat 5,SLES)
ReiserFS (SLES)
LVM (RHEL)

- Data Encryption
- Secure Mobile Voice Recording
- E-Discovery
- Audit & Event Management
- Protective Marking
- Managed Security Services
- Data Leakage
- Smart Building Reporting
- Penetration Testing
- User & Session Recording

Digital Pathways

0844 586 0040 | intouch@digitalpathways.co.uk | www.digpath.co.uk
Harlow Enterprise Hub, Edinburgh Way, Harlow, Essex CM20 2NQ