On-premise & **in the Cloud**

EQUINITI
TOPLEVEL

JUNE 2016

GOVERNMENT-STRENGTH SECURITY BUILT-IN

This paper aims to share the security strengths of Toplevel's Outreach digital platform and show how Outreach's robust digital security platform enables Agile Digital by Default service development.

Online services have revolutionised the way we live and work, driving economic growth and giving us new ways to connect and co-operate with one another. Falling costs mean accessing the internet has become cheaper and easier, allowing more people in the UK and around the world to use it, feeding the flow of innovation and productivity and reducing time to market. The Government Digital by Default programme brings new opportunities but also new threats.

Along with the advantages brought by the public sector shift from office and paper based services to digital services are the additional threats represented by cyber crime and data loss. Many of the problems are well documented:

- 23% increase in losses per security incident in 2014, whilst in 2015 there was a further 75% increase with organisations reporting over £6m per incident[1].
- Cyber criminals have shifted their targets and are now focusing more on accessing, extracting and selling confidential information.
- Government bodies are particular targets due to their high public profile and the amount of personal data they hold.
- Reputational damage is uppermost as an issue in the mind of public sector bodies, given the responsibility of securing taxpayers' confidential information.
- Denial of service attacks are rising and the severity has grown by more than 73% in the last year[2] and is a particular threat to stored consumer data.
- Data protection. Organisations that are found to have breached data protection rules can be charged up to £500,000 per incident. Local government alone has been fined over £2.3m since 2011.

Toplevel's answer to this security challenge has been to enhance the inbuilt security capabilities of our digital and case management development product Outreach. Outreach is a secure COTS (commercial off-the-shelf) based software product that enables a range of channel shift digital services, compliant with both the Government's Digital by Default Service Standards and HMG's Security Policy Framework.

OUTREACH OVERVIEW – SMART SECURITY BUILT-IN

Built to deliver Government-strength security 'out-of-the-box', all Outreach implementations, whether on-premise or in the (G)Cloud, have e-security built-in with government-strength security testing. Our architecture allows government, customers and outside agencies to interact safely through a single joined-up system.

Outreach is designed to provide a smart 'security-built-in' model for public sector organisations, that demand high levels of security, and delivers a range of out of box security capabilities making it a low-risk, fast deployment product.

Outreach delivers a range of security capabilities to control access to sensitive data through inbuilt password protection, digital signatures, fine grained access control, one time security codes and single sign-on functions, as well as white and black listing and user auditing. Architecturally, Outreach provides inbuilt protection from denial of service attacks, strong encryption (AES 256), antivirus integration and ISAPI allowing for dual skinned firewall architectures.

Outreach implementations have a proven track record of accreditation to IL3 /OFFICIAL Sensitive levels for the likes of organisations such as The Legal Aid Agency and OFSTED.

CYBER PROBLEMS

"Our increasing dependence on cyberspace has brought new risks, risks that key data and systems on which we now rely can be compromised or damaged, in ways that are hard to detect or defend against."

THE RT HON FRANCIS MAUDE MP,
MINISTER OF STATE FOR TRADE (2015-2016).

1 Annual Global Information Security Survey 2015
2 Arbor Networks

OUTREACH SECURITY BENEFITS OUT OF THE BOX

- Used and accredited to host IL3 / OFFICIAL Sensitive information assets in organisations including the Legal Aid Agency and OFSTED. All solutions use the same technology as our high threat customers.
- All sensitive data is protected according to the HMG Security Policy Framework.
- Enhanced protection for citizen data by allowing individual database records and users to be individually encrypted, each with its own separate key.
- Allows the collection of sensitive data on systems connected to the Internet whilst still complying with Data Aggregation rules.
- Inbuilt protection from denial of service attacks.
- Out of the box integration with antivirus and firewall technologies.
- Staff have authorised access, enabling them to access customer data as appropriate to their role.
- Self-service customers are protected from seeing each other's confidential information.
- Independently tested – 2015 example. Pan Government Accreditation (PGA) awarded by CESG for the handling of OFFICIAL data by the Toplevel GCloud e-Forms Software-as-a-Service (SaaS).
- AES 256 encryption (optional) for all data at rest, staff applications and case records.

DEVELOPING AND KEEPING OUTREACH SECURE

Penetration Testing

We commission penetration testing and security reporting on behalf of our customers using different CHECK approved security firms. Recommendations are incorporated into our products' R&D, which means that our entire customer community stands to benefit from reuse and continuous improvement through product security upgrades and enhancements.

