e2e assure

E2E SECURE CLOUD CONNECT SERVICE - SERVICE DEFINITION DOCUMENT

Overview

A cloud connectivity service that connects users, devices, offices and clouds together over the Internet and other Government secure networks. We can provide all the security and service advantages of commissioning dedicated private links but much more quickly, cost effectively and flexibly by providing a secure resilient gateway that creates a complete VPN and security hub.

Our service enables you to consume the benefits of the cloud without compromising security and affordability. There are four typical scenarios in which our service is used:

- To establish fixed secure VPNs between clouds and between cloud services and customer p networks
- To provide mobile workforces with secure remote access to line of business applications and cloud applications
- To rapidly establish highly secure Internet or Cloud Gateways
- To establish and manage secure mobile devices enabling flexible business practices (includes provision of MDM)

Organisations can choose a service that suits their security and connectivity requirements. The service includes VPN clients that support Windows, Mac, Linux, most tablets, and phones to provide secure anywhere access to cloud resources. This is a cloud independent service which can connect any cloud together and provide high levels of security, provide necessary compliance evidence, and that can flex along with your business needs.

Features

- Securely connects clouds and users together
- Creates a 'security blanket' wrap around all the cloud services
- Provides fixed VPNs for intra-cloud and cloud to customer connectivity
- Provides secure Remote Access and mobile client VPNs
- Fixed and Mobile VPNs include threat monitoring/IDS/AV/Botnet scanning
- Provides Secure Internet Gateway/Cloud Gateway with assured proxy and filtering services
- Monitoring provides Web, AV, IPS/IDS scanning, botnet detection, SMTP, DNS/NTP
- Provides SSL Breakout and Traffic inspection with flexible scaling on demand
- Mobile Device Management services available
- All Cloud Connect services have the option of additional protective monitoring
- Suitable for handling COMMERCIAL through to OFFICIAL SENSITIVE data

Benefits

- ✓ Reduced cost of security monitoring, increased security coverage
- ✓ End-to-end business security confidence and essential security audit assurance
- ✓ Allows you to connect, leverage, use and manage cloud resources securely
- ✓ Reduced exposure to the cyber threat, provides incident response
- ✓ Helps you comply with standards such as ISO27001 and CES+
- ✓ Simplify and reduce your cloud access methods
- ✓ Ensure all cloud access is centrally audited, monitored, and logged
- ✓ Enables connection to Government secure cloud services with built-in compliance
- ✓ Speed of delivery, available now, setup within 2 weeks
- ✓ Cloud agnostic (including private clouds, public and hybrid clouds, Azure, Office365, AWS, Skyscape, Google)

Why is Cloud Connect needed?

Cloud services can offer outstanding value for money but the connectivity to and from the cloud is often overlooked. e2e's Secure Cloud Connect Service takes away all the challenge of implementing and managing the connectivity required to consume the services securely.

Our Cloud Connect service reduces an organisation's exposure to threats by consolidating all cloud connectivity into a single security gateway that cleanses and monitors all your traffic.

The service provides a complete VPN and security hub that provides strong encryption with certificate based, always-on full tunnel client/mobile VPNs as well as on demand, two-factor based thin client style connectivity from appropriately secured devices.

Our gateway provides in-line antivirus scanning, intrusion prevention and also optional protective monitoring.

You can also choose to close down all other outbound internet access from your other corporate services, other than the Cloud Connect VPNs, and take advantage of our proxy services to dramatically increase your business security and simplify your cloud landscape. We can provide Web, DNS, NTP, SMTP and SSL Breakout proxy services reducing your organisation's exposure to internet borne attacks. You can quickly deploy assured protective monitoring to your business services without the cost and delay of the design, development, testing, assurance, and implementation process. Using our service it is possible to consolidate all your gateways into one central, protectively monitored, secure gateway leading to reduced management costs and a reduction in the corporate attack surface. Existing gateway services can be extended without impacting the risk profiles of your business services.

When it comes to cyber defence our service will give you a real-time view of the active cyber threats to your network and data, helping you gain insight to the actual risks facing your business faces. The service actively defends your organisation; blocking malicious traffic and ensuring your business traffic is threat free using a large cloud based open source and commercial threat intelligence system. Central DDOS services protect you from traffic overloads.

