SYMANTEC TECHNICAL SERVICES, CAPABILITIES & COMPETENCIES

"Securing and protecting businesses since 1997"

CYBER ESSENTIALS PLUS

Celebrating 20 YEARS
DEDICATED TO THE SECURITY OF INFORMATION

ABOUT CST

Computer Security Technology (CST) is a specialist supplier of services and solutions, to secure information and system technology. Its dedication to information security since 1997, has made CST one of the longest established IT security specialists within the UK.

CST provide security solutions, software development, consultancy services, penetration testing, and managed security services, typically for IT departments who are either challenged with resource or expertise. CST are recognised and highly regarded by leading industry vendors, as well as representing niche security solution suppliers.

SYMANTEC SKILLS

CST have partnered with Symantec for over 17 years. In 2011 Symantec divested itself of its Consultancy Dept. and at the same time created a scheme for Partners to deliver on their behalf. CST reached MASTER status and (amongst many other awards) remained the only UK partner to have achieved this. The Master award required peer reviews, technical qualifications, customer satisfaction surveys and the use of best practice techniques. The Master program has moved on, however CST's approach and delivery quality remains the same. We continue to be one of the few Partners in the UK that are subcontracted by Symantec for customer consultancy delivery across the following:

Symantec Endpoint Protection (SEP) – multi endpoint security with AV, USB control, desktop firewall, host NAC, intrusion prevention, with advanced machine learning defence capabilities

Managed Security Services (MSS) – augmenting Symantec's monitoring services, with Care Plans, bespoke configuration, report & alert management, incident analysis and localised onsite support

Symantec Advanced Threat Protection (ATP): Network/Email/Endpoint – protection, detection, investigation and mitigation against Advanced Persistent Threats (APTs)

Symantec Messaging Gateway (SMG) / Symantec Mail Security for MS Exchange (SMSMSE) – email traffic content and malware protection

Symantec Encryption (formerly PGP) / Symantec Endpoint Encryption (formerly GuardianEdge) – encryption of attached media, hard-drive, network files, email, and third party file transfer protocols

Symantec Control Compliance Suite (CCS) – assessing and measuring policies or best practice standards, for technical controls and procedural actions

Symantec Protection Engine (SPE) – malware scanning of files during file transfer protocols, and within proprietary storage mediums

Symantec Data Centre Security: Server (DCS:S) – agentless malware protection for VMware platforms

Symantec Data Centre Security: Server Advanced (DCS:SA) / Symantec Embedded Security: Critical System Protection (SES:CSP) – non-signature based host protection, incorporating: FIM, OS and app hardening, least privilege access, and service sand boxing

Symantec.Cloud – On-boarding, policy configuration and Enhanced support for Endpoint, Email and Web security from the cloud, formerly known as Messagelabs

PROJECT EXAMPLES: **COMPLIANCE**

PROJECT: MAJOR UK HIGH STREET BANK

A long established and well regarded UK Bank with over 70,000 staff, across 2,000 branches.

Solution: Symantec Control Compliance Suite (CCS)

Scope: Requirement analysis and associated design of CCS Standards Manager into the bank's various datacentres, in order to centralise the reporting and measurement of technical controls, as well as system compliance policies.

PROJECT: MAJOR EASTERN INVESTMENT BANK

European HQ (London location) for a large global Bank established in the Far East.

Solution: Symantec Control Compliance Suite (CCS) – Standards Module

Scope: The upgrade of existing compliance tools to CCS Standards Manager, including bespoke policy check creation, agentless collection, key system risk scoring, and CISO team handover/knowledge transfer.

PROJECT EXAMPLES: **COMPLIANCE**

PROJECT: INVESTMENT BANK

The UK office for a Middle East based private wealth investment office.

Solution: Symantec Control Compliance Suite (CCS) – Standards Module

Scope: The design, implementation, and on-going management of the policy auditing as well as assessment requirements, for key high risk servers and network assets.

PROJECT: GLOBAL SERVICES PROVIDER

This Services company provides central Government and defence agencies with various specialised outsourced functions, incorporating 7,000 staff in the UK, and 40,000 staff globally.

Solution: Symantec Control Compliance Suite (CCS) – Vulnerability Manager (VM)

Scope: The design and implementation of CCS-VM to automatically detect exploitable conditions with key network assets, as well as prioritisation remediation plans based on elevated risk order ranking.

PROJECT EXAMPLES: ENCRYPTION

PROJECT: INTERNET BASED RETAILER

Retail business that pioneered the use of the web to replace traditional high street sales. A high tech internet savvy organisation that required staff to be productive and secure whilst in the field.

Solution: Symantec PGP Encryption

Scope: The design and implementation of PGP whole disk encryption for over 1,000 mobile devices, with a requirement to secure the 'data at rest' for key assets that reside outside the physical perimeter of the business.

PROJECT: HIGH STREET & ONLINE GAMBLING

One of the UK's major high street and online gambling companies.

Solution: Symantec PGP File Share Encryption

Scope: The project was driven by various industry mandates such as PCI, Anti money laundering, Responsible Gambling, and internal audit compliance actions. The remit was to design and install PGP Netshare to protect sensitive information from inappropriate access and data loss. Privilege enforcement for internal users, staff, as well as external parties was also required. The result was an effective compartmentalisation of information enforcing a "need to know" strategy.

PROJECT: LEGAL PRACTICE

This legal practice specialised in highly sensitive topics.

Solution: PGP Email Gateway Encryption

Scope: Design and install the gateway solution to encrypt email going to key customers automatically. The result was a policy driven encryption solution that did not require user action, and met the information security demands of their customers across ten separate email domains.

