Symantec – Overview and Information Centric Security

Dharmendra Lad
Sr. Principal Solutions Engineer

HCISPP®
Global market leader in Endpoint Security, Email Security, Data Loss Prevention and Website Security, User Authentication

Enterprise focus on three core solution areas:
• Advanced Threat Protection
• Information Protection Everywhere
• Cybersecurity Services

Largest consumer security footprint on the planet – 67M

Secures 90% of F500 and 370,000 organizations around the world

Symantec

The Global Leader in Cyber Security

Global market leader in Web Security and Cloud Security

Delivers integrated solutions in six primary security arenas:
• Advanced Web and Cloud Security
• Advanced Threat Protection
• Encrypted Traffic Management
• Incident Response, Analytics and Forensics
• Web Application Protection
• Network Performance and Optimization

Secures 15,000 organizations globally including over 70% of the Fortune 500.

Blue Coat

Leader in Network + Cloud Security
Symantec | At a Glance

- **175M** endpoints under protection
- **$4.6B** annual revenue
- **2123** patents
- **385,000** customers worldwide
- **3000+** R&D engineers
- **6 SOCs** threat response centers
Complex User Definition
Evolving Data Attack Surface
Expanding Perimeter
Multi-Phased, Multi-Staged Attacks
Complex User Definition
Complex User Definition
The Expanding Network
Direct Connect Creates Expanded Networks to Protect

SSL Encryption
Security Stack

Headquarters
Data Center
Regional Office
Roaming Users

Personal Devices
IOT Devices

Copyright © 2017 Symantec Corporation
Multi-Phased and Multi-Staged Attacks

SSL Encryption

Security Stack

Regional Office

Data Center

Headquarters

Roaming Users

SSL Encryption

Personal Devices

IOT Devices

Copyright © 2017 Symantec Corporation
Innovation for the Cloud Generation: Ensuring Safe Cloud Usage
Symantec | Global Intelligence

Discovered **430 million** new unique pieces of malware last year

**1B** malicious emails stopped last year

**100M** social engineering scams blocked last year

**12,000+** Cloud applications discovered and protected

**182M** web attacks blocked last year

**1 Billion** previously unseen web requests scanned daily

**2 Billion** emails scanned per day

**175M** Consumer and Enterprise endpoints protected

9 global threat response centers with **3,000** Researchers and Engineers
Integrated Information Protection Solutions
Challenges with information protection

Adoption of cloud workloads
Cloud repositories
Cloud email
Accessed from everywhere by any device
Data shared with employees and others
Comprehensive Symantec Email Security Solution
- Hosted Service (Email Security + ATP + DLP)

A single control point for Threat & Information Protection

Solution Overview

- Blocks targeted attacks, spear phishing, viruses & malware, spam, and bulk mail
- Controls sensitive data and helps meet compliance & privacy requirements
- Detects new and stealthy targeted & advanced attacks
- Provides deep visibility into targeted attacks and accelerates remediation
DLP + Cloud Proxy (WSS) Overview

Enterprise Network

1. All web/cloud traffic is routed through the Web Security Service (WSS)
2. Information sent to Symantec DLP Cloud for Inspection
3. DLP decision is sent back to WSS, incident is generated in DLP console in case of violation
4. Information sent to web/cloud if appropriate
Extending DLP to the Cloud with CASB

Extend DLP to 60+ Cloud Apps
Apply Fine-Tuned Policies to Cloud
Leverage Workflow Integrations
Gain CASB Functionality
• Shadow IT Analysis
• Granular Visibility and Control
• User Behavior Analytics

Symantec CASB
Symantec Cloud DLP

Unmanaged devices
Extended perimeter

Managed devices with DLP
Endpoint Agent

Corporate Datacenter

Symantec DLP Management Console

Copyright © 2016 Symantec Corporation
DLP for API based CASB Protection

Coverage for 5 SaaS Apps
DLP for Gateway based CASB Protection

Coverage for 57 SaaS Apps
Detection Rules based on Contextual Data from CASB

- Enhanced DLP policy language enables combining context (including UBA) from CASB with advanced content detection in DLP

- Rules based on six contextual dimensions:
  - **User** (User Risk Score, Internal/External)
  - **Region** (Country/Geo-location of the device)
  - **Cloud Application** (Application Name/Sanctioned)
  - **Activity** (Upload/Download, Sharing)
  - **Device Posture** (Managed/BYOD)
  - **Doc Meta-Data** (Internal/External, File Type)

- Allows for highly targeted DLP Policies
Use Case 1
Device & Region-based Policies

Prevent Downloads to unmanaged devices outside a country
Use Case 2
Combine UBA User Threat Score with DLP Content Rules

Prevent High Risk Users from Sharing Intellectual Property
Deep-links with CloudSOC’s User Threat Tree

User Details

User Threat Score: More Info
User is Internal: Yes
User Activity: More Info
Deep-links with CloudSOC’s User Activity

![Enforce Console](image_url)
Information Centric Security
New Approach – Introducing Information Centric Security

See Data Wherever It Lives

Visibility

Control Authorized User Access

Control

Protect Data from Being Leaked

Protection
Maintain visibility

DLP provides visibility to business critical data – on endpoint, storage, in motion, and email

CASB extends the granular DLP policy to cloud apps

Every Device

Public WiFi
Home Office
On-prem datacenter
Regional Office
Mobile
BYO

Every Location
How can I protect my sensitive data when it’s outside my control?

Encryption will keep your data secure from unwanted access, wherever it resides.
How can I ensure my data will not be compromised?

Multi-Factor Authentication (MFA) controls access by protecting your data from stolen credentials.
How it all works

- Per File Encryption
- Identity driven decryption, simple user experience
- Granularly Revocable Files
- Central monitoring & control

VIP
DLP
ICE
CASB

Centralized Management Console

AUTHENTICATION

Vendors
Clients
Partners
Co-workers

Access Granted
Access Denied
Revoke File

Per File Encryption
Identity driven decryption, simple user experience
Granularly Revocable Files
Central monitoring & control
Solution Benefits

Solution at a Glance

Solution Overview
Information Centric Encryption integrates with DLP, CASB and Identity to automatically protect sensitive data, and ensure only intended users can access it. Cloud based monitoring and controls allow user access to be revoked remotely, ensuring data protection throughout its lifecycle.

Combined Solution Benefits

- **Automatically protect sensitive data using DLP policies:** Automatic encryption of sensitive data using existing DLP policies
- **Improved DLP Effectiveness:** Extend control over data as data access can be set and controlled from the cloud, with a simple user experience
- **Comprehensive Policy Enforcement:** Apply consistent DLP controls for on-premises and cloud applications.
- **Maintain Privacy Compliance** – ability to protect and monitor data and revoke an individual user’s access as required
- **Integrated:** With DLP and VIP, no special APIs required
Thank you.

dharmendra_lad@symantec.com
707-331-0336