We can help you flexibly and securely deploy and manage all your Mobile devices and help you reduce risks to these devices or your corporate infrastructure.

Drawing on our many years of experience providing highly secure services to the UK Government, and Military our service is designed to the highest security standards and follows NCSC best practice and architectural guidelines. All our services are ISO27001:2013 and CES+ certified, suitable for handling COMMERCIAL through to OFFICIAL SENSITIVE data.

The e2e Cloud Connect Services

This is a fully managed service that covers the creation of the Fixed VPNs, provision of the Mobile VPN devices and Cloud Connect security services. Each customer solution has dedicated VPN devices at the e2e datacentre and customers can either use existing VPN devices or e2e provided devices at their managed VPN end points. NCSC CPA foundation approved products are used to establish all VPNs.

Cloud Connect Secure Fixed VPN Service

Our Cloud Connect service provides Fixed VPN connectivity between clouds, and between clouds and your non-cloud business services. This service comes with high levels of security to ensure that all traffic passing between the clouds is monitored for threats and appropriate alerts are raised. Security components include the following (subject to the type of traffic being monitored):

- Threat Alerting
- Threat Indicator detection
- Malware Detection
- Botnet Detection (traffic type dependent)
- SPAM detection and blocking (traffic type dependent)
- Network Antivirus (traffic type dependent)
- Intrusion Prevention (traffic type dependent)
- Trojan Prevention (traffic type dependent)
- Protective Monitoring Options Including
    - DNS analysis
    - Traffic Analysis
    - Packet Analysis
    - Network IDS
    - DNS Inspection

There are multiple levels of protective monitoring available. Should you wish to have more than alerting we can provide incident response and full incident management with our Protective Monitoring options.

Cloud Connect Secure Mobile VPN Service

Mobile workforce monitoring

With the expansion of mobile and remote working, and the consequent fluidity of working environments, our service offers some unique Protective Monitoring and alerting features:

Geo alerting

It is possible to define acceptable location policies that control which countries your personnel can connect from when travelling. Once defined we monitor your mobile devices and alert should a breach occur.

Location reputation checking

It is possible to define in our system which types of environment are acceptable for use by your mobile work force. Our service monitors the environments your mobile devices are in (such as a coffee shop, hotel Wi-Fi, airport Wi-Fi, or other known compromised networks) and alerts if a potential policy breach has occurred. Our service determines and alerts on how private a mobile users internet link is. Many environments pose serious threats to privacy either by enabling an attacker to sweep up all communications on a compromised network, providing compromised network elements (such as DNS services) from which to attack, or by spying on a mobile device with cameras or close proximity individuals.

Identification of compromised home networks

Home working is becoming a norm and although it offers great flexibility, organisations cannot rely on the security of the home environments. Although it is possible to encrypt mobile devices and communications, corporate assets are still vulnerable to attacks from a compromised home network. Many home routers are insecure and traffic and user behaviour will often reveal much insight to an attacker. This could lead to data loss, reputational damage, or corporate compromise. Our service can identify and alert when a home network is compromised.

Cloud Connect Secure Gateway Proxy services

Our Cloud Connect Secure Internet Gateway Proxy Service enables you to quickly secure your organisations perimeter. Our service provides a range of individual security services. It's possible to take on individual capabilities and add to these incrementally in line with your business growth.

You will need to configure all your services to point to a cluster of proxy services in e2e's cloud services and close down all other outbound internet access from your other services other than these Fixed VPNs. We provision these proxy services per customer providing segregation of customer traffic as it passes through the service. This dramatically increases your security and simplifies your cloud landscape. If required we can also provide SSL inspection of all outgoing HTTPS traffic to look for threats buried in encrypted traffic. This method of cloud security is highly effective at bringing your gateway or cloud services under control and allows us to identify anomalous traffic by its characteristics as well as by matching against known threats.

