



Think You Know Symantec?

Working Together to Secure the Cloud Generation

Quick Reference Guide to Symantec's Cyber Defence Platform



www.thinkyounowsymantec.com

QUICK REFERENCE GUIDE

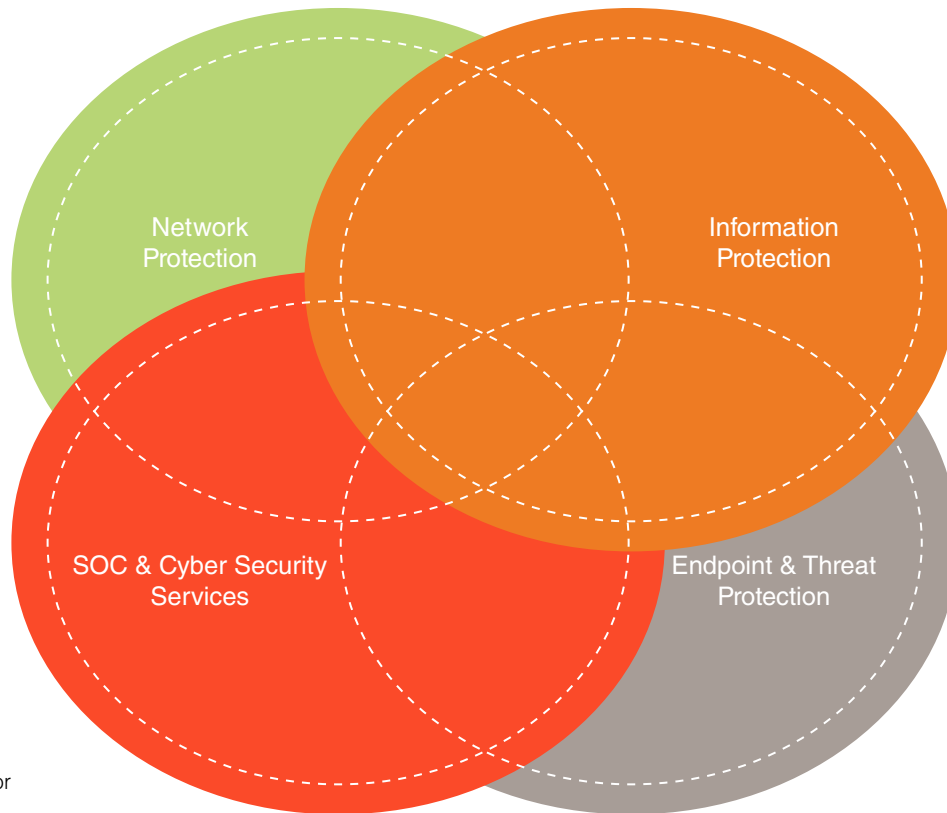
Symantec's integrated products offer unparalleled protection and insight to reduce risk and lower costs across organisations.

Solutions fall into 4 main categories:

-  Network Protection
-  Information Protection
-  Endpoint & Threat Protection
-  SOC & Cyber Security Services

Use this quick reference guide to gain an overview of the core products and solutions that make up Symantec's integrated Cyber Defence Platform.

Sections are colour coded by category with indexed items placed in alphabetical order for fast referencing.



