e2e assure

e2e Cloud Protective Monitoring and SOC Service - Service Definition Document

OVERVIEW

e2e-assure provide a complete cloud based cyber defence Protective Monitoring Software as a Service which is delivered remotely from our secure cloud Security Operations Centre (SOC). The service has been designed to address two principal scenarios:

Cloud users wishing to secure their cloud deployments and services

Organisations wishing to procure security as a service to provide subscription based protective monitoring service delivered from the cloud.

The service uses a unique suite of in-house, commercial and open source security monitoring applications and processes. We have a proven track record of delivering this service to a variety of customers running a mixture of private, multi-tenant, public and private cloud environments. The service comes in three service operational variations that align with the organisation's threat posture.

The services are highly flexible and agile and can be scaled up or down as the threat landscape changes. This flexible service model provides outstanding value for money. Our service includes device log monitoring, intrusion detection, risk analysis and threat monitoring, threat intelligence, traffic analysis, and packet capture using a combination of commercial and open source tools up to OFFICIAL SENSITIVE. The service combines and integrates multiple toolsets to gain high levels of situational awareness enabling advanced analysis and efficient incident response and management. We provide a holistic, business service driven, SOC operations model and we focus upon your business priorities and business risks.

Our service supports secure collaboration between customer, supplier, service providers and third parties. The service can be provided in private clouds, in pubic clouds, and in any combination. We also provide protective monitoring of our other secure services such as Cloud Connect. The service can be provided fully managed, as a joint service, or we can provide a SOC solution and let you perform the security operations.

TOP LEVEL FEATURES

- Continuous Cyber Defence Protective Monitoring with alerts and incident response
- Triage, analysis and response integrated into a comprehensive SOC operating model reducing time and improving effectiveness
- Multiple delivery models including Private Cloud, Public Cloud , and Hybrid configurations
- Protective monitoring can be provided for public cloud including Azure, Office365, AWS, UKCloud, Google etc.
- SOC/virtual SOC/CERT functions 24/7 using SC Cleared UK staff working with data in UK Datacentres
- Integrated Threat and Risk modelling with security Analysis and Reporting
- Provides context and situational awareness to allow confident response decisions
- Integrated dynamic asset management and network discovery
- Log and event correlation and analysis, monitors mobile users and devices
- Traffic Analysis, Deep Packet Inspections, IDS, Vulnerability Scanning, Blacklist monitoring
- Privileged User monitoring, Collaboration and continuous service improvement

- Consumes Threat Intelligence from open and commercial sources
- Designed to provide user and customer level customisation
- Services accommodate any OFFICIAL or OFFICIAL-SENSITIVE requirement
- Distributed and Federated architecture, multi domain and multi classification
- Incident Response, dedicated Cyber Case Management and generated Playbooks
- Supports GPG-13 profiles, B (DETER), C (DETECT/RESIST), D (DEFEND)
- Mobile and Remote workforce monitoring - Geo alerting, Location reputation checking, Identification of compromised home networks
- Cyber Investigation and Analysis service

BENEFITS

- ✓ Reduced cost of security monitoring, increased security coverage
- ✓ End-to-end business security confidence and essential security audit assurance
- ✓ Single holistic view of risk and threat across the enterprise including private and public clouds Centralised integrated security knowledge repository with enhanced anomaly detection
- ✓ Speed of delivery - get real value in just 2 weeks
- ✓ Maximise extant IT and investment in security
- ✓ Can be developed 'onto, into and out of' quickly and efficiently supporting the Government Digital Agenda
- ✓ Triage and analysis services identify threats before they become incidents
- ✓ Alerting, expert advice and evidence of potential and verified threats
- ✓ Agile, adaptive cloud-aware service secures your journey to the cloud
- ✓ Creates a common platform hiding the complexity of the underlying tools
- ✓ Dynamically discover assets, learn what is connected to every system
- ✓ Enhanced Mobile and BYOD user risk monitoring
- ✓ Standards compliance for ISO27001:2013, Cyber Essentials Plus, PCI
- ✓ Breaking security technology stove pipes to identify anomalies quicker
- ✓ Flexibility and scalability up and down, short term options for busy periods or heightened threats
- ✓ Scales on protected devices/asset/user and aligns closer to the business need rather than a technical straight-jacket (log sources or eps)
- ✓ Allows you to creates an agile ecosystem of technology, services and suppliers

WHY IS IT NEEDED?

Organisations using the service benefit immediately by being able to detect potential high impact attacks and they can rest easy when potential customers or other parties perform audits or other assessments. Our service is suitable to address any of the following business requirements:

- Compliance and Audit
- Maximising the benefit of security investment
- Managing enterprise risk and threat
- Establishing an end to end security view of corporate and cloud services
- Being able to identify and manage security incidents effectively
- Provide security monitoring on specific parts of the corporate network - e.g. gateways

- Provide flexible and scalable security services, up and down, as needs change
- Support real time asset management especially in the use of mobile and BYOD
- Integrate and reuse of existing tools to improve situational awareness
- Establish an open secure platform that supports collaboration between corporate, supplier and third parties
- Provide security capabilities that facilitates business change, rather than get in the way or delay business change
- Reduce implementation and delivery risks through the use of proven, assured services

THE PROTECTIVE MONITORING SERVICE INTRODUCTION

The service provides a complete security monitoring system, designed and developed by e2e experts who have spent over 15 years designing and building security systems for Government, Agencies, Military, major banks, telco's, and payment providers.

e2e have taken the best of open source and commercial systems and blended them together to provide a formidable arsenal of security services. Every e2e solution is designed by Senior CESG IA Architect and assured by IA Auditors, CLAS consultants and other similarly skilled persons to ensure our service to you is of the highest quality and aligned to the latest government security objectives and industry best practice.

