Croner™
HR · Tax · H&S · Reward

Croner Hosting Services

The Hosting Options, Process Controls and Security models used in Croner's Simply Personnel software platforms.

We know that system security is of paramount importance for all of our clients, which is why we have reinforced systems and options in place to guarantee the best possible protection.

Our standard of service is not at the expense of security. We pride ourselves on offering an invaluable and unrivalled service, coupled with robust processes and controls to maintain solid security.

Hosting Options

Croner provide a data centre to deliver an application platform which utilises best of breed technologies in visualization, data replication and security practices.

These provide a redundant primary data centre, with full site disaster recovery capabilities to a warm secondary site.

Data Centre and Physical Security

Croner provide and support a robust IT platform, through a best of breed UK based data centre.

Key deliverables of this Data Centre provision include, but are not limited to:

- Secondary, warm DR site at remote UK location
- Diverse fibre routing via multiple carriers
- Cross connection to a number of Tier 1 carriers
- Dual Power supply, UPS & onsite generator backup
- Fire, power, weather, temperature, and humidity monitoring
- ISO 9001:2008 & ISO 27001:2013 compliant.

All Croner hosted equipment sits on physical hardware which is completely dedicated to running Croner services alone, and the hosted solution is designed for full high availability – no single point of failure – providing enterprise class resilience.

Isolated directory services ensure that only allowed management servers or approved internal staff are able to access the servers. External access is limited to servers in a DMZ zone, with database servers being further segmented into a restricted security zone, using our full redundant firewall solution, which is only accessible by documented web servers on restricted TCP ports.

Data Centre access is restricted to the minimum number of staff who need access for operational purposes. Access logs are kept and audited monthly. Physical access is limited to remote hands staff and Systems Engineers, and this list is limited to only those who require physical access to replace hardware. There are no console screens in the Data Centre permanently attached to any equipment.

Primary Site Disaster recovery

By maintaining a second UK based data centre, Croner are able to achieve and maintain full site disaster recovery.

We have designed a solution which utilises the latest technologies in virtualization, san and database snapshot and replication.

Data Security and Access Control

Croner takes the security of our customers' data extremely seriously, and all practical measures are made to ensure protection and appropriate access to your data at all times.

Database Server Access: is limited to Systems Engineers; this is handled remotely through Remote Desktop Connections or Virtualization Administration Applications.

Application Access: where passwords are sent to a user, they are set to expire and require change on first login.

Data Backup Process

All production servers and data are backed up daily on an incremental basis, and weekly on a full basis. These backups are retained for one month on a rolling cycle. Using the state of the art snapshot and replication technology deployed on the platform, these backups are replicated to our DR site, so there is redundancy on point in time backups as well as the Croner application across both sites.

Application Support

With a dedicated in-house technical support team, all initial customer queries are answered quickly, and resolved or escalated to other Croner technical teams as required.

Application Monitoring

Croner have engaged with a leading cloud application monitoring program so that at an application level, Croner's support team have the most comprehensive insight into the performance and availability of the software's production platforms.

Release Management

Application Enhancement and Review

System enhancements are built into Croner Products using a standard Agile software development methodology. We use a consultative approach of involving clients heavily in determining system requirements which are then turned into specifications, which are prioritized for release and included into the product roadmap.

Once a software release commences, agreed scope items are worked through using an Agile approach to develop and test in three week 'sprints'.

Once a sprint is completed, end to end testing is performed to ensure the accuracy of the new enhancements and the existing system functionality. Software is then packaged and released, and often beta tested by designated clients.

Security is ensured via code reviews, standards reviews, and thorough testing of all new and revised components which link into the security model of the application.

Security

Security is critical to our business and is not something we take lightly.

To ensure that your data is protected to the highest possible security level our data centres are located in Europe's two most secure data centres - The Bunker in Newbury, Berkshire and in Ash, Kent. Both sites are accredited and certified to ISO27001 and PCI DSS security standards.

We employ multiple strategies to keep your data safe and inaccessible to third parties.