QUICK REFERENCE GUIDE

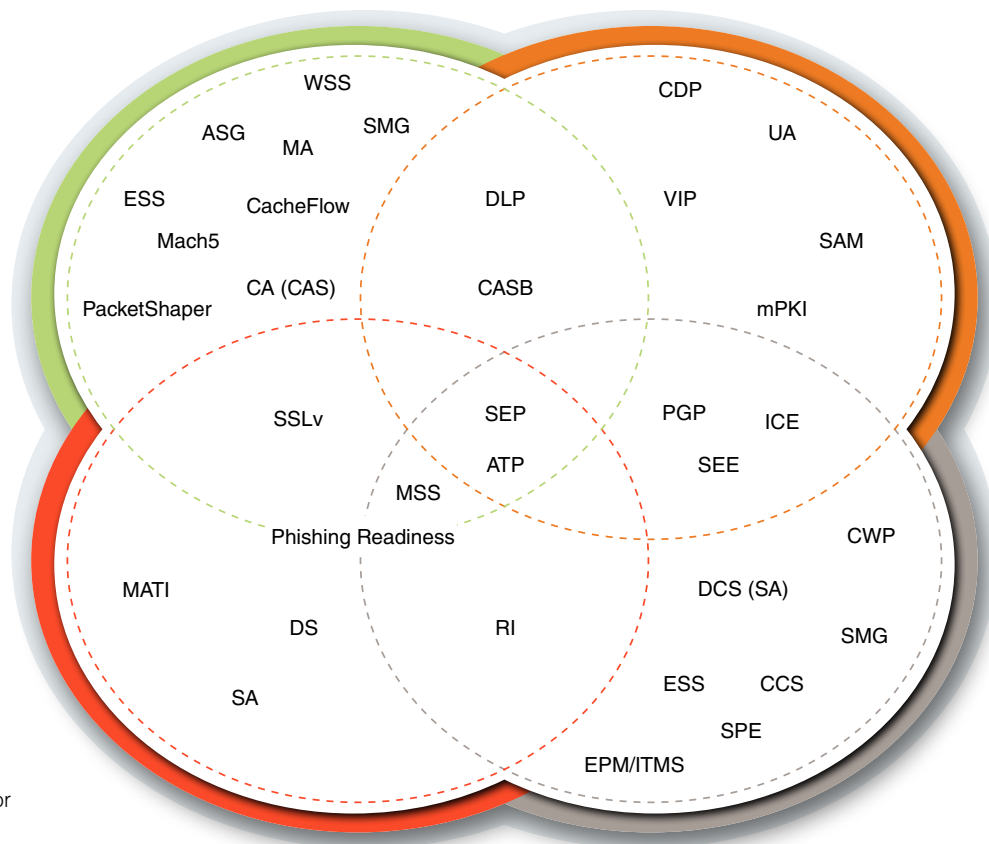
Symantec's integrated products offer unparalleled protection and insight to reduce risk and lower costs across organisations.

Solutions fall into 4 main categories:

-  Network Protection
-  Information Protection
-  Endpoint & Threat Protection
-  SOC & Cyber Security Services

Use this quick reference guide to gain an overview of the core products and solutions that make up Symantec's integrated Cyber Defence Platform.





Sections are colour coded by category with indexed items placed in alphabetical order for fast referencing.





NETWORK PROTECTION

Symantec's integrated network protection solutions protects users and critical assets with multi-layered security. By applying artificial intelligence to distil *nine trillion* lines of security data, Symantec offers the most extensive threat intelligence anywhere. Symantec applies visibility across all endpoints, mobile, network and cloud servers, to protect enterprises both on-premise and in the cloud.

INDEX TO SERVICES					
ASG	Advanced Secure Gateway	✓			
ATP	Advanced Threat Protection	✓	✓	✓	✓
CA (CAS)	Content Analysis (System)	✓			
CacheFlow	Caching Appliance for Service providers	✓			
CASB	Cloud Access Security Broker and CloudSOC (Previously Elastica)	✓	✓		
DLP	Data Loss Prevention	✓	✓		
ESS	Email Security Cloud	✓		✓	
MA	Malware Analysis (engine)	✓			
Mach5	WAN Optimisation (ProxySG) Appliance	✓			
MSS	Managed (Monitoring) Security Service	✓		✓	✓
PacketShaper	Bandwidth Management and Visibility Appliance	✓			
Phishing Readiness		✓		✓	✓
SEP	Symantec Endpoint Protection	✓	✓	✓	✓
SMG	Symantec Messaging Gateway	✓		✓	
SSLv	SSL Visibility Appliance	✓			✓
WSS	Web Security Service	✓			