Some of the components of this system have been provided below:

- Log collection, storage and monitoring (any type of IP device that can send logs)
- 'Google-fast' searching, querying and indexing with typical VM systems capable of processing 10s of thousands of logs per second per device
- Network and Host based IDS (we provides as part of the service and we can integrate with extant customer security tools)
- Traffic monitoring and intelligent traffic analysis (i.e. detects and classifies traffic based on its type not it's port number – e.g. detects data tunnelling and applications using nonstandard ports, exfiltration and other data leakages)
- Packet capture and analysis to enable investigations into alerts and to support incident response
- DNS monitoring to detect DNS lookups to known or suspected malware or other suspicious domain names
- Botnet monitoring – hunts for and alerts on any type of connection known to be used by botnets
- Web and email threat monitoring – monitors access to the Internet and emails and hunts for known threats and signs of potential threats in web site browsing, URLs and emails
- Threat indicator monitoring and latest threat intelligence monitoring
- Geographic analysis of all attacks and traffic
- Cloud-focused service design that provides monitoring of the latest cloud based threats and intelligence
- Fully managed cloud service that can be provided with varying levels of customer involvement as appropriate
- In depth reporting on all aspects of the service

- Service can be delivered from e2e's virtual Security Operations Centre (vSOC), a highly resilient cloud based system that provides secure connectivity, collaboration, threat sharing and secure operations
- Service can be delivered to any type of cloud, or combinations of clouds (private, public, community, hybrid, etc.)
- Monitoring data and security events can stay complete within the customer cloud or on premise or reside in the e2e vSOC depending on customer requirements
- Options for the whole security monitoring and incident response to be provided by the service (for customers who have no security teams or in house expertise)
- All e2e staff have SC level clearance or above

E2E PROTECTIVE MONITORING SERVICES INCIDENT MANAGEMENT

Our service management processes are ITIL V3 aligned and have particular focus upon Security Incident Management and Continuous Service Improvement. The following is our approach to the Incident Management lifecycle:

Prior to a security incident our SOC analysts focus upon:

Prediction: The gaining and application of threat intelligence to attempt to anticipate future attempts at compromise

Prevention: The understanding of and application of insight gained from the intelligence, operational performance, previous incident responses etc. to counter future known or suspected threats

During a cyber-attack our analysts focus upon:

Detection: The interpretation of any events of interest occurring to discriminate between legitimate and abnormal events to identify anomalous activity

Investigation: The analysis of anomalies to determine whether they are emerging threats that may lead to a security incident. Our analysts use the combined data from the deployed toolsets to create high levels of situational awareness. The gaining of situational awareness through bringing business, intelligence, infrastructure, and trend information together is key at this phase so that correct analysis can take place

Following a cyber-attack the focus will be on:

Reaction: The activities needed to record and triage a security incident. Our analysts use tailored, predefined and configured Playbooks to efficiently inform their reaction to an identified threat

Response: The planning of effective mitigations in response to the cyber-attack, the communication of these plans to all relevant stakeholders, and the collaboration with all relevant third parties to carry out mitigations. Forensic Analysis and investigation are carried out along with collaboration with relevant agencies.

Defence: The execution and monitoring of the response or remediation to contain and defend against the attack and neutralising the threat, and recovering affected business systems

Service Improvement: The review of mitigation plans, the development of longer security improvement plans, review of incident management performance, analysis of indicators to create insight and intelligence to help pre-empt future attacks, and the creation of technical measures to assist in improving efficiency of detection and response. Day to day activities include tuning, practicing and improving incident response plans and playbooks.

THE INTEGRATION OF TOOLSETS WITHIN THE SERVICE

Based upon the benefits the modular open source architecture within our protective monitoring service, we have integrated a number of different class leading toolsets into our SOC service and our in house developed system is based on standard APIs which also integrates with the majority of security tools in the market place. This approach de-risks and speeds the delivery of our service to you and shortens the time it takes us to add new capabilities to the service in response to a changing threat landscape.

Our SOC analysts perform anomaly detection across all the toolsets, breaking the stove pipe approach of traditional security technologies. This allows situational awareness to be gained more quickly and better informs incident prioritisation and response planning. Our service further supports advanced anomaly detection by enabling longer term cross trending of all information held within our centralised data store and repository regardless of data source.

THREAT INTELLIGENCE IN THE SERVICE

Threat Intelligence is used at various points within our service to identify anomalous behaviour and to correctly categorise the identified threats. For-example, anomalous patterns of internet traffic will be picked up, unusual activity behaviours will be identified and appropriate alerts will be raised. Our service also uses a wide range of Intelligence sources to enhance anomaly detection during the Triage process. Our analysts use reputational database checks for IP, Domain, URL, and mail addresses etc. to assist the initial triage process; identifying emerging threats and placing them in your organisation's business context.