Traffic reaching our Cloud Connect service passes through one or more different security services which include:

Web proxy service

- Web filtering – Examines web traffic and blocks unauthorised content
- Web proxy – Protects your organisation by using our web proxy to examine application requests for anomalous behaviour
- Web category blocking – Protects your organisation and personnel from inappropriate web sites
- Web policy enforcement – Monitors and Enforces corporate web usage policies
- Web blacklist blocking – Prevents sites known to carry threats from being accessed or from communicating with your corporate resources
- Web whitelisting - Restricts corporate access to a known list of authorised web sites
- Web traffic antivirus – Monitors all corporate web traffic for internet borne malware
- DNS proxy – Protects against DNS attacks by using our secure DNS proxy services
- DNS filtering – Filters DNS requests to prevent Botnet or other internet attacks compromising your organisation
- NTP service – Uses our NTP service to protect against amplification DDOS attacks launched on NTP servers which can disrupt or disable business services
- Botnet Detection – Uses our service to detect and prevent Botnet subversion
- Premium Services also include Data Loss Prevention (DLP) and APT Detection

SMTP Proxy Service

- SMTP proxy – uses our service to secure your external mail and detect malware and Trojans

SSL Inspection Service

- SSL inspection – Uses our service to look for threats buried in encrypted traffic

Additional Protective Monitoring services

- Trojan prevention – uses our service to prevent internet borne Trojans entering your organisation Web traffic IPS – implements web intrusion protection to monitor and secure your corporate web traffic from threats within web packet streams
- Web traffic logging – Logs web traffic to support forensic investigations and to provide enhanced situational awareness for improved anomaly detection
- Web packet logging – Captures web traffic to support forensic security analysis and better incident response
- DNS inspection – Inspects DNS requests to gain insight into the behaviour of corporate resources to ensure that external communications are understood and follow expected patterns of use

Our gateway service has been designed by senior security architects . Our services are CES+ Certified and ISO27001:2013 Certified, located in secure UK datacentres, and are operated using ISO27001:2013 certificated processes. All our staff are UK based and hold SC clearance as a minimum. This means that our gateway service can support your legal and regulatory compliance obligations, support your assurance requirements for connectivity to other government services and can immediately enhance your protective monitoring capability and reduce your organisations exposure to external threats.

Secure Domain Controller Service

Provides a Windows Domain Controller with Anti-Virus Console, Managed Patching with an internal file sharing capability (1TB) with backup. There is an option to provide Managed Endpoint Anti-Virus per Device.

Mobile Device Management Service

The Cloud Connect service is designed to securely deploy and manage mobile devices. This allows your organisation to quickly support mobile working, providing protection to corporate systems without incurring the delay and costs of designing a service, taking this through accreditation, and supporting it going forward. Our services are very flexible and can scale up or down as your business needs change. We can provide you with mobile devices or can enrol existing corporate or personal devices as required. We protectively monitor both of our service options alerting you when a device fails a compliance policy and can provide enhanced protective monitoring to manage compliance failures and security incidents for you. The fully managed MDM service provides all software and gateways services based in our secure cloud with secure links to customer clouds and applications.

Service details

Our service supports a diverse fleet of Android, Apple iOS, BlackBerry, Mac OS, Symbian and Windows devices. It can help you leverage existing corporate investment and utilise BYOD configurations. It provides device and user security, Application, content, email, and network security, and supports your compliance responsibilities.

Our service:

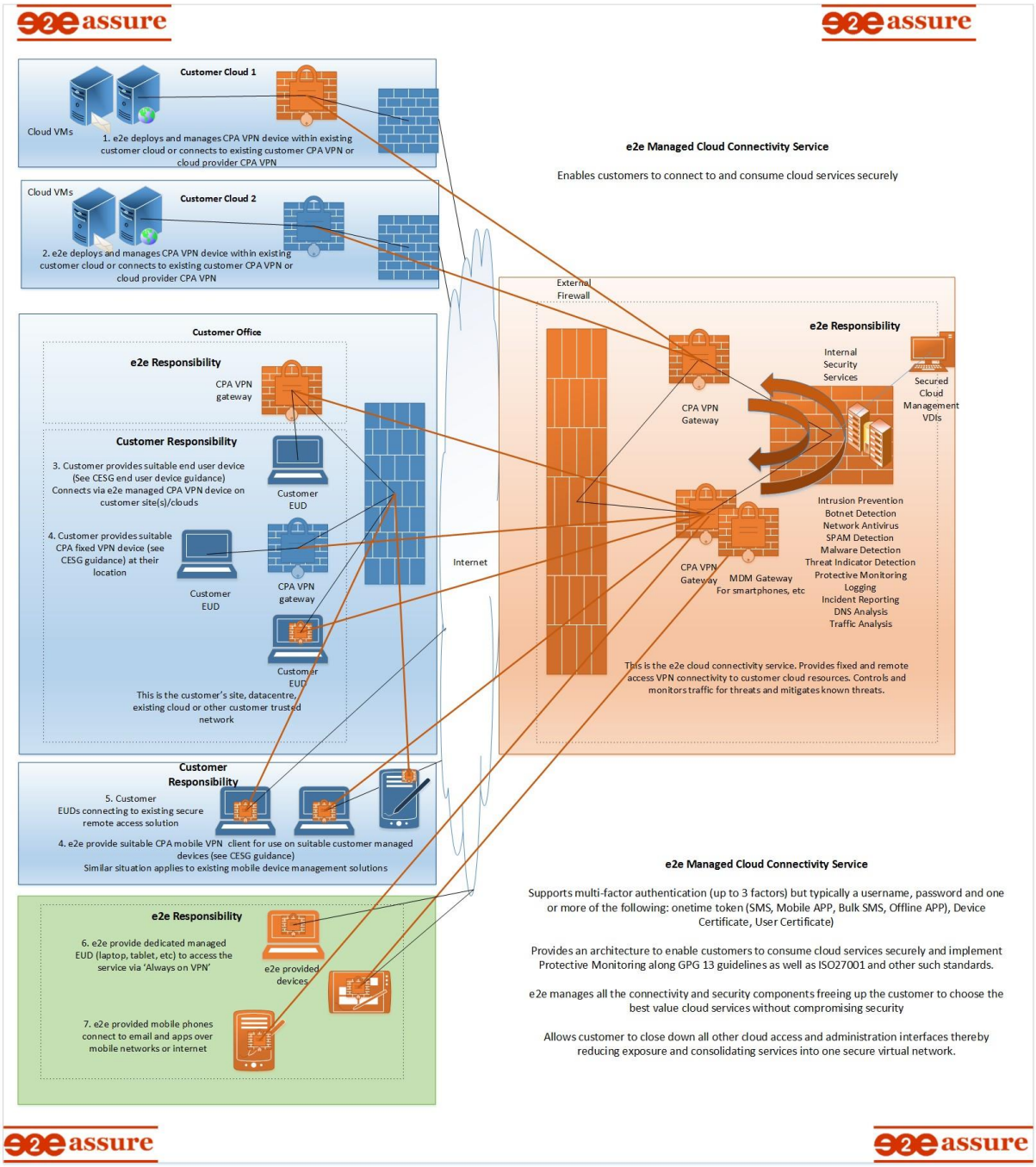
- Manages and controls iOS, Android, Symbian, Mac OS, Blackberry, and Windows Phone devices
- Configures device policies for content and web browsing, and deploys them over-the-air
- Enforces built-in security features such as passcodes and device encryption
- Supports application execution with whitelists and blacklists
- Supports a Content Locker that securely stores corporate content and keeps (FIPS-140 compliant 256-bit SSL encryption) allowing location and time-based access, and printing restrictions
- Can secure corporate email and attachments within a secure device container, restricting access to features such as copy/paste and using a secure mail client
- Can remotely locate, lock, and wipe devices erasing all container contents
- Provides full loss and theft protection for lost or stolen devices
- Can provide corporate documents to user devices
- Monitors device compliance ensuring that devices do not pose a threat to your business

Relationships between our Cloud Connect Service options

Service Name	Fixed VPN	Mobile VPN	MDM services	Proxy Services	Comments
Fixed VPN	N/A	N/A	Optional	Optional	Allows connectivity between private and public clouds, clouds and corporate networks
Mobile VPN	1 minimum	N/A	Optional	Optional	Allows mobile users to connect to a fixed destination
Secure Gateway Proxy Services	Optional	Optional	Optional	N/A	Standalone or can be deployed in conjunction with fixed. Mobile, and MDM services
MDM Service	1 minimum	1 minimum	N/A	Optional	MDM services need to have one mobile client and be able to connect to one fixed destination as a minimum

e2e Secure Cloud Connect Service – Connectivity options and responsibilities

The service level is designed to offer a level of security that fits your organisations risk appetite and business goals. Every service is designed to a set pattern with levels differentiated by service, support, and security features. The diagram below illustrates how the service works.