NETWORK PROTECTION

ASG – Advanced Secure Gateway

- Powerful web security solution delivering world-class threat protection
- A scalable proxy designed to secure web communications and accelerate business applications
- Unique proxy architecture allows it to effectively monitor, control, and secure traffic to ensure a safe web and cloud experience
- Strong user authentication, advanced real-time web filtering and risk scores
- Multi-layered deep content inspection and analysis to identify data loss and threats
- Complete protection and control with layered defences
- Unmatched performance and reliability

ATP – Advanced Threat Protection

- A unified platform that Uncovers, Prioritises, Investigates, and Remediates advanced threats across multiple control points from a single console
- Each control point represents a vector which attackers can take advantage of to invade an organisation
- Four ATP modules:
 - ATP: Endpoint
 - ATP: Network
 - ATP: Email
 - ATP: Roaming
- Each module sends event information from different control points to the ATP platform that correlates and prioritises all the malicious events

CA (CAS) – Content Analysis (System)

- Unequalled protection against known, unknown, and targeted attacks
- A layered approach to protect against web and mail threats when paired with Symantec Blue Coat ProxySG or Secure Mail Gateway
- Uses Symantec and other leading security vendors for whitelisting and file reputation services
- Dual anti-malware engines, static code analysis, and dynamic analysis (on-box sandboxing)
- The best malware protection against targeted attacks available





NETWORK PROTECTION

CacheFlow – Caching Appliance for Service Providers

- Enables internet access providers, including ISPs, mobile operators and large institutions to better manage subscriber growth and excessive increases in network traffic
- Utilises highly effective caching technology to dramatically accelerate the delivery of rich web 2.0 content, including large files and video
- Saves bandwidth on expensive international links and backhaul traffic, which reduces infrastructure costs while improving customer satisfaction

CASB – Cloud Access Security Broker and CloudSOC (Previously Elastic)

- Enables companies to confidently leverage cloud applications and services while staying safe, secure and compliant
- Cloud application visibility and risk intelligence for thousands of apps
- Data governance, UBA and policy controls for sanctioned cloud apps
- Real-time user behaviour analytics, data security, and threat protection for un-sanctioned cloud apps
- Cloud data encryption and tokenization for regulatory compliant use of cloud apps

DLP – Data Loss Prevention

- Discover where data is stored across cloud, mobile, network, endpoint, and storage systems
- Monitors how data is being used, whether employees are on or off the network
- Protects data from being leaked or stolen—no matter where it's stored or how it's used
- Automates the process of detecting sensitive data with its comprehensive content-aware and context-aware detection capabilities
- Employs a powerful combination of industry-leading textual, non-textual, and machine-learning-based detection technologies

ESS – Email Security.cloud

- Filters unwanted messages and protects users from targeted attacks
- Self-learning capabilities and Symantec intelligence delivers highly effective and accurate email security
- Encryption and data loss prevention help control sensitive data
- Supports Microsoft Office 365, Google Apps, on-premises or hosted Microsoft Exchange, and other mailbox services
- Protects organisations from email-borne viruses, malware, cspam, phishing, targeted attacks, and bulk email





NETWORK PROTECTION

MA – Malware Analysis

- Automatically escalates and brokers zero-day threats for dynamic sandboxing and validation before sending content to users
- Allows enterprises to analyse unknown content from one central location
- Leveraging Symantec ProxySG, this solution uses a unique multi-layer inspection and dual-sandboxing approach to reveal malicious behaviour and expose zero-day threats, and safely detonate suspicious files and URLs



Mach5 – WAN Optimisation (ProxySG) Appliance

- Dramatically improves the performance of virtually all applications and workflows – from file transfers to backups, email, databases, video, and cloud applications
- The MACH5 S200, S400 and S500 families combine optimisation features such as protocol acceleration, compression, and caching to deliver high performance across IPv4 or IPv6 environments
- Deployed at the network core or the branch to ensure that every user experiences superior performance



MSS – Managed (Monitoring) Security Service

- Symantec Managed Security Services helps to determine which events are most dangerous and critical to organisations
- Delivers real-time notifications of threats, enabling teams to take fast action
- Continual 24x7 advanced threat monitoring
- Allows prioritisation of critical incidents and remediation needs
- Lowers incident investigation time