ABUSE AND REPUTATION MONITORING

This is an additional optional G-Cloud service that uses commercial and open source IP reputation and abuse detection services that support mass querying of large sets of IP addresses at frequent intervals. This service will be used to monitor these sources to see if any of the known Public IP addresses of the customer (any public IP address used anywhere) to see if it has been recently found to be sending spam email, infected with a virus, Trojan or participating in a botnet or is known to host malicious content or has been used to launch attacks of some sort. In a similar way to external vulnerability scanning, it is a good early warning and safety net function that can be used to look for known problems across the customer estate.

PLACING THREATS WITHIN THE BUSINESS CONTEXT

Key to the successful management of incidents is an understanding of what the actual threat may be; who could it be, what could be their motivation, what business systems may be impacted, and what impact would it have on the Confidentiality, Integrity and Availability of business services. Our Protective Monitoring Service supports the creation of business models that incorporate threat and risk information. Our service supports the definition of threat actors, threat types, severity levels, and associated risk types and risk impact levels.

Customer Business Systems are defined within the Protective Monitoring Service and are logical groups of assets that perform a key function. Systems may have child and parent systems. Systems are typically defined in our service as IP address ranges with associated additional attributes. This design makes it possible to design and deliver large scale, distributed Protective Monitoring Service systems where there are clear boundaries between tenants (Customers or Key Systems or Service Providers). It helps us place anomalies in your business context and allows better prioritisation of responses.

TOOLSETS THAT MAY BE DEPLOYED

To facilitate the protective monitoring service we may require the installation of software agents or a deployment of our multi-function sensors within your environment.

SOFTWARE AGENTS FOR LOG COLLECTION

Where necessary we provide software agents for Log Collection to you or your nominated service provider. Agents can generate and send log files from servers. By default these are sent via TCP syslog but it is possible to use TLS encryption to encrypt the syslog data or send data via a variety of formats. Dual sending is also possible, where one agent can send logs to two destinations. It is possible to read, parse and send most types of event log and the contents of files and it the architecture supports creating custom parsers and collectors to collect from non-standard sources of data. Our service has agents available for both *NIX and Windows. These agents are designed to be as lightweight as possible and can be deployed in a variety of ways (flexibility is key when installing agents on servers).

The provision of server agent software is included within the Baseline Protective Monitoring service, but it is assumed that the agents will be installed by third parties. If there is a significant number of agents to be configured, this planned activity should be treated as a project under change control.

NETWORK DISCOVERY

e2e will provide a Network Discovery capability as a part of the Baseline service. Additional appliances can be provided centrally or distributed (i.e. with many local network discovery devices). All appliances come with a variety of open source tools and e2e developed scripts which are used to run automated collections from network equipment via SSH or Telnet. They support usernames and

passwords as well as keys for authenticating to network component. These can be used to gather an understanding of the assets and networks which allows our Protective Monitoring Service to create a dynamically generated network and asset map. This helps organisations understand their assets and helps the analysts carry out analysis and Triage more effectively.

Passive Discovery, Network and Traffic Analysis

Passive discovery is delivered through the use of other open source tools and through the Multi-Function Probe appliances. Passive discovery relies on packet data being received by capture interfaces on the Protective Monitoring Service Multi-Function Probe appliances. Network taps or SPAN/mirror sessions (provided by the customer) are used to present traffic to these devices. In data centre environments we provide appliances with many network interfaces which are bonded together on the hardware chassis. On high traffic environments there may be one device per interface but Protective Monitoring Service can utilise as many as are available. The Protective Monitoring Service also makes extensive use of open source tools which provides extremely powerful network traffic inspection as well as supporting scripting which can be used to write custom detections for all types of network traffic.

The tools are very effective at passively detecting and analysing network traffic to identify aspect useful to the security analyst such as DNS, HTTP, HTTPS and FILES. They allow extraction of key information such as domain name queries, http URI's, user agents, browser versions, SSL versions, IPSec Ciphers/encryption methods and produces MD5 and SHA1 checksums of all files transferred - vital for identifying data loss and malware files.

Multi-Function Appliance

In capture environments it will be appropriate to use our Multi-Function Probe to provide a dedicated traffic capture appliance. Provision of a single appliance may be used to monitor a key network ingress/egress point in your infrastructure. Detailed design activity will determine the most effective initial implementation. Additional appliances can be provided as an option as required.

The appliance is provided with eight 1Gigabit interfaces, 16 CPU cores and 98GB RAM and 8x900 GB drives for on board storage. Multiple NICs can be used for packet capture; either individually or cumulatively in bonded groups. Using VMWare to provide the virtual switching fabric allows these devices to run all the Protective Monitoring Service tools as virtual machines, each receiving the same copy of the traffic. These appliances will run all the packet capture related tools; packet capture, traffic analysis and inspection, IDS/IPS as dedicated Virtual Machines. MFA's are also available with four 10Gbps interfaces and high speed disk storage.

These appliances scale predictably based on overall traffic load. This allows one appliance with lots of interfaces to cover many networks at once or allows us to monitor just one large network.

