Symantec Ransomware Protection
Protection Against Ransomware

Defense in depth across all control points is required to stop ransomware

Email
Symantec Email Security.cloud, Symantec Messaging Gateway
- Perform static analysis of malicious indicators within files or documents
- Detonate potentially malicious scripts in sandbox before email delivery and block if signs of malicious behavior evident
- Block malicious links with real-time link following before email delivery and link analysis at click-time post delivery

Web
Symantec Secure Web Gateway Solutions*
- Block malicious sites including command & control and encryption server
- Analyze files for suspicious behavior from unknown URLs for ransomware activity using multi-layer and live threat feeds
- Malware Analysis looks for ransomware-specific behaviors and detonates unknown files in a sandbox before delivering

Endpoint
Symantec Endpoint Protection 14, ATP: Endpoint (EDR)
- Advanced Machine Learning detects polymorphic malware
- Emulator unpacks evasive malware while Behavior Analysis uncovers ransomware actions
- IPS blocks ransomware's attempt to download encryption keys
- Isolate endpoints when ransomware is detected to prevent lateral movement
- Hunt for ransomware IoCs across all endpoints

Workload
Symantec Data Center Security: Server Advanced
- 'Out of the box' IPS rules can prevent ransomware executables from being dropped or executed on the system
- Customers not using full IPS protections can deploy policies to block specific malware executables
- Additional rules can be applied to block all in/outbound SMB traffic
- Ransomware can also be blocked by adding executable hashes to global no-run lists

*ProxySG, WSS, GIN, Content and Malware Analysis, Security Analytics, SSLV
How do Ransomware Attacks Work?

1. Malicious Email or Website Armed
2. Malware Delivery
3. Malware Installed
4. Call C&C Server
5. Encryption
Symantec Email Security.cloud Ransomware Protection

1. Email with Malicious Payload or Link
   - Advanced Heuristics
     - Static/Dynamic Detections
     - Script Analyzers

Cloud-Based Sandboxing
- Advanced Machine Learning
- Behavioral & Network Analysis

2. Malicious Email Blocked
   - Real-Time Link Following & Click-Time URL Protection
     - Link Evaluation at Email Delivery
     - Link Evaluation at Click-Time
Messaging Gateway Ransomware Protection

1. Email with Malicious Payload or Link
   - Reputation Analysis
     - Email Sender Authentication
     - URLs
   - Anti-Malware Scan
   - Sanitize URLs & Files
     - Reconstruct & reattach clean links & attachments before sending to end user
   - Malicious Email Blocked
Symantec Content Analysis: ID and Block Ransomware
First Layer of Analysis Identifies and Blocks Ransomware

Content Analysis

- Hash Reputation
  Custom user whitelist/blacklist + Risk Scoring
  5 Billion file reputation database

- Dual Anti-Malware/Anti-Virus
  Combine Kaspersky, Sophos or McAfee
  Files up to 5GB / Signature updates every 5 minutes

- Predictive File Analysis
  Static Code Analysis / Machine Learning
  Parse and collect files / Match code to 4B "bad"

- Dynamic Sandboxing
  VM + Emulation Sandboxing using custom
  "Gold Images" Behavior and YARA rule analysis

- Global Intelligence Network

- Ransomware identified and blocked
- Signatures evaluated for known Ransomware
- Analyzes code for Ransomware attributes
- Sandboxing reveals Ransomware behavior

Proxy/SMG
Web / Mail Threat Protection
- URL Reputation
- SSL Decryption
- Categorization / policy
- Spam detection
- Real-time blocking

Additional Sandbox
SEP 14: Ransomware Protection

1. Malware Delivery
2. Malware installed
3. Call C&C Server
4. Encryption

- Exploit Mitigation, Machine Learning
- Intrusion Prevention
- Behavior Analysis, App Control
Data Center Security: Server Advanced Ransomware Protection

- Attack from Internet or Peer on Local Network
  - Out of the box’ IPS Policies
    - Windows 6.0 (and up)
      - Basic, Hardening and Whitelisting
  - ‘Out of the box’ IPS Policies
  - Kernel and Network Policies
    - Block all in/outbound SMB traffic
  - Custom IPS Policies
  - Global No-run List
    - Ransomware hashes added to no-run list
    - Block ransomware executables

- Attacks and Malware Blocked at Any Stage
IT Management Suite: Stop Ransomware

1. Patch Assessment

CVE 2017-0144

2. Patch Delivery

ITMS Determines Appropriate Patches

3. Patches Installed

ITMS Delivers Patches to Endpoint

4. Malware Delivery

5. Exploit Fails
Cyber Security Services
Actionable Threat Intelligence, Continuous Threat Monitoring, & Rapid Incident Response

**Actionable Intelligence**
*Symantec DeepSight Intelligence*
- Get ahead of an attack with advance notice of threat activity
- Prioritize patching with vulnerability ratings/alerts to protect against ransomware
- Implement countermeasures against attacks by leveraging in-depth adversary intelligence on threats, campaigns, attribution, and motivation

**Continuous Monitoring**
*Symantec Managed Security Services*
- Detect ransomware spread to minimize impact
- Monitor SOC operations 24x7 and apply global intelligence to identify threats and prioritize actions
- Apply advanced analytics and machine learning to identify previously unknown indicators and stealth attacks

**Rapid Response**
*Symantec Incident Response Services*
- Respond quickly to engage the adversary, contain the attack, and mitigate future attacks
- Reconstruct the attack to determine 'Patient Zero' and whether data is encrypted, deleted, or being stolen
- Hunt for advanced threats with intelligent forensics tools and expert analysis