Physical Security

Our primary data centre, The Bunker in Newbury, is an ex-MOD base situated on Greenham Common, which was built as a nuclear command and control centre.

Our secondary data centre, The Bunker in Ash, was built as a NATO Radar Station to protect people and technology from nuclear attacks.

Both sites guard our systems and data from every potential threat or disaster that could compromise the availability and safety of your business critical data.

Specific security features include:

- **Steel reinforced blast proof walls**
- **Military electro magnetic pulse protection**
- **Solid steel doors**
- **Tempest RFI intrusion protection**
- **CCTV**
- **Sophisticated access controls**
- **Fire suppression system**
- **24-hour video recording**
- **Visual verification of all persons entering the data floor**
- **No unescorted access**

The security of your data is paramount therefore we provide the following safeguards:

All transmissions over the Internet to and from your remote desktop are encrypted. We use SSL encryption – the same as that used for online banking and secure payments.

Additional protection is provided by enterprise grade firewalls on our network, with antivirus, anti-spyware and content filtering systems all with intrusion detection protection (IPS) on our systems to monitor and block any unauthorised access.

All security systems are backed up by certificates issued by trusted authorities to ensure they are trusted.

Each customer's data is partitioned in separate storage containers to ensure there is no possibility of unauthorised access.

Random generated passwords.

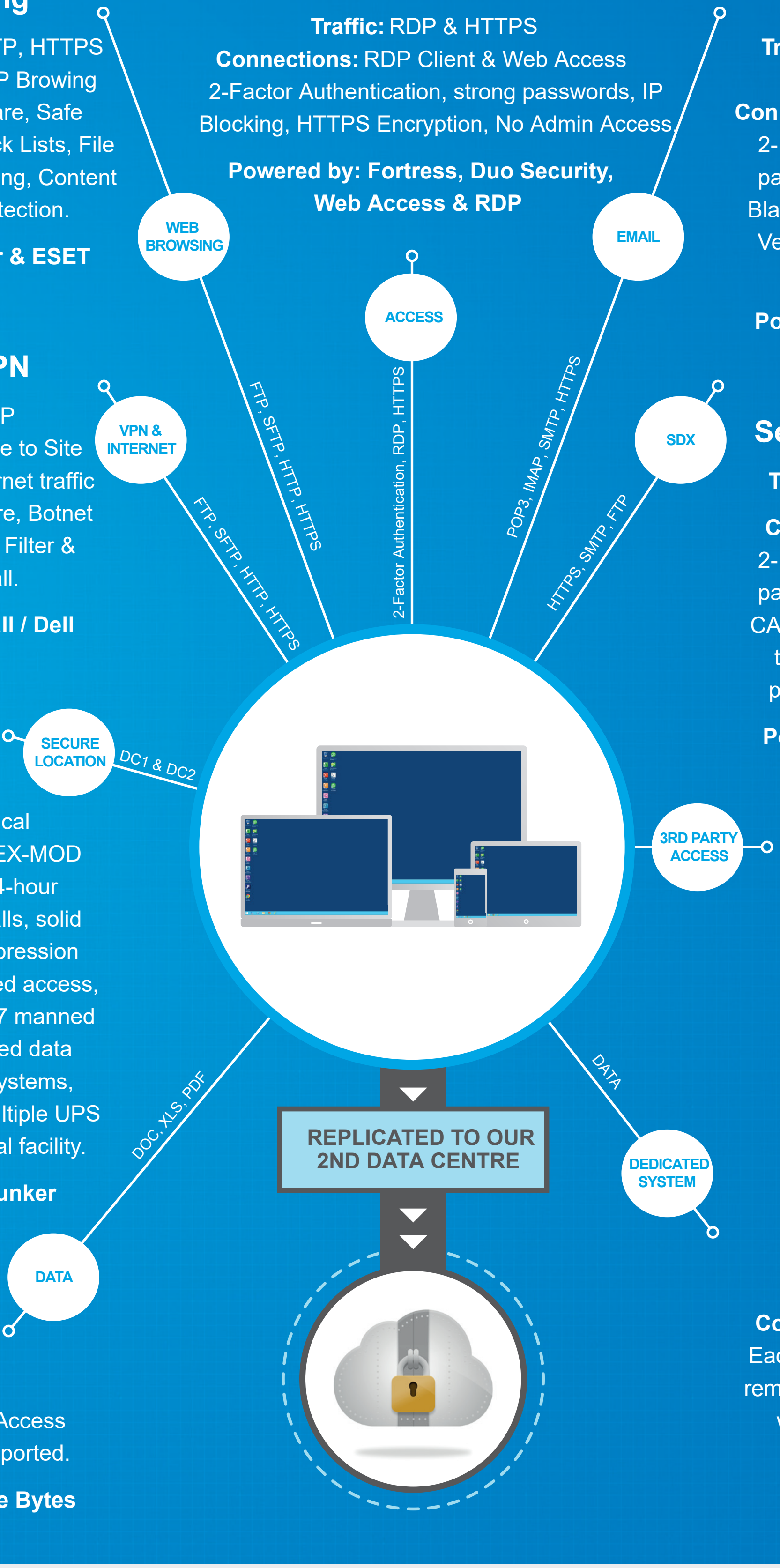
The only people with access to your data, outside of your organisation, are our staff with restricted access provided to certain trusted software providers once authorised by the customer.