Deep Packet Capture

The full packet capture solution will store as much as the underlying storage will allow and continue to use the full amount of storage overwriting the oldest data so that packet capture is continuous. If required, additional storage would be provided as an option.

Intrusion Detection System (IDS)

Network IDS is based on Snort. Snort is open source and supports a variety of signature sources from open and commercial sources as well as custom signatures unique to Government and industry. The service uses standard snort engines and because of this can use all or few of Snort's features and can run many snort processes per appliance if required. Snort runs on the same devices as packet capture. Snort sends alerts through to Protective Monitoring Service via an API. Commercial Network IPS/IDS solutions can also be integrated into the service.

Our Protective Monitoring Service can also integrate with commercial tools such as Niksun and Endace for packet capture, Arbor for flow monitoring and many other best of breed solutions in order to leverage existing customer investments.

Our service also includes an option of a software agent for Host based IDS which will be made available to you, or your nominated service provider, for installation within your ICT estate.

Internal Vulnerability Management Scanning

Vulnerability Assessment and Vulnerability Management are part of the Protective Monitoring Service solution for the purpose of internal scanning and assessment. e2e provides a single Vulnerability Scanner appliance as a part of the Enhanced Protective Monitoring service. Options are provided for the provision of additional Vulnerability Scanner Appliances and the provision of a standalone internal Vulnerability Management Service. The dedicated scanning appliance includes leading commercial vulnerability scanning tool (Nessus) and a number of other open source tools for this purpose. Nessus is a leading full featured vulnerability scanner. Using Nessus on scan devices allows for full Nessus scan reports to be generated and sent to owners of scanned systems, etc. In addition to Nessus, e2e have integrated other vulnerability scanners such as Tripwire IP360 and McAfee. If there any other proprietary vulnerability scanners within the Customer estate, e2e can implement a simple integration under change control.

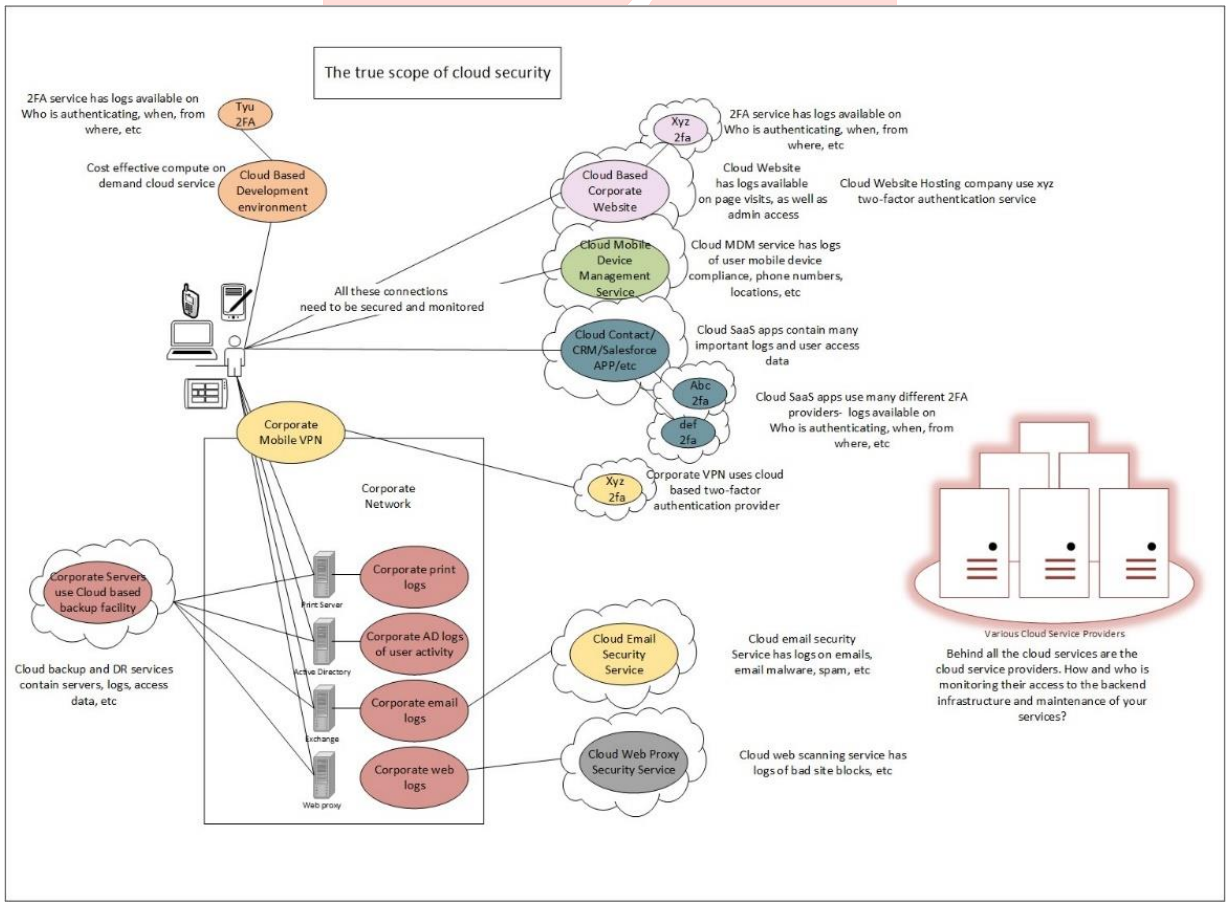
e2e External Vulnerability Scanning Service

