Outreach Dual Zone: **Protecting data in the public sector**

EQUINITI TOPLEVEL

JUNE 2016

AN UNCOMFORTABLE TRUTH

Connectivity sits at the heart of all we do: digital infrastructure is the foundation for communication and is where critical data is stored.

Digital by Default is dependent on the internet and private networks. Data breaches are on the increase due to a number of factors, from the increased mobility of data to poor enforcement of security policy. This both empowers the public sector and opens up vulnerabilities; what is valuable to you is also valuable to the cyber criminal.

No organisation – whether in the private or public sector is immune to attack, and we have to accept that government organisations are particularly tempting targets for "hacktivists" to cause damage and embarrassment by attaining access to personal data.

Attacks where this data is exposed to unauthorised users can be devastating in loss of time and costs associated with remediating the issue, not to mention the damage done to the reputation of the organisation involved.

Background

With the rise of the internet, the 1998 Data Protection Act (DPA) was passed by Parliament to control the way information is handled and to give legal rights to people who have information stored about them. There are two types of data that the Act is concerned with: personal data is about living people such as name, address, medical details or banking details and sensitive personal data also including racial or ethnic origin, political opinions, religion, membership of a trade union, health and criminal record.

And the forthcoming EU Data Protection Regulation is due to be put to Parliament in 2016. Part of the proposal is that organisations that believe they have suffered a breach will have 72 hours to report it to the Information Commissioner. Encryption is expected to be a saviour in this because if the data lost is encrypted this will be a defence against mandatory breach notification.

Many organisations do not encrypt stored personal data, or perhaps they encrypt stored credit card details but not all personal data.

Outreach Dual Zone: protecting data in the public sector

Ultimately, secure data handling underpins public sector compliance with the Data Protection Act (DPA), the Government Protective Marking Scheme (GPMS) and the EU Data Protection Directive Reform Bill.

Our focus is to make it easier for citizens and public sector staff to use digital services in order to help reduce costs and improve efficiency. To achieve this, it is increasingly important to be able to securely partition data so that different pieces of information can be treated differently and accessed only by specified individuals or teams. One of the primary concerns in putting sensitive data online is, of course, the risk to confidentiality. It is, therefore, important to ensure that individual records cannot be retrieved or altered by unauthorised personnel.

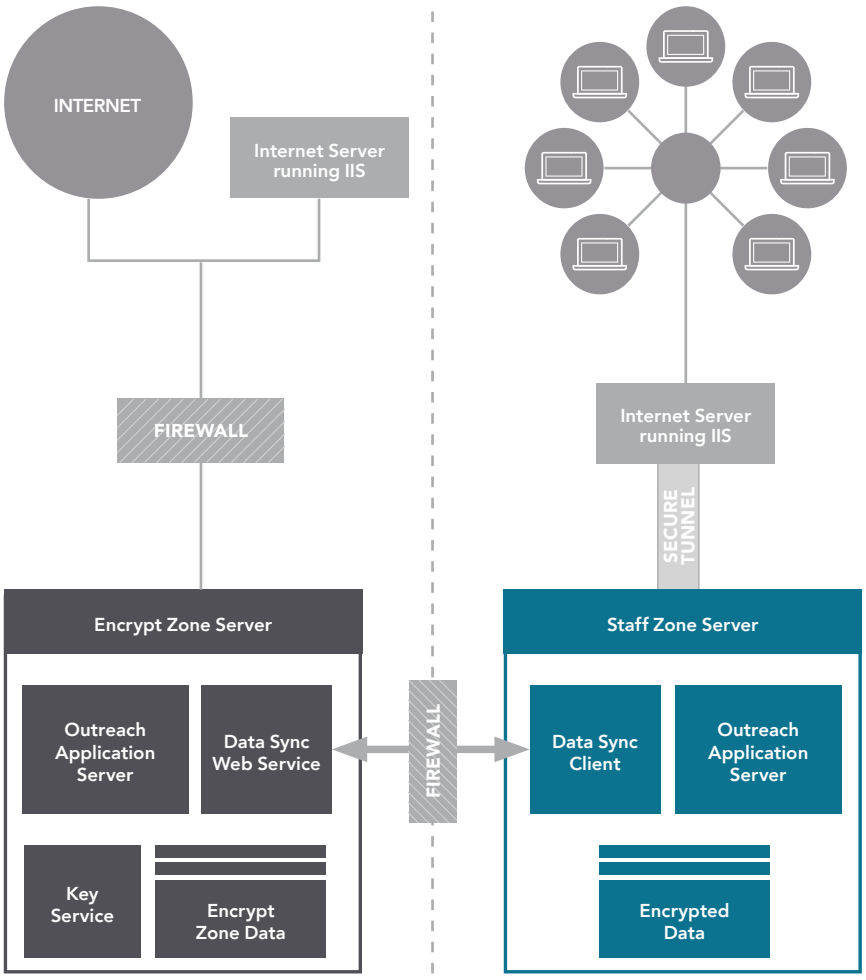
In response to this, and to help solve critical data security and data aggregation issues as well as to support compliance, Toplevel has developed a unique dual server architecture (Dual Zone) option which allows government, customers and outside agencies to communicate and participate through a single joined-up system while keeping all personal information protected and secure.