PacketShaper – Bandwidth Management and Visibility Appliance

- Controls bandwidth cost, delivers a superior user experience and aligns network resources with business priorities
- A cloud-connected WAN and internet appliance that provides visibility into applications and web content on the network
- Powerful application level policy management
- Integrated with the Symantec Global Intelligence Network to provide real-time traffic discovery and classification of hundreds of applications and tens of millions of websites



Phishing Readiness

- Conditions employees to recognise and report attacks
- Organisations can carry out simulated phishing attacks from a simple, centralised platform
- Easy to create and deploy targeted emails
- Analyses employee behaviour using detailed metrics to assess an organisation's susceptibility to phishing attacks





NETWORK PROTECTION

SEP – Symantec Endpoint Protection

- Addresses today's threat landscape with a comprehensive approach that spans the attack chain and provides defence in depth
- Utilises the world's largest civilian threat intelligence network - the Symantec Global Intelligence Network
- Can effectively stop advanced threats with next generation technologies that apply advanced machine-learning, file reputation analysis, and real-time behavioural monitoring



SMG – Symantec Messaging Gateway

- Delivers on-premises inbound and outbound messaging security on a single platform
- Catches more than 99 percent of spam, with less than 1 in 1 million false positives
- Real-time automatic antispam and antimalware updates
- In-depth reporting
- Can be implemented as a virtual or physical appliance



SSLv – SSL Visibility Appliance

- Provides unmatched visibility into encrypted traffic to protect against advanced threats, automatically identifies all SSL/TLS traffic regardless of port number or application
- Uncovers hidden threats that use SSL to bypass detection
- Selectively decrypts traffic to meet data privacy and compliance requirements
- Integrates seamlessly with the existing security infrastructure
- Simplifies management and administration



WSS – Web Security Service





- Proactive web protection capabilities delivered by the market's leading on-premises Secure Web Gateway, the Blue Coat ProxySG
- Resilient and effective cloud security service
- Protects enterprises from cyber threats
- Controls and protects corporate use of the cloud and the web
- Prevents data leaks
- Ensures compliance with information and web/cloud access policies





INFORMATION PROTECTION

Symantec has been named a leader in the Gartner Magic Quadrant for Information and Data Loss Prevention for the tenth consecutive time. Symantec Data Loss Prevention allows organisations to discover, monitor and protect sensitive corporate data. Data analysis is critical to GDPR compliance, understanding where data is stored and how it moves through the organisation is a crucial first step in order to meet the regulation.

INDEX TO SERVICES					
ATP	Advanced Threat Protection	✓	✓	✓	✓
CASB	Cloud Access Security Broker and CloudSOC (Previously Elastica)	✓	✓		
CDP	Cloud Data Protection (previously Perspecsys)		✓		
DLP	Data Loss Prevention	✓	✓		
ICE	Information Centric Encryption		✓	✓	
PGP	Encryption		✓	✓	
SEE	Symantec Endpoint Encryption		✓	✓	
SEP	Symantec Endpoint Protection	✓	✓	✓	✓
UA	User Authentication		✓		
VIP	Validation & Identity Protection		✓		
SAM	Access Manager		✓		
mPKI	Managed PKI		✓		





INFORMATION PROTECTION

ATP – Advanced Threat Protection

- A unified platform that Uncovers, Prioritises, Investigates, and Remediates advanced threats across multiple control points from a single console
- Each control point represents a vector which attackers can take advantage of to invade an organisation
- Four ATP modules:
 - ATP: Endpoint
 - ATP: Network
 - ATP: Email
 - ATP: Roaming
- Each module sends event information from different control points to the ATP platform that correlates and prioritises all the malicious events

CASB – Cloud Access Security Broker and CloudSOC (Previously Elastica)

Enables companies to confidently leverage cloud applications and services while staying safe, secure and compliant

- Cloud application visibility and risk intelligence for thousands of apps
- Data governance, UBA and policy controls for sanctioned cloud apps
- Real-time user behaviour analytics, data security, and threat protection for un-sanctioned cloud apps
- Cloud data encryption and tokenization for regulatory compliant use of cloud apps