The e2e Vulnerability Scanning, Assessment, Alerting and Monitoring Service is offered as a separate service through G-Cloud. It is designed to scan an organisations public IP addresses over the Internet. It provides the same capability as the internal scanning system but runs out of e2e's datacentres (both in the UK). It is aimed at profiling and monitoring the external exposure of organisations – there is a lot to be gained by simple scanning external IP ranges checking for obvious flaws, misconfigurations

and vulnerabilities. Over the last year we have successfully identified, notified and helped mitigate some major vulnerabilities for our clients which would otherwise have gone unnoticed, resulting in considerable reputational impact or potential data breach.

WHY IS PROTECTIVE MONITORING IN THE CLOUD DIFFERENT?

Traditional protective monitoring relies on capturing the logs and events from all devices in the network/system (or at least the key devices). These are typically servers, workstations, network devices, etc. Often these devices are on the internal network and it is relatively straightforward to map internal users to these devices through correlating audit logs, etc. Users typically connect via local networks or corporate mobile VPNs. In the cloud model users may be connecting from anywhere, using a variety of devices and a variety of authentication services that are outside of the corporate network. This creates a situation whereby a lot of the protective monitoring data is external to the corporate network. A modern organisation that is benefiting from cloud service will have users accessing a variety of cloud services and the internal corporate network itself will also be consuming cloud services, such as Backup as a Service, Cloud Disaster Recovery, Email and Web filtering services and so on. The picture below shows just some examples of how this looks and how monitoring the corporate network is only part of the story…..e2e's cloud protective monitoring combines these two elements - the internal corporate logs and the external cloud system logs to ensure effective Protective Monitoring of cloud model computing.



WHY YOU SHOULDN'T RELY ON YOUR CLOUD SERVICE PROVIDERS

Each cloud service will have a different amount of extant security monitoring but it is all based on monitoring the cloud service itself – not at performing any monitoring for you, your users or user data. Cloud service providers are also focused on driving down costs so relying on them to detect security problems is not a realistic perspective – as recent failures such as Apple iCloud have taught us.

The Cloud Model widens the Threat Surface

Users and indeed computers connect to cloud services in a variety of ways and this presents would be attackers with a much wider attack surface to use against you and many different communications paths where data in transit could be captured. A breach in any one of your cloud services could lead to a breach of many of them – if your users' device is compromised it could be used to compromise all its connected cloud services.

PUBLIC CLOUD PROTECTIVE MONITORING

Public clouds offer convenient and cost effective cloud IaaS, PaaS and SaaS services. One of the least understood aspects is how to use these services securely, and how key security and standards compliance requirements can be met when using public clouds. e2e have developed a range of solutions to address these problems:

- Cloud connect provides a secure way to use public cloud services.
- e2e protective monitoring services are designed to provide the monitoring, compliance assurance and incident response services to public clouds.
- e2e Vulnerability Scanning, Assessment Monitoring and alerting service

The challenge is how to deliver these services to public clouds. From a technical perspective there are a few key differentiators; the starting point is that the service provider is responsible for the IaaS and because of this there is very little more to do. Customers must review the security assertions and certifications, the cloud location and providers jurisdiction to ensure they all align and meet their requirements. With an IaaS service, the customer will typically be responsible for the virtual machines. This makes it possible to install security monitoring agents and collect logs although here are still some key gaps as log collection is only a small part of what is required. In order to fill in some of the gaps, e2e have developed software agents, virtual machine appliances and integrations with Cloud API's to specifically address the lack of visibility and monitoring in public clouds. The software agents use standard operating system features and supported tools to ensure they are compatible with the target machine and low overhead and highly reliable. They gather snippets of information continuously that are fed to a central repository using a secure API. This API can work in either direction to meet customer requirements. These agents can also perform discovery and asset management functions.

Virtual appliances perform asset management, rogue VM detection and also internal vulnerability and compliance by scanning and providing crucial visibility into the accessible VMs. We have developed API integrations with most public clouds, at all levels of the cloud service (IaaS, PaaS and SaaS services). These integrations provide access to cloud provisioning, diagnostic, security, usage and reporting data that when combined with the software agents and appliances provide cloud visibility.

We support the provision, support and maintenance of Cloud based virtual firewalls (those included with the cloud service and cloud independent suppliers such as Cisco and Juniper. Using these devices provides us with an advanced level of infrastructure visibility. We have also developed a transparent cloud bridge device to provide a drop in monitoring solution and it can also function as a firewall but its main function is to duplicate and replicate all ingress and egress traffic to and from the cloud. The traffic is then picked up by our multi-function appliance enabling us to perform packet capture and related functions such as traffic analysis, DNS analysis, Intrusion Detection (IDS) etc.

MOBILE WORKFORCE MONITORING

With the expansion of mobile and remote working, and the consequent fluidity of working environments, our service offers some unique 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.