TREAT CITIZENS AS INDIVIDUALS. TREAT THEIR RECORDS INDIVIDUALLY TOO

Encrypt Zone and Staff Zone which make up the Dual Zone element of Outreach are optional installations with separate agents, servers and stores, but each zone's servers operate in tandem as a single joined-up Case Management and digital services.

Using government-strength encryption (AES 256) and data segmentation, Dual Zone partitions and secures case management data using managed key encryption while still allowing public sector staff, their customers and outside agencies to communicate seamlessly. Because it uses a different encryption key for each customer record, it is much harder for an attacker to compromise and the effort required would act as a deterrent in itself, giving sensitive personal information maximum protection.

The technology features a dual architecture comprising the 'Encrypt Zone' for customers to access encrypted data and the 'Staff Zone' from where case management staff initiate and control communications. See diagram below.



BUILT-IN SECURITY FROM OUTREACH

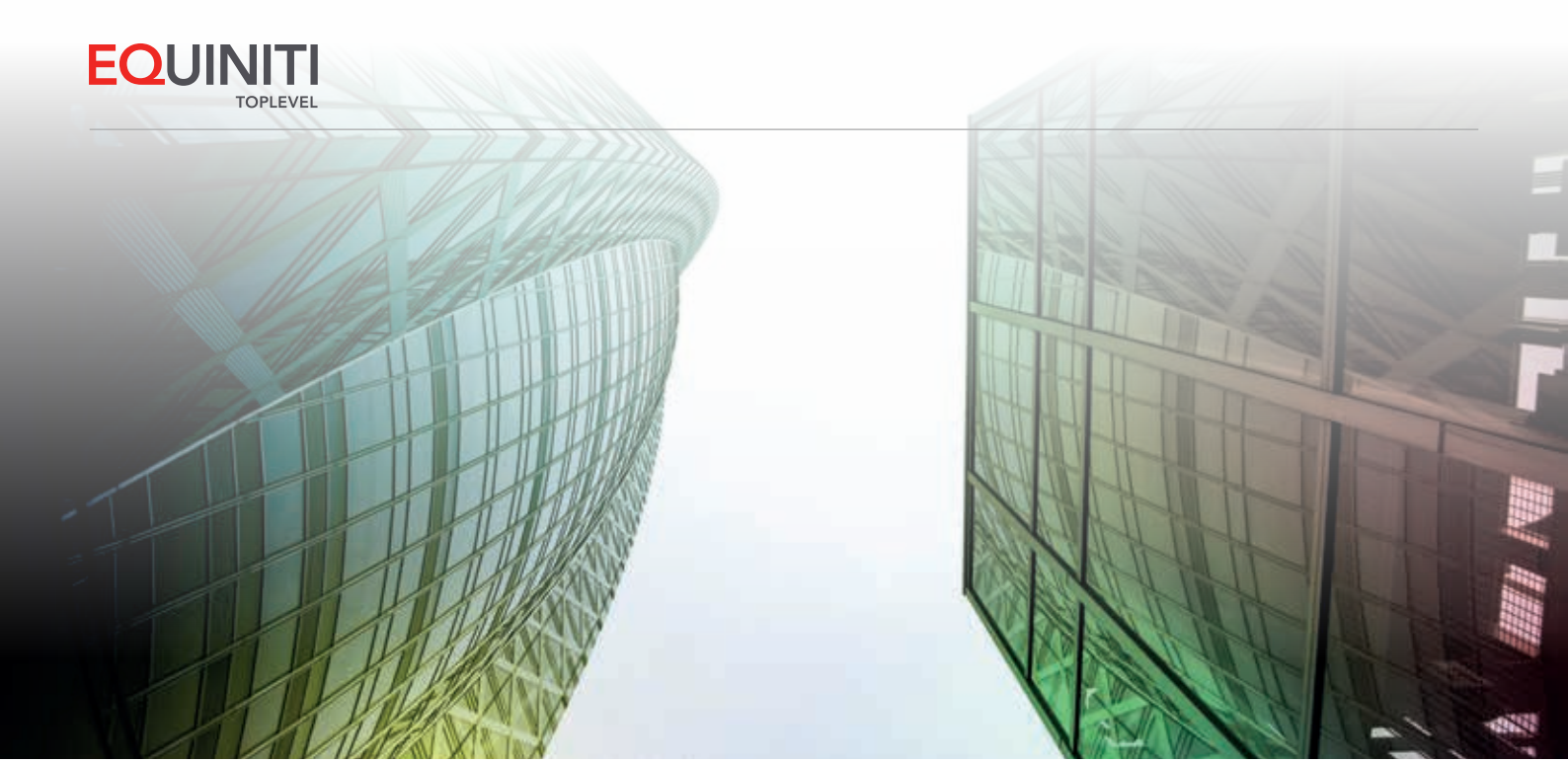
Outreach (Toplevel's secure platform which delivers robust, reliable digital and case management solutions) already has many security controls to protect data from unauthorised access:

- Password protection
- Digital signatures
- Fine grained access control
- One time security codes
- White- and black-listing
- User auditing
- Single sign on functionality
- Strong encryption (AES 256)
- Antivirus integration
- ISAPI support allowing for dual skinned firewall architectures

Challenges with encryption key management

- Key derivation - How are keys generated, rotated and are they asymmetric in design?
- Key storage - Where the keys are held? How are they retrieved? How are tokenising or reversing queries dealt with?
- Key management - Who has access to them? What happens in the event of a compromise (what happens to existing keys)?