OUTREACH'S 'OUT OF THE BOX' SECURITY FEATURES

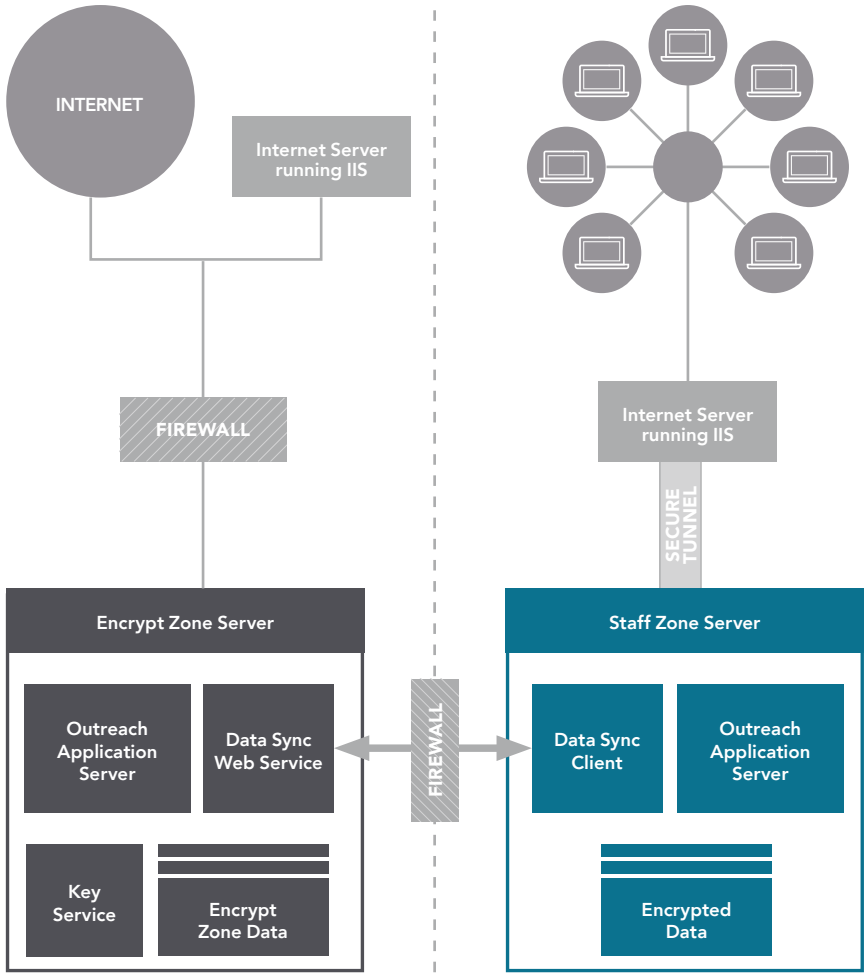
Outreach provides a host of 'out of the box' security features – here is more detail on what we believe are some of the most important features in the product:

Data protection and aggregation

Outreach provides two unique capabilities that support Data Protection Act (DPA) compliance and help futureproof customer environments against upcoming Data Protection Regulations:

- Dual Zone and Staff Zone– dual server architecture option that allows internal staff, citizens and outside agencies to communicate across a single joined-up connection.
- Encrypt Zone – protects citizen data allowing individual database records associated with processes, saved tasks and users to be individually encrypted, each with its own separate key.

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



Encrypt Zone is a 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 and data aggregation 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.

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 digital services system under the control of the Staff Zone.

Identity Management

Configurable user profiles and secure role-based access control underpin a flexible authentication module that delivers permissions based access to functionality and data. Supports single-sign-on and federated environments in which it can either act as the identity provider or be configured as a service provider.

- Single Sign-On – gives users the ability to access other services without the need to constantly reauthenticate and also reduces the number of passwords people require.
- Self-Registration – A security image check (Captcha) containing a security code is displayed to the user, who must supply it back to the registration process before accessing the systems, preventing automatic registration.
- Role-Based Access – Controlled access to sensitive data based on groups and individuals' roles. Changes to authorised users and roles are audited. Administrative staff can view connection audits to track when users have made changes.

Accessibility

- Strong passwords can be mandated for example to: insist on a minimum number of characters, at least one numeric digit, mixed upper and lower case characters or the ability to lock out users after successive failed logon attempts.
- Information on attempted passwords are not stored in the source code of the generated web page. All password fields in the web page are cleared whenever the web page is newly generated or reloaded. This means that information about users' passwords cannot be accessed via failed password attempts either on screen or via the HTML source code of the web page.
- Electronic signatures – Once a data field has been signed, fields are locked so that they cannot be changed.
- Screen access restrictions – Administrative screens can be limited to internal network addresses only.