E2E PROTECTIVE MONITORING SERVICE LEVELS

The following is a summary of the four service levels available:

SERVICE FEATURE AND SERVICE LEVELS

The Service collects events, logs and other information continuously and generates security alerts on a 24/7 basis. The Service Hours below refers to responses to service requests and the invocation of triage and incident response by the e2e SOC. Customers may choose to create alerts that will notify them via email, SMS or via the portal which can escalate critical or high priority alerts within 15 minutes of detection. Alerts and Incidents to the customer will be made via phone or email in accordance with agreed incident response playbooks.

BASELINE LOG MONITORING AND COMPLIANCE SERVICE LEVELS

- Log Reporting, Log Collection, Logging and Storage
- Log collection up to 5,000 eps
- Log and Threat Alerting
- Email alerts to customer
- Monthly summary report and compliance reports
- Retention periods of 6 months
- Any log source capable of generating standard collectable logs. Includes Server Agents
- Alerts analysed and triaged by e2e vSOC
- Customer is responsible for investigating events, threats, or purchasing e2e incident response days to be used for this purpose

Baseline Log Monitoring and Compliance Service	Target
Target Availability/Month (during service hours)	**99.50%**
Service Hours (for Service Requests)	**8am to 6pm Mon-Fri**
Systems and Service Hours Response Time	**4 hours**
Emergency/out of hours 24/7 Response Time	**8 hours**
Security Alerting 24/7 from Playbooks (used to create alerts that can be sent to notification groups)	**15 minutes**
Security Alerting during Service Hour after initial analysis and triage Response Time (High Priority Incidents)	**4 hours**
Emergency/out of hours 24/7 response time	**8 hours**
Change Windows	**Service hours**
Backup Archive	**30 Days**
Equipment/System Patching Routine	**Up to twice Monthly outside Service Hours**

Critical Patches including Security Patches	**8 working hours**

BASELINE PROTECTIVE MONITORING SERVICE LEVELS

- Log Reporting, Log Collection, Logging and Storage
- Log collection up to 5,000 eps
- Log and Threat Alerting
- Email alerts to customer
- Monthly summary report and compliance reports
- Retention periods of 6 months
- Any log source capable of generating standard collectable logs. Includes Server Agents
- One Multi-Function Sensor, includes one virtual network IDS, one instance of packet capture (limited storage), DNS monitoring, botnet, web and email monitoring , Traffic analysis and monitoring, up to a max throughput of 500Mbps
- Alerts analysed and triaged by e2e SOC
- Customer is responsible for investigating events, threats, or purchasing e2e incident response days to be used for this purpose

Baseline Protective Monitoring Service	Target
Target Availability/Month (during service hours)	**99.50%**
Service Hours for Service Requests	**8am to 6pm Mon-Fri**
Systems and Service Hours Response Time	**4 hours**
Emergency/out of hours 24/7 Response Time	**8 hours**
Security Alerting 24/7 from Playbooks (used to create alerts that can be sent to notification groups)	**15 minutes**
Security Alerting during Service Hours after initial analysis and triage Response Time (High Priority Incidents)	**4 hours**
Change Windows	**Service hours**
Backup Archive	**30 Days**
Equipment/System Patching Routine	**Up to twice Monthly outside Service Hours**
Critical Patches including Security Patches	**8 working hours**

ENHANCED PROTECTIVE MONITORING SERVICE LEVELS

- Alerts analysed and triaged by e2e SOC and escalated to customer when appropriate with remediation recommendations
- Log Reporting, Log Collection, Logging and Storage - retention periods of 6 months
- Any log source capable of generating standard collectable logs. Includes Server Agents
- Multi-Function Sensors (1Gbps), Network IDS, packet capture/inspection, DNS monitoring, botnet, web and email monitoring , traffic flow analysis, Network Discovery (up to a maximum of one sensor per band of 500 devices. Additional implementation charges in accordance with the Rate Card may, at the Suppliers discretion, apply for separate physical locations)
- Includes one Internal Vulnerability Scanner
- Includes Host based IDS agents (if required)
- Asset Management and Threat Model. Threat indicator detection (detects typical signs of threats by their indicators), Customer Business Services Prioritised
- Threat Intelligence
- Customer responsible for investigating incidents with assistance from e2e. Additional incident response support services may be required
- Weekly and Monthly summary report and monthly review meeting
- Portal access for reports and dashboards - monthly event, threat and alerts summary

Enhanced Protective Monitoring Service	Target
Target Availability/Month during service hours	**99.90%**
Service Hours (for Service Requests)	**8am to 6pm Mon-Fri**
Systems and Service Request Hours response time	**2 hours**
Emergency/out of hours 24/7 response time	**8 hours**
Security Alerting 24/7 from Playbooks (used to create alerts that can be sent to notification groups)	**15 minutes**
Security Alerting 24/7 after initial analysis and triage Response Time during service hours (High Priority Incidents)	**2 hours**
Manual Security Blocking via pre-agreed change	**4 Hours**
Change Windows	**Out of hours**
Backup Archive	**30 Days**
Equipment/System Patching Routine	**Up to twice Monthly outside Service Hours**
Critical Patches including Security Patches	**8 working hours**