As always with encryption, there is a balance to be struck between making sure the keys are available when needed, including for disaster recovery purposes, and not available when they shouldn't be. That's the beauty of Dual Zone.



THE ZONES

Encrypt Zone

Encrypt Zone is an optional security feature whereby data is individually encrypted, each with its own separate key. It adds to the existing controls found in Outreach by using industry standard (AES 256) encryption for the stored data. It connects to the public Internet to allow communication with people and agencies outside of the organisation.

Where compliance rules would otherwise prevent the collection of sensitive data on a system connected to the Internet, Encrypt Zone avoids this by individually encrypting each record with its own separately managed security key. This allows sensitive personal information to be collected and communicated but not stored en masse.

Because each record is encrypted with a different key, breaking into one record by cracking its encryption will not allow an attacker to break into any other record. Where data aggregation rules would otherwise ban the collection of sensitive data on a system connected to the internet, Encrypt Zone avoids this by individually encrypting each record with its own separately managed key. This allows sensitive personal information to be collected and communicated but where all records are not at risk through hacking of an individual record. Key service at Encrypt Zone manages encryption keys separately from the application.

Staff Zone

Staff Zone connects to the organisation's intranet and to the people within it through a secure connection (e.g. VPN / PSN); it does not connect to the external Internet. The Staff Zone server is designed to operate with sensitive aggregated data, allowing staff to process, search and report on the data. It is in complete control of arm's length communication with the Encrypt Zone server to eliminate the possibility of externally initiated cyber-attack.