All data stays in the UK.

With your business data never leaving the secure remove desktop environment, there is no risk of it being stolen on a portable device such as a laptop.

Remote desktops offer unparalleled data safety and security, which cannot be matched by a normal desktop PC set up.

Security Measures



Web Browsing

Traffic: FTP, SFTP, HTTP, HTTPS
Connections: Web & FTP Browing
Anti-Virus, Anti-Spyware, Safe Browsing, Dynamic Block Lists, File Type blocking, Ad blocking, Content blocking, privacy protection.

Powered by: WebFilter & ESET

HD Access

Traffic: RDP & HTTPS
Connections: RDP Client & Web Access
2-Factor Authentication, strong passwords, IP Blocking, HTTPS Encryption, No Admin Access.

Powered by: Fortress, Duo Security, Web Access & RDP

Email

Traffic: POP3, IMAP, SMTP, HTTPS
Connections: Mail & Web Client
2-Factor Authentication, strong passwords, HTTPS Encryption, Blacklists, SPF, Rate limits, DKIM Verification, Anti-Virus, GTUBE tests etc.

Powered by: Email Filtering & ClamAV

Internet & VPN

Traffic: TCP, UDP
Connections: IPSec Site to Site Encrypted VPN & Internet traffic
Anti-Virus, Anti-Spyware, Botnet Filters, IPS, Content Filter & Hardware Firewall.

Powered by: Sonicwall / Dell

Secure Doc Exchange

Traffic: HTTPS, SMTP, FTP

Connections: Web Client
2-Factor Authentication, strong passwords, HTTPS Encryption, CAPTCHA protection, Anti-Virus, trackable links, Brute Force protection, time limited links.

Powered by: Duo Security & SDX & ClamAV

Data Centres

Traffic: Physical
Connections: Physical
ISO27001 Certified, EX-MOD secure locations, 24-hour CCTV, blast proof walls, solid steel doors, Fire suppression systems, No unescorted access, Tempest RFI IPS, 24/7 manned security, EMP shielded data floors, N+1 cooling systems, backup generators, multiple UPS systems, carrier neutral facility.

Powered by: The Bunker

3rd Party Access

Traffic: Remote Access/ Software companies
Connections: Remote Access app
Validated by client, monitored by data centre staff.

Data

Traffic: Data
Connections: Local Access
Daily scanned & reported.

Powered by: Malware Bytes

Dedicated System

Traffic: Data
Connections: Local Access
Each firm has their own dedicated remote desktop platform separated with Firewalls on both sides.

Powered by: Microsoft & Sonicwall / Dell

Let's Talk

PHONE 0808 145 3386
ONLINE croner.co.uk

Croner™
HR · Tax · H&S · Reward