PREMIUM PROTECTIVE MONITORING SERVICE LEVELS

- As per Enhanced Service Level plus;
- Full incident response and management that includes analysis and coordination of all response and remediation actions as required
- e2e full incident response engagement (first 5 days) for any incident e2e escalate to customer as a Priority 1 (High Priority). All other incidents treated as per Enhanced.
- Active and Automated Cyber Defence remediation (where agreed)
- Forensic investigation and Malware Analysis services providing collection of evidence and advice and options to mitigate, contain or manage threat.
- Retention period of 12 Months
- Remote portal and dashboard providing access to security applications and case management toolsets to support joint investigations if required
- Full event and incident reporting, security processes management including Incident Response Planning, monthly and quarterly review meeting (on site or as agreed) and continuous service improvement
- Includes external Vulnerability Scanning and Alerting Services at the Baseline Level up to 16 IP addresses or URLs
- Includes one internal virtual vulnerability scanner per band of 500 devices
- Includes Office365 Protective Monitoring (if applicable)

Premium Protective Monitoring Service	Target
Target Availability/Month	**99.99%**
Service Hours (Alerting and Response)	**24/7**
Service Hours for Service Requests	**8am to 8pm Mon-Fri**
Service Requests response time	**1 hour**
Emergency/out of hours 24/7 Service Request response time	**4 hours**
Security Alerting 24/7 from Playbooks (used to create alerts that can be sent to notification groups)	**15 minutes**
Security Alerting 24/7 after initial analysis and triage Response Time (High Priority Incidents)	**1 hour**
Automated Security Blocking via Playbook	**15 minutes**
Manual Security Blocking via pre agreed change	**2 Hours**
Change Windows	**24/7**
Backup Archive	**30 Days**
Equipment/System Patching Routine	**Up to twice Monthly outside Service Hours**
Critical Patches including Security Patches	**8 working hours**

Additional Security Operations and Protective Monitoring Optional Services

The standard service types above have been designed to address typical deployments and requirements for most customer needs. However some organisations may have more complex distributed environments and different security requirements and therefore we have a range of additional options to support this and provide fixed service prices for more complex service environments. The following table summarise the additional options for the Protective Monitoring Service

Additional Security Operations and Protective Monitoring Optional Services	
Service Option	**Description**
Additional Storage/Data Retention	Enable additional storage for increased data retention or log storage. This is priced Per 500GB per month
Secure VPN Access	Installation of an e2e provided additional fixed VPN service to an existing Cloud
SIEM Virtual Appliance	Provides a proprietary receiver/collector, Log Management, SIEM/Correlation up to 5000 eps (Please note, this is not required for any standard implementations)
Network Discovery Software Appliance	For additional distributed discovery or locations.
Vulnerability Scanning Software Appliance	Typically required for each additional 500 IP addresses. For additional distributed scanning locations.
Multifunction Sensor Bundle Appliance (1Gbps and 10Gbps)	includes Traffic Analysis and Monitoring, Event and Log Management, Packet Capture, IDS
IDS Sensor Appliance	Provision of an Intrusion Detection sensor
Custom Connector	Professional Services
Customer specific Rules or Tuning	Professional Services
Customised Monthly or Weekly Report	Professional Services
Internal Vulnerability Management Service	Provides a central manager for vulnerability management and reporting
Security Operations Collaboration and CERT Module	Provides additional capability for fully featured SOC and CERT capability including Portal, Document management, email, PGP and collaboration services, Knowledge Management (assumes availability of underlying cloud compute and storage services) Only available in addition to the Premium Service

Protective Monitoring Customisation Module	Provides customisation development and support services
Remote Security Operation Office and Secure Printing	See separate e2e Remote Cloud Office and Secure Printing Service
Additional SOC/CERT End User Access Devices	See separate e2e Managed EUD service for provision of fully managed Secure Desktops/Laptops/Tablets/Mobiles
Security Operation Development and Test Environment (PaaS)	See separate e2e Managed Development and Test Service
Protective Monitoring Heightened Cover	Scale up service for a Day, Weekend, or extended periods. Provides1 hour alerting and response.
Standalone Security Incident Case Management and Analyst Playbook Service	Per User (minimum 5 users) Requires a CC Fixed VPN or Mobile VPN
Abuse and Reputational Monitoring	IP Address Abuse and Reputation lookup and alerting service Per 100 IP addresses
Office365 and Cloud SaaS monitoring	See Description below
Security Investigation and Analysis Service	See Description below
Additional Incident Security Services	See Pricing Document

THE PROTECTIVE MONITORING SERVICES AND GPG13

All our services incorporate relevant GPG13 recommendations at varying levels depending on the service. e2e separate security from compliance and for cloud based systems the emphasis is on security event detection as this delivers the most effective security.

The reason for this is that customers using clouds are doing business on the Internet and are have end users on the Internet. Prior to cloud adoption the rule was that 90% of the threats you face were internal. In the cloud 90% of the threats you face are external*.

*see the Verizon 2014 Data Breach Intelligence Report (*DBIR): http://www.verizonenterprise.com/DBIR/2014/

That's what we mean by 'cloud focused'. If you are using cloud services you need to choose a protective monitoring service that aligns with the threats you are facing.