CDP – Cloud Data Protection (previously Perspecsys)

- Ensures sensitive data remains secure
- Enables organisations to maintain the control they need to confidently adopt cloud services and comply with relevant guidelines and regulations
- Organisations can use cloud applications, such as Salesforce.com and ServiceNow, and continue to satisfy stringent data privacy and residency requirements
- Easily integrates into an organisation's cloud service implementation





INFORMATION PROTECTION

DLP – Data Loss Prevention

- Discover where data is stored across cloud, mobile, network, endpoint, and storage systems
- Monitors how data is being used, whether employees are on or off the network
- Protects data from being leaked or stolen—no matter where it's stored or how it's used
- Automates the process of detecting sensitive data with its comprehensive content-aware and context-aware detection capabilities
- Employs a powerful combination of industry-leading textual, non-textual, and machine-learning-based detection technologies

ICE - Information Centric Encryption

- Delivers strong, simple protection that follows data wherever it's stored, used, or moved
- Protects data with enterprise-strength techniques through the integration of Symantec Data Loss Prevention and Symantec CloudSOC (Cloud Access Security Broker) technologies
- Uses highly accurate data discovery engines, detects sensitive data on-premise, in cloud and mobile locations

PGP – Encryption

- Safeguards data on computers, laptops, tablets, hard drives, removable media, files, email systems, and cloud-based applications (including SaaS)
- Allows enterprises to collaborate with confidence, protect data and facilitate compliance without compromising performance
- A family of robust and scalable encryption options that represent the widest variety of encryption offerings on the market - Symantec Endpoint Encryption, Symantec Email Encryption, Symantec File Share Encryption, Symantec SSL Suite for Enterprise

SEE – Symantec Endpoint Encryption

- Strong full-disk and removable media encryption
- Maximum protection including support for virtual machines, native OS encryption such as BitLocker, FileVault 2 and OPAL compliant self-encrypting drives
- Ease of use with single sign on support
- Multiple recovery options including self-recovery and web console for Helpdesk staff
- Flexible removable media support





INFORMATION PROTECTION

SEP – Symantec Endpoint Protection

- Addresses today's threat landscape with a comprehensive approach that spans the attack chain and provides defence in depth
- Utilises the world's largest civilian threat intelligence network - the Symantec Global Intelligence Network
- Can effectively stop advanced threats with next generation technologies that apply advanced machine-learning, file reputation analysis, and real-time behavioural monitoring

UA – User Authentication

• VIP: Validation & Identity Protection

- A leading user-friendly, cloud-based, strong authentication service that provides secure access to sensitive data and applications anytime, anywhere, from any device

• SAM: Access Manager

- A next generation access control platform that establishes a new control point for cloud security
- Enables enterprise IT to meet user demands for ease of use with single sign-on for multiple web and cloud applications; while ensuring a high level of security
- Captures related access and security event information to meet compliance requirements

• mPKI: Managed PKI





- A cloud-based service that enables organisations to issue, renew, and revoke digital certificates that can be used to power strong authentication, encryption, and digital signing applications





ENDPOINT & THREAT PROTECTION

Symantec's integrated endpoint and threat protection solutions work together to protect users and improve detection, encryption and security management. Symantec's award winning solutions boast over 15 year's market share leadership, with Symantec recognised as a Leader in every Gartner Magic Quadrant for Endpoint Protection Platforms.