Encrypt Zone and Staff Zone servers operate in tandem as a single joined-up case management and e-Forms system under the control of the Staff Zone.

The Dual Zone Difference

Other encryption solutions on the market can be applied at the hardware level and at the software level. The unique advantage of Dual Zone is the way it encrypts customer facing records individually, whilst also offering the option to partition customer facing and staff facing data into two separate zones with a different encryption approach for each zone.

This means that we can apply different encryption approaches to the two zones, thereby increasing the security of the customer-facing zone.

In contrast, the use of encryption in the Staff zone is designed so that we can still allow staff to view lists that aggregate multiple customers' information and run reports.

Dual Zone and the Cloud

Many organisations in the public sector are under increasing pressure to deliver more for less through efficiency gains or delivering new and innovative services.

Cloud services represent one of the ways to lower operational costs and free up skilled resources for other important tasks. However, concerns about security and data protection have put the brakes on the adoption of Cloud services – so many businesses continue with on-premise solutions.

Dual Zone gives you the option to adopt the efficiencies of Cloud services as it can be deployed in a number of different ways, from an externally hosted 'Encrypt Zone' and internally housed 'Staff Zone', to a fully hosted solution in a UK-based data centre or the Cloud.

WHY ENCRYPT DATA NOW?

The Information Commissioner's Office (ICO) has the power to issue Civil Monetary Penalties of up to £500,000 for data breaches found to contravene the Data Protection Act, with several organisations fined between £80,000 and £325,000 over recent years. Local government alone has been fined £2.3m over the past five years.

Significantly, there have been examples of individual directors of private organisations being held personally liable for data breaches, facing devastating penalties (up to 5% of turnover) and even serving time in jail. The EU Data Protection Regulation is a regulation not a directive and places more accountability on those responsible for data protection within an organisation (and not only in the private sector). And the upper limit on fines is to be significantly increased. Encryption of data –not only when being accessed or transferred but also at rest – is essential.

The Damage Done

With SC Magazine reporting that 64% of consumers won't do business with breached companies, data loss can destroy business reputations, damage brands and even threaten a business's existence.

Just look at what happened at Sony and Carphone Warehouse, not to mention Talk Talk. And these are just the ones that have been reported –often only after a third party –a partner organisation or even a customer -alerted the company to a breach, and in some cases months after the original breach took place.

Of course, it is not only in the private sector that breaches have highlighted a need for data compliance; there have been some high profile examples within the public sector too. Arguably, the trust of citizens is even more important to maintain.

33%

say responsibility for ensuring data is protected is not clear.

ISBR 2015

CONCLUSION

Dual Zone, as part of our flexible defence-in-depth security approach, has been developed in response to the growing threat of data breaches which all too often hit the headlines, and the regulations put in place to protect information.

As a result, we can provide you with a robust way to demonstrate that strong measures are put in place to protect information.

We understand that the organisations with which we work in the public sector continue to be key targets for cyber criminals and we are committed to, not only keep your systems compliant and your data secure, but also your reputations intact. Like you, we want people to make full use of digital services, but in order to do this, they have to be comfortable that their data isn't at risk.

If you would like to find out more about Dual Zone or our Outreach platform, please take a look at our brochure or call us directly on 01453 852 700 to discuss your specific requirements.

About Equiniti Toplevel

Toplevel provides end-to-end digital and case management solutions that allow Public Sector organisations and individual case-workers to interact more easily with other departments and the citizens they serve.

We improve customer experience and help staff to do their jobs quicker and better by replacing paper, telephone and face-to-face services with more efficient digital alternatives

EQUINITI
TOPLEVEL

Call us now or use the enquiry form on our website to discuss how we can help you deliver your next project
T: +44 (0)1453 852 700

E: email@equiniti-toplevel.com W: www.equiniti-toplevel.com
500 Stonehouse Park, Stonehouse, Gloucestershire, GL10 3UT