PROJECT EXAMPLES:
ENDPOINT PROTECTION

PROJECT: INSURANCE BROKERS GLOBAL UNDERWRITERS

This large Insurance Broker has over 40 UK offices and employees 2,000 staff.

Solution: Symantec Endpoint Protection (SEP)

Scope: The design and implementation of SEP across multiple endpoints and servers, with diverse operating systems over 40 office locations within the UK.

PROJECT: JAPANESE CONGLOMERATE – UK'S FINANCE & LOANS DIVISION

This section of the business provides loans and securities to UK business as well as' consumers.

Solution: Symantec Protection Engine (SPE)

Scope: The organisation commenced loan provision via the web, incorporating the upload of loan applications and supporting agreements from intermediary brokers or directly from customers. SPE was designed and implemented to intercept any file uploads that may borne malware prior to the files touching (stored or copied) the corporate LAN or web apps.

PROJECT: INFRASTRUCTURE & CIVIL ENGINEERS

A FTSE100 business that builds and manages some of the largest UK building projects.

Solution: Symantec Endpoint Protection (SEP)

Scope: The healthcheck and upgrade of SEP core component including those within the 4,000 field offices spread throughout the UK.

PROJECT EXAMPLES:
ENDPOINT PROTECTION

TELECOMS PROVIDER

This long established provider of telecom services has an international presence, and is a well recognised provider within the UK.

Solution: Exceeding 10,000 Symantec Endpoint Protection (SEP) and Data Centre Security Advanced (DCSA)

Scope: The design and implementation of SEP onto systems supported by the OS vendor. DCSA for systems that were out of OS support, consequently lacking ongoing patching and preventive security actions. SEP was deployed with all the advanced security functions enabled across data centres and endpoints. DCSA was deployed across Data Centre key production assets using least privilege access control and system hardening polices, to mitigate the lack of patch and anti-virus protection.

PROJECT: FINANCE INVESTMENT & ACQUISITIONS

A London based finance institute.

Solution: Symantec Protection Engine (SPE) for NAS

Scope: Design and install the SPE to ensure NAS or other third party proprietary storage protocols are not harbouring malware, and file shares are free from threats when being accessed or stored on such systems.

PRESS ASSOCIATION

"We needed our staff to focus on key business systems; having them distracted by non-core responsibilities is not the best use of resources. At the same time we recognised that we couldn't afford to compromise on the security of endpoints, as ultimately it's the strength of endpoints that keeps the underlining network safe from attack. It was this drive, to be able to focus our own resources and outsource key security responsibilities that led us to the managed SEP service from CSTL."

Damion Osborne – Head of Infrastructure Delivery

LOCKTONS INSURANCE PLC

"In the UK alone, we have offices on the south coast, in the Midlands, and in the city of London with just about every operating system and configuration you could imagine. We needed a product that offered maximum protection for users with flexible installation and management options. CSTL helped us identify an AV strategy, before installing and deploying the product in a professional whilst swift manner. The SEP solution has provided centralised control and complete protection against viruses, all of which has proved we made the right choice."

Nick Tam – Network Consultant

CUSTOMER **REFERENCES**

EXPRESS NEWSPAPERS & CHANNEL 5 NEWS

"We used CSTL to assist with the installation and setup of SEP, including the use of their "SUPA product" (Symantec Uninstaller Product Appliance) which allowed for a clean and rapid removal of the existing AV client solution. CSTL services enabled us to move very quickly to the latest version of SEP, allowing us to realise the investment we made in the shortest amount of time."

Dr Ben Dyer – Joint Head of IT

KUWAIT INVESTMENT OFFICE - LONDON

"CSTL have helped us with our Symantec security installation and setup services for over 8 years; allowing us to get on with our core IT objectives, whilst they take care of the SEP upgrades, policy tweaking and optimisation. Additionally CSTL played an instrumental role in the design and installation of our Symantec NAC solution to both to our production and DR sites."

Peter Groves – IT Security Manager

CUSTOMER **REFERENCES**

SYMANTEC PROFESIONAL SERVICE **OPTIONS**

Strategy & Architecture Design
Establish a customer's security objectives, understand the environment, and contrast with the Solution functionality and operational parameters to create high and low level designs.

Quick-Start
Rapid deployment and installation on a limited representative sample of systems. Used where the customer plans to complete the full roll out themselves, but wishes to quickly get to grips with the key setup tasks and benefit from knowledge transfer.

Deployment
Undertaking the full or partial Implementation of the Security Solution design. This option can remove the need for client personnel involvement, although we recommend that key staff are present to ensure product awareness and education.

Upgrade
Optimum performance and security protection will at some point require product upgrade. This service ensures existing options and policies are maintained, while introducing new functionality with supporting knowledge transfer.

Health-Check
An assessment and analysis to ensure optimum configuration[SML1] of security solution. Providing suggestions for improvement and best practice adoption. The scope of the service typically includes a review of:

- Version, installation review, sub component validation
- Architecture & structure design
- Policy and configuration best practice
- Functionality usage, and feature adoption

ELS (Early Life Support)
A service to assist Customers post- deployment, to help their technical team with the early stages of new technology adoption; to ensure optimum usage and technical familiarity.

Managed Support Service
A service designed to remove, and/or significantly reduce the resource burdens that a Customer has to sustain for the administration, usage and optimum performance of the Symantec solution or technology.

0207 627 7836

sales@cstl.com

www.cstl.com

GET IN TOUCH