INDEX TO SERVICES					
ATP	Advanced Threat Protection	✓	✓	✓	✓
CCS	Control Compliance Suite			✓	
CWP	Cloud Workload Protection			✓	
DCS (SA)	Data Center Security (Server Advanced)			✓	
EPM/ITMS	Endpoint Management/IT Management Suite			✓	
ESS	Email Security Service (or Email Security.cloud)	✓		✓	
ICE	Information Centric Encryption		✓	✓	
MSS	Managed (Monitoring) Security Service	✓		✓	✓
PGP	Encryption		✓	✓	
Phishing Readiness		✓		✓	✓
RI	Risk Insight			✓	✓
SEE	Symantec Endpoint Encryption		✓	✓	
SEP	Symantec Endpoint Protection	✓	✓	✓	✓
SMG	Symantec Messaging Gateway	✓		✓	
SPE	Symantec Protection Engine (for NAS, SharePoint, Exchange & Cloud)			✓	





ENDPOINT & THREAT PROTECTION

ATP – Advanced Threat Protection

- A unified platform that Uncovers, Prioritises, Investigates, and Remediates advanced threats across multiple control points from a single console
- Each control point represents a vector which attackers can take advantage of to invade an organisation
- Four ATP modules:
 - ATP: Endpoint
 - ATP: Network
 - ATP: Email
 - ATP: Roaming
- Each module sends event information from different control points to the ATP platform that correlates and prioritises all the malicious events

CCS – Control Compliance Suite

- A compliance and security assessment solution that provides users with the ability to run security and compliance assessments on their environment (public, private, and physical) across servers, endpoints, and critical network infrastructure
- Organisations can report on their compliance posture against industry best practices and key mandates like Payment Card Industry, International Organisation for Standardisation, National Institute of Standards and Technology, and many others

CWP – Cloud Workload Protection

- Automates security for public cloud workloads, enabling business agility, risk reduction, and cost savings for organisations, while easing DevOps and administrative burdens
- Rapid discovery, visibility, and elastic protection of AWS and Azure workloads enable automated security policy enforcement to protect applications from unknown exploits

DCS (SA) – Data Centre Security (Server Advanced)

- Provides complete server protection
- Full application control enables micro segmentation, administrator privilege de-escalation, patch mitigation, and protection against zero day threat in private/public cloud data centres





ENDPOINT & THREAT PROTECTION

EPM/ITMS – Endpoint Management/IT Management Suite

- Helps IT administrators securely manage endpoint configuration, PC personality migration, and software applications across Windows, Mac, Linux, UNIX, and virtual environments
- Allows management of assets and patches to reduce costs and increase productivity
- Reduces user downtime and increases IT efficiency through automated, repeatable processes

ESS – Email Security.cloud

- Filters unwanted messages and protects users from targeted attacks
- Self-learning capabilities and Symantec intelligence delivers highly effective and accurate email security
- Encryption and data loss prevention helps control sensitive data
- Supports Microsoft Office 365, Google Apps, on-premises or hosted Microsoft Exchange, and other mailbox services
- Protect organisations from email-borne viruses, malware, cspam, phishing, targeted attacks, and bulk email

ICE - Information Centric Encryption

- Delivers strong, simple protection that follows data wherever it's stored, used, or moved
- Protects data with enterprise-strength techniques through the integration of Symantec Data Loss Prevention and Symantec CloudSOC (Cloud Access Security Broker) technologies
- Uses highly accurate data discovery engines, detects sensitive data on-premise, in cloud and mobile locations

MSS – Managed (Monitoring) Security Service

- Symantec Managed Security Services helps to determine which events are most dangerous and critical to organisations
- Delivers real-time notifications of threats, enabling teams to take fast action
- Continual 24x7 advanced threat monitoring
- Allows prioritisation of critical incidents and remediation needs
- Lowers incident investigation time

PGP – Encryption

- Safeguards data on computers, laptops, tablets, hard drives, removable media, files, email systems, and cloud-based applications (including SaaS)
- Allows enterprises to collaborate with confidence, protect data and facilitate compliance without compromising performance
- A family of robust and scalable encryption options that represent the widest variety of encryption offerings on the market - Symantec Endpoint Encryption, Symantec Email Encryption, Symantec File Share Encryption, Symantec SSL Suite for Enterprise





ENDPOINT & THREAT PROTECTION

Phishing Readiness

- Conditions employees to recognise and report attacks
- Organisations can carry out simulated phishing attacks from a simple, centralised platform
- Easy to create and deploy targeted emails
- Analyses employee behaviour using detailed metrics to assess an organisation's susceptibility to phishing attacks