It is possible to provide GPG13 alignment with any of the level of e2e protective monitoring service as GPG13 requires you to take a risk based approach to monitoring; and that's exactly what our service

does, and is the reason why three level of service exist – they are aligned to the outcomes of your risk management process.

Furthermore, GPG13 describes protective monitoring as a set of business processes with supporting technology. It is not possible for any security managed service to claim to provide 'GPG13 Compliance' as GPG13 is a set of guidelines and recommended best practice, not a standard. It does not mandate any particular technology or control.

e2e's protective monitoring services were created using GPG13 as a guideline and take on board many of the recommended best practice processes and technologies and merges them with the latest industry based practice, CESG Cloud Security Principles and wider CESG and government best practice and advice.

All our services are designed by a Senior CESG IA Architect and are independently reviewed and assessed on a continual basis to ensure our service aligns with the latest guidelines and the latest threats.

Cyber Investigation and Analysis Services

Summary

Provision of Cyber Investigation and Analysis Service for organisations that suspect that they have been subject to a security incident, cyber-attack or are concerned that they might be vulnerable to an external or internal attack. Detailed analysis and investigations will be carried out by GIAC qualified analysts. The service will be carried out at an agreed location for up to 2 weeks and the completion of a final report detailing conclusions and recommendations.

Description:

e2e will install a cyber analytics sensor at agreed locations with remote access from our SOC. We will also perform a thorough scan and assessment of the organisations external internet presence for vulnerabilities and threats. Forensic investigation and malware analysis provides collection of evidence and advice and options to mitigate, contain or manage threat.

Detailed analysis and investigations will be carried out by GIAC qualified analysts. Feedback will be provided on an ongoing basis and preliminary results may be available within 3 days. If agreed, daily and weekly reviews will be scheduled to review progress and activities. We will recommend any specific remediation actions or activities in consultation with you and the perceived threats and risks.

We will provide a final report at the end of investigation summarising the investigation activity performed and any conclusions or recommendations for future activity.

Investigation activity may lead to full security incident response which will remain the responsibility of the customer and e2e will provide additional support as required.

OFFICE365 MONITORING

Office365 and Cloud SaaS Protective Monitoring is included with the Premium service level and available as a standalone or optional service for Baseline and Enhanced Protective Monitoring Services. The key features include:

Usage Analytics	Identifies all users and groups accessing Office 365 and reveals which users are accessing sensitive data.
Cloud Activity Monitoring	Provides a comprehensive audit trail of all user and admin activities to support post-incident investigations and forensics.
Portal and Incident Response	Provides Cloud based Portal access and delivers a threat protection dashboard with incident-response work flow for potential insider/privileged user threats, compromised accounts
Untrusted and Geo-Location Analysis and Alerting	Visualizes global access patterns and analyses activity to identify impossible cross-region access attempts indicative of compromised accounts.
User Behaviour Analytics	Identifies anomalies indicative of insider threat data exfiltration.
Privileged User Analytics	Identifies excessive user permissions, dead administrator accounts, inappropriate access to data, escalation of privileges and user provisioning.

The service provides the collection, monitoring and alerting of Office365 Protective monitoring information. Protective Monitoring of other Cloud SaaS service will be dependent upon the data and information available from the cloud service provider. Included with the service is monthly service reports of all services, alerts and incidents, PCI compliance reports and resilient off site backup of all audit data. The service pricing is based upon number of Office365 subscriptions the selected Service Level and volume discounts are available.

HOW DO I KNOW WHICH SERVICE IS APPROPRIATE?

There is a level of service appropriate for all organisations. If you do not currently know what the right level of service is we offer a simple process:

1. e2e provide a free, one day on site workshop provided by a CESG Senior IA Architect where we work with your organisation to establish risk profiles, determine levels of threat and exposure and determine the recommended service. This initial workshop can also be used to identify the scope of the service and provides some simple advice in the form of recommended next steps.

2. The initial visit provides a report and includes a heat map similar to the below that rates your risk level based on your exposure and your perceived level of threat and the value of your organisation (in terms of the value/cost of a loss due to a hack):

Heat Map/Risk Matrix			
	Level of Threat	Level of Exposure	Organisation Value
Very Low	1	1	1
Low	2	2	2
Medium	3	3	3
High	4	4	4
Very High	5	5	5

3. The workshop report includes expert advice from e2e and includes generating your heat map similar to above and this gives us a score:

Heat Map Scoring Chart												
0-3	4	5	6	7	8	9	10	11	12	13	14	15
Very Low	Low			Medium			High			Very High		

4. This score then maps to our recommended services:

Recommended Protective Monitoring Strategy				
Score	Basic	Enhanced	Premium	Custom
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

5. If you need more the free one day workshop is offered with no commitment from you. We will walk you through a risk based approach that starts with your business requirements and allows you to decide which service aligns best.

MORE INFORMATION AND CONTACT DETAILS

For more details on this service and to see the other services we offer visit

www.e2e-assure.com

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

WHO ARE E2E?

e2e are 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 have 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 three 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, local government as well as other public sector organisations.

Our Ambitions

e2e are 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, CLAS members, CESG 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 (CESG Cloud Security Principles, 10 steps, Get safe on line, etc.) and are active CiSP members with strong links within UK Cyber.