The diagram above shows the managed cloud on the right. Items in blue are the customer's responsibility and items in orange and green are e2e's responsibility. The service is designed to be consumed over the Internet using IPSec VPNs or TLS encryption. e2e can provide an optional dedicated VPN device at any of the customers' locations in order to provide a managed site to site VPN service. The customer can also choose to provide their own fixed VPN endpoint. Remote access VPNs follow the same pattern; e2e can provide a VPN client or the customer can use their existing VPN client (so long as it is a NCSC CPA foundation approved product).

e2e Secure Cloud Connect Service levels of service

Baseline		
Target Availability/Month (during service hours)	99.50%	
Service Hours	8am to 6pm Mon-Fri [1]	
	Response Time Target	**Resolution Time Target**
Service Incident - First Response/Resolution Time Target (CRITICAL)	4 hours	16 hours
Service Incident - First Response/Resolution Time Target (HIGH)	8 hours	24 hours
Service Incident - First Response/Resolution Time Target (MEDIUM)	24 hours	5 days
Service Incident - First Response/Resolution Time Target (LOW)	24 hours	10 days
Service Incident - First Response/Resolution Time Target (INFORMATIONAL)	n/a	n/a
Service Request - First Response/Resolution Time Target (CRITICAL)	8 hours	16 hours
Service Request - First Response /Resolution Time Target (HIGH)	16 hours	5 days
Service Request - First Response/Resolution Time Target (MEDIUM)	16 hours	5 days
Service Request - First Response/Resolution Time Target (LOW)	16 hours	5 days
Service Request - First Response/Resolution Time Target (INFORMATIONAL)	n/a	n/a
Protective Monitoring Service	Optional (Baseline recommended)	
Onward Internet Connection	Included up to 100Mbit/s	
DOS and DDOS Protection	Not Provided	
Security features	Mobile VPN, fixed VPN, double-tier firewalls, two factor authentication	

Enhanced		
Target Availability/Month (during service hours)	99.90%	
Service Hours	8am to 6pm Mon-Fri [1]	
	Response Time Target	**Resolution Time Target**
Service Incident - First Response/Resolution Time Target (CRITICAL)	2 hours	8 hours
Service Incident - First Response/Resolution Time Target (HIGH)	4 hours	16 hours

Service Incident - First Response/Resolution Time Target (MEDIUM)	8 hours	4 days
Service Incident - First Response/Resolution Time Target (LOW)	16 hours	7 days
Service Incident - First Response/Resolution Time Target (INFORMATIONAL)	n/a	n/a
Service Request - First Response/Resolution Time Target (CRITICAL)	6 hours	12 hours
Service Request - First Response /Resolution Time Target (HIGH)	12 hours	3 days
Service Request - First Response/Resolution Time Target (MEDIUM)	12h	3 days
Service Request - First Response/Resolution Time Target (LOW)	12h	3 days
Service Request - First Response/Resolution Time Target (INFORMATIONAL)	n/a	n/a
Protective Monitoring Service	Optional (Enhanced recommended)	
Onward Internet Connection	Included up to 100Mbit/s	
DOS and DDOS Protection	**Provided**	
Security features	Mobile VPN, fixed VPN, double-tier firewalls, two- factor authentication, network anti-virus, network IPS, network IDS	

Premium		
Target Availability/Month during service hours	**99.99%**	
Service Hours	24/7	
	Response Time Target	**Resolution Time Target**
Service Incident - First Response/Resolution Time Target (CRITICAL)	1 hour	4 hours
Service Incident - First Response/Resolution Time Target (HIGH)	2 hours	8 hours
Service Incident - First Response/Resolution Time Target (MEDIUM)	4 hours	3 days
Service Incident - First Response/Resolution Time Target (LOW)	8 hours	5 days
Service Incident - First Response/Resolution Time Target (INFORMATIONAL)	n/a	n/a
Service Request - First Response/Resolution Time Target (CRITICAL)	4 hours	8 hours
Service Request - First Response /Resolution Time Target (HIGH)	8 hours	2 days
Service Request - First Response/Resolution Time Target (MEDIUM)	8 hours	2 days
Service Request - First Response/Resolution Time Target (LOW)	8 hours	2 days

Service Request - First Response/Resolution Time Target (INFORMATIONAL)	n/a	n/a
Protective Monitoring Service	Optional (Premium recommended)	
Onward Internet Connection	Included up to 100Mbit/s	
DOS and DDOS Protection	**Provided**	
Security features	Mobile VPN, fixed VPN, double-tier firewalls, two- factor authentication, network anti-virus, network IPS, network IDS, Botnet detection, DLP, triple-factor authentication	

A dual site option is available to provide higher levels of availability. Please see the pricing document for details.