RI – Risk Insight

- Provides security risk scores on over a dozen key performance metrics that enterprises can measure and track
- Quantified measures of security risk, benchmarked against peers allows organisations to confidently assess the risk to their environment
- Allows organisations to make informed decisions on which security settings to change, actions to take, and investments to make to improve security posture

SEE – Symantec Endpoint Encryption

- Strong full-disk and removable media encryption
- Maximum protection including support for virtual machines, native OS encryption such as BitLocker, FileVault 2 and OPAL compliant self-encrypting drives
- Ease of use with single sign on support
- Multiple recovery options including self-recovery and web console for Helpdesk staff
- Flexible removable media support

SEP – Symantec Endpoint Protection

- Addresses today's threat landscape with a comprehensive approach that spans the attack chain and provides defence in depth
- Utilises the world's largest civilian threat intelligence network - the Symantec Global Intelligence Network
- Can effectively stop advanced threats with next generation technologies that apply advanced machine-learning, file reputation analysis, and real-time behavioural monitoring





ENDPOINT & THREAT PROTECTION

SMG – Symantec Messaging Gateway

- Delivers on-premises inbound and outbound messaging security on a single platform
- Catches more than 99 percent of spam, with less than 1 in 1 million false positives
- Real-time automatic antispam and antimalware updates
- In-depth reporting
- Can be implemented as a virtual or physical appliance

SPE – Symantec Protection Engine

Scalable, high-performance malware detection and prevention for cloud services, NAS devices, and SharePoint servers





- **For NAS**
 - Provides scalable, high-performance threat detection services to protect valuable data stored on network attached storage (NAS) devices
 - Increased scanning performance and improved detection capabilities for protection against multi-blended threats
 - Protection Engine includes Symantec's industry-leading malware protection, including Symantec Insight™ technology, for fast, scalable, and reliable content scanning services
- **For SharePoint**
 - Detects and removes viruses, spyware, and other threats in files uploaded to and downloaded from SharePoint server(s)
 - Using Symantec award-winning antivirus technologies quickly scans files for potential threats.
 - Integrates with the SharePoint Administration Console, enabling easy and seamless management of SharePoint server environments
- **For Cloud**
 - A flexible and feature-rich client/server application that allows customers to incorporate malware and threat detection technologies into almost any application
 - Powered by Symantec Insight, Protection Engine gives customers access to innovative security that will ensure their information and employees stay safe on the Web
 - Puts files in context using their age, frequency, location, and more to expose threats otherwise missed
 - Includes Symantec's proprietary, patented URL categorisation technology and industry-leading malware protection for fast, scalable, and reliable content scanning services





SOC & CYBER SECURITY SERVICES

Symantec's Cyber Security Services cover everything from awareness and intelligence to risk insight and managed security services. Symantec's Cyber Security Services empowers customers with global threat visibility and the expertise of over 500 security professionals around the world, 24x7x365 global threat monitoring and analysis; a constant stream of adversary and threat intelligence; incident readiness and response retainers, and a simulated virtual training environment so customers can quickly detect, assess and respond to advanced threats.

INDEX TO SERVICES					
ATP	Advanced Threat Protection	✓	✓	✓	✓
DS	DeepSight intelligence feeds				✓
MATI	Managed Adversary Threat Intelligence				✓
MSS	Managed (Monitoring) Security Service	✓		✓	✓
Phishing Readiness		✓		✓	✓
RI	Risk Insight			✓	✓
SA	Security Analytics (previously Solera)				✓
SEP	Symantec Endpoint Protection	✓	✓	✓	✓
SSLv	SSL Visibility Appliance	✓			✓





SOC & CYBER SECURITY SERVICES

ATP – Advanced Threat Protection

- A unified platform that Uncovers, Prioritises, Investigates, and Remediates advanced threats across multiple control points from a single console
- Each control point represents a vector which attackers can take advantage of to invade an organisation
- Four ATP modules:
 - ATP: Endpoint
 - ATP: Network
 - ATP: Email
 - ATP: Roaming
- Each module sends event information from different control points to the ATP platform that correlates and prioritises all the malicious events