Usability

- User profile audits – Changes to authorised users and roles are audited meaning that staff can see when changes are made and who made them.
- Co-browsing – Outreach allows call centre staff to answer questions on how to complete a given form by allowing them to see where the customer is having difficulties. The security surrounding this includes i) Citizens must choose to activate co-browsing and can deactivate it at any point, ii) Staff must be given a unique one-time security code by the citizen be able to view the page.

Secure workflows

- Business process management for online services allows routing tasks to the specific individual, role or team responsible for each stage in a process - for example the person authorised to sign off claims or applications.

Business continuity – Denial of Service attack (DoS) protection

Outreach can help mitigate the effect of a DoS attack through configuration of session timeouts, blocking of new sessions whilst still protecting 'good' traffic flows.

- Outreach can identify when session limits of simultaneous users are being reached. For example the system intelligently closes sessions when no data has been received, and reduced timeout criteria may be switched on during periods of high usage.

- Blocking new sessions - When the server is close to the maximum number of sessions, new ones can be blocked.
- Good traffic flows - Selected IP addresses can be configured to be excluded from being blocked. This overcomes situations where known organisations are using NAT (network address translation) which result in multiple PCs legitimately using the service from the same IP address.

Encryption

- Secure HTTP(S) – Mandatory securing of the connection between users and server. (There is also the option to do this selectively for some services if required).
- Full AES 256 encryption option for all data at rest, staff applications and case records, as well as additional password security features around access to failed passwords attempts. Encryption demonstrates that best practice around data protection is being followed and can be used as protection against mandatory breach notifications.
- Internal staff who process, search and report on customer data can have their case records and supporting documents encrypted, futureproofing against data protection regulations.

Antivirus and Firewall integration

- File upload restrictions – Outreach can be configured to only allow upload of files with selected extensions (white list) or to block files with selected file extensions from being uploaded (black list). Outreach integrates with virus checking software to screen each file as it is uploaded.
- Multiple firewall support – Defence in depth. Outreach uses an ISAPI extension to mediate between Microsoft Internet Information Services and Outreach which runs as a service on Windows. This means that the system can be protected by a double firewall for additional security. Similarly the systems database can be installed on a third machine – again protected by a firewall.

OUTREACH SECURITY IN THE CLOUD

For customers who want secure access through a GCloud Software as a Service (SaaS) option, Outreach also sits at the heart of a set of pre-built and configurable online applications. This facilitates digital interactions around self-service appointment bookings, online form presentation and data collection, service eligibility and application processing to case management.

Toplevel is ISO 9001 and ISO 27001 accredited. In addition, we utilise multiple data centre hosting partners for resilience – all of which are ISO 9001/27001 accredited as a minimum - with security levels that meet or exceed those of the best 'private cloud' providers. It is our policy that our operational staff are SC cleared and our GCloud hosting sites conform to the highest levels of physical and cyber security.

This resulted in Outreach's GCloud e-Forms services being awarded Pan Government Accreditation for the handling of OFFICIAL data by CESG in June 2015. Further elements of our GCloud service security approach include:

- Penetration testing of the infrastructure, COTS product and custom web application layer by the security testers.
- Partitioning between web server, application server and database server with firewalls between each partition.
- Hardened operating systems, SQL server and IIS based web services to standards specified by the Security testers.
- Application development processes adhere to OWASP principles.
- Operation of an ITIL-based service department with responsibility for monitoring and maintaining security levels including maintaining patch levels on operating systems, anti-malware software, applications and devices such as firewalls.
- VPN support for data in transit.
- Protect+ virtual private Cloud environment. Advanced segregation techniques; employs increased authentication security for remote support / management. Protect+ has been tested and proved to meet the high standards required for PGA accreditation.

GCLOUD BENEFITS

- ISO 9001 and ISO27001-accredited.
- June 2015 - awarded Pan Government Accreditation for the handling of OFFICIAL data by CESG.
- Used/accredited in major government departments to host IL3 / OFFICIAL Sensitive information assets.
- Regularly penetration tested.
- All customers leverage the benefits of a single protected environment reserved exclusively for them.

AGILE ON ITS OWN IS NOT ENOUGH

At Toplevel we believe that having a simple to use Agile development tool for digital or case management services in a world where security threats are growing and the public sector is becoming a major target is not enough. We hope that our approach of robust 'out of the box' built security features, unique data protection capabilities and the CESG's backing for our GCloud service makes Outreach a great option for organisations where securing official and customer data is a top priority.

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