Roles and responsibilities

This is a fully managed service that covers the creation of the Fixed VPNs, provision of the Mobile VPN devices and cloud connect security services. Each customer solution has dedicated VPN devices at the e2e datacentre and customers can either use existing VPN devices or e2e provided devices at their managed VPN end points.

Your organisation will be responsible for installing and configuring the mobile VPN clients and supporting your end users. You will need to provide details of which users require access to the service and let us know when your users stop using the service.

We will manage all VPN devices that we provide as part of our service to you and you will be responsible for managing any of your own VPN devices used in the service or delegating management of these devices to e2e.

If your organisation lacks the capability to in/configure or support the end user devices we can assist, either with support days or through our separate e2e Managed Peripherals Service

More information and contact details

Enquiries, and more information is available on request, email info@e2e-assure.com with any queries.

Who Are e2e?

e2e is a cloud security company with 20 years' experience of providing military grade cyber security. We provide repeatable cloud-based services to the public sector. Security depth, quality and service excellence set us apart from our competition.

Our Origins

e2e was founded by two industry experts, each holding 20 years' experience of delivering secure, end-to-end solutions. We have a history of designing secure networks for online payment systems; designing, developing and delivering cyber defence solutions; developing and starting up complete Managed Service solutions; and have built several worldwide Data Centres. Our clients over the years have covered most sectors from banking to the MoD.

Our People

e2e has brought together a highly experienced team of cloud experts, developers, security architects, CESG CLAS consultants, support specialists, security analysts and expert cyber security business development specialists. This core team has since been bolstered by the addition of a vibrant cloud support and cyber analyst team, recruited through channels such as the Cyber Security Challenge UK, SANS Cyber Academy and other government backed schemes to find cyber talent.

Our Work in Government

We have earned an excellent reputation over the last six years as a trusted service provider to government and our cloud services are helping deliver key UK wide services. All our services are ISO27001:2013 accredited, CES and CES+, IASME certified, and we are the go-to organisation when a need for cost effective, cloud based services are required that must be secure to protect UK sovereign reputation. Our services to government cover central government and local government, as well as other public sector organisations.

Our Ambitions

e2e is a service company. We have a well-developed range of cloud-based services, all of which are designed to be repeatable, scalable, flexible and on-demand.

- We aim to be the best supplier: the easiest to deal with, the most reliable, and the best at delivering cloud service support and managed services. So far we have made a huge impression with our existing customers – e2e just does it better than the competition.

- We aim to be the most secure supplier, to deliver and maintain the most secure services. There is simply no other supplier on the market with our security credentials and no other supplier with the technology and team to deliver security-as-a-service at our level. We are miles ahead in this area and this is where we want to stay.

Our Methodology

We focus on applying well established skillsets and a wealth of experience to ensure highly responsive delivery without sacrificing quality. We invest in our technology and our people so that our customers can benefit from our thirst for excellence. We understand how to integrate security seamlessly into our services, giving you secure cloud-based services that 'just work'.

We have fully embraced the 'As a service' model: e2e is a cloud-based business, with a cloud business model, operating model, service delivery model and we deliver all our services from our cloud-based operations centre.

Our Qualifications

e2e is a UK based SME Company operating exclusively from within the UK using SC cleared staff. We operate out of two UK datacentres (Tier3 and Tier4). We are ISO27001:2013 accredited, CES and CES+, IASME certified, CCP Senior level, UKCEB members, TechUK members, BCS and IoD members, Crown Commercial Suppliers, UK Cyber Security Forum members. We sponsor and recruit from the Cyber Security Challenge UK as well as the SANS Cyber Academy. We understand how to work with partners and ensure we are honest and straightforward to deal with. We embrace the cloud first approach and are heavily involved in UK Cyber in general; we want to help spread the UK cyber messages (NCSC Cloud Security Principles, 10 Steps, Get safe on line, etc.) and are active CiSP members with strong links within UK Cyber.