DS – DeepSight intelligence feeds

- A cloud-hosted cyber threat intelligence platform
- Provides access to both Adversary Intelligence and Technical Intelligence
- Intelligence is drawn from Symantec's broad portfolio of security products, as well as its adversary intelligence operations, which include security research and analysis teams positioned across the globe
- DeepSight Intelligence data is enriched, verified and analysed to provide attribution and to connect seemingly disparate indicators into campaigns with known actors and motivations
- The solution is available via a web portal, data feeds or restful APIs

MATI – Managed Adversary Threat Intelligence

- A complete range of threat intelligence along with supporting research tools that encompass information on vulnerabilities, malware, indicators of compromise, campaigns, tactics/techniques/procedures, and adversary profile
- Provides enterprises with a complete view of relevant threats and exposures
- Managed Adversary and Threat Intelligence (MATI) research, Directed Threat Research (DTR), a full range of technical intelligence, and management mechanisms for data feeds and the API are accessible via a customisable portal





SOC & CYBER SECURITY SERVICES

MSS – Managed (Monitoring) Security Service

- Symantec Managed Security Services helps to determine which events are most dangerous and critical to organisations
- Delivers real-time notifications of threats, enabling teams to take fast action
- Continual 24x7 advanced threat monitoring
- Allows prioritisation of critical incidents and remediation needs
- Lowers incident investigation time



Phishing readiness

- Conditions employees to recognise and report attacks
- Organisations can carry out simulated phishing attacks from a simple, centralised platform
- Easy to create and deploy targeted emails
- Analyses employee behaviour using detailed metrics to assess an organisation's susceptibility to phishing attacks



RI – Risk Insight

- Provides security risk scores on over a dozen key performance metrics that enterprises can measure and track
- Quantified measures of security risk, benchmarked against peers allows organisations to confidently assess the risk to their environment
- Allows organisations to make informed decisions on which security settings to change, actions to take, and investments to make to improve security posture



SA – Security Analytics (previously Solera)

- Combines security visibility, security analytics, and real-time intelligence for immediate detection and effective incident response
- Provides the details that expose the full source and scope of any threat or attack targeting an organisation's assets
- Significantly speeds up the time to conduct complete network forensic investigations
- Award winning technology & features





SOC & CYBER SECURITY SERVICES

SEP – Symantec Endpoint Protection

- Addresses today's threat landscape with a comprehensive approach that spans the attack chain and provides defence in depth
- Utilises the world's largest civilian threat intelligence network - the Symantec Global Intelligence Network
- Can effectively stop advanced threats with next generation technologies that apply advanced machine-learning, file reputation analysis, and real-time behavioural monitoring

SSLv – SSL Visibility Appliance

- Provides unmatched visibility into encrypted traffic to protect against advanced threats, automatically identifies all SSL/TLS traffic regardless of port number or application
- Uncovers hidden threats that use SSL to bypass detection
- Selectively decrypts traffic to meet data privacy and compliance requirements
- Integrates seamlessly with the existing security infrastructure
- Simplifies management and administration



Network Protection



Information Protection



Endpoint & Threat Protection



SOC & Cyber Security Services



Think You Know Symantec?

Working Together to Secure the Cloud Generation

www.thinkyouknowsymantec.com

SALES

Adam Perks
Business Unit Manager
APerks@exclusive-networks.com

Kadie Bradder
Product Sales Specialist
KBradder@exclusive-networks.com

Samantha Ward
Product Sales Specialist
SWard@exclusive-networks.com

TECHNICAL

Kevin Hughes
Senior Security Consultant
KHughes@exclusive-networks.com

MARKETING

Vanessa Cardwell
VCardwell@exclusive-networks.com

For further information, technical advice or support on any of the Symantec products listed please contact your Exclusive Network's Symantec Channel team.

Exclusive Networks Ltd, Alresford House, Mill Lane, Alton, GU34 2QJ

Tel: +44 (0)845 521 7217

www.exclusive-networks.co.uk

