**Symantec DLP User Group: Detailed Notes for 12-6-11**

**User Group Member Presentations:**

1:15 PM

- Jeff Streelman (Citi)

- Tom McMahon (Weill Cornell Medical College)

**Symantec Presentations**

2:00 PM

- DLP for Tablets by Mario Espinoza

- DLP 12 (Whitney)

**Key Interests from Introductions:**

Al Carvallo, UPS

Key Interests: Maturation Product with integration with a correlation of incidences. DLP is a maturation process with multi-year effort to process and integrate with other processes and integration with other products.

Various Key Interests from the group:

* DLP for Tablets
* Remediation and whole practice around DLP
* Best Practices and “Golden Rules”
* Looking to absorb the information from the group
* Looking to get ideas on DAR implements
* Web prevent in monitor mode in a large scale implementation
* ICAP integration with BlueCoat
* Interest in Data Insight
* Looking to exchange ideas
* Looking to get a consensus of what people are doing with DLP
* General roadmap
* Integration: RSA Archer product and trying to do remediation
* Integration: Web Prevent integration with Checkpoint proxy solution
* Integration: WebSense security gateway with DLP solution

**1st User Presentation: Weill Cornell Medical College Presentation, Tom McMahon**

* Organization Size: 7K Users
* Provider for New York Presbyterian, 36K Users
* Security services: email, internet, perimeter security

**Symantec Systems**

* Vontu DLP
* SEP 11
  + Win 4500 systems
  + OS X - 100 systems
* PGP WDE
  + PC 600 Systems
  + OS X (Apple)

**Deployment:**

* Network Prevent
  + 37K mailboxes
  + 20 GB a day
  + 10K incidents a day
* Endpoint Prevent
  + 600 Endpoints
  + 1K incidents a day
* Network Discovery
  + 150 external web sites
  + 1 Server
* Network Monitor
  + ~600 mbps
  + 120 GB a day
  + 10K incidents a day
  + 6 restarts a day!

**Not Deployed**

* Data Insight
* SharePoint Scanner

**Trouble Points**

* Network Prevent for Web
* Blue Coat and Symantec integration issues (DLP 11)
  + Initially deployed in August with BlueCoat engineer with SSL interception using icap. Bluecoat was trying to send to Symantec via icap with service not recognized. There was back and forward coordination with Symantec and Bluecoat. We will retry the Blue Coat integration after the DLP11 upgrade.
* DLP11 Upgrader
  + Fixing network detect
  + Fixing EDM
* EDM (SQL Preindexer for MSSQL)
  + EMR system: 1.3 MM patient records and doing an EDM pull. DLP 11 stops supporting MSSSQL on the preindexer.
  + Currently using Indexer for 10.5 in DLP 11 systems

Would want more information on the following:

* DLP for Tablets
* DLP in Virtual Infrastructure

**Key System Integration:**

* Asset Management System (what systems a person has access, help create response rules with attributes about the person)
* IDM Systems (take data from the IDM systems into DLP to get all the contacts and managers, key person vs. students)
* ArcSight
* VDI and DAR Scanning

**DLP Architecture:**

* Asset Management Systems ----> reference database DB to do attribute lookups from Enforce
* Clinical Warehouse for EDM process with Enforce
* Load balancers with network monitors and smtp gateways

**Challenges:**

* Effective remediation
* Too many incidents to manage
  + 100K a month
  + Need to triage the ones we care about
  + Correlation and severity in ArcSight
    - IDS/IPS, Av, Breach Detection log
    - Asset and User Sensivity
  + Repeat offenders need more security
  + Institution acceptance
    - Clinical Departments
    - Academic Department
    - Research Departments

**ArcSIght Use Cases:**

* Anonmyous activity: looking at 250 patients records
* AV and DLP

**Current DLP Portfolio Status / Follow-up Projects:**

* No blocking of email (blocking is next year)

**ArcSight Integration:**

* DLP Events to Syslog server to ArcSight
* Breach Detection system provides Fair Warning (Identity View from ArcSight to look at)
* ArcSight Integration Benefits:
  + Regulatory
    - Finding messy and insecure business process before they cause an incident
    - Help identify target departments for HIPPA and HITECH Assessments
  + Breach Prevention / Detection
    - Fining data and cleaning a system before it leaks sensitive data
    - Knowing that a system was infected when it has sensitive data on it
  + Time Savings: able to triage DLP events faster with SIEM (ArcSIght)

**DLP Endpoint Environment:**

* Deploying DLP Agents
* Adding systems in the vulnerability scanner
* Priority patching of servers

**DLP Support Resources:**

* No one is dedicated for DLP
* 3 people:
  + Engineer responsible for all security systems
  + Engineer for policy
  + Architect for design of security environment

**DLP Database:**

* Vontu database size is kept in check with only 6 month retention on data only (purging every 60 days).
* High severity events are not deleted.

**Repeat Offenders:**

* Repeat Offenders identify with ArcSight; processes with Compliance and HR group to facilitate identification. Legal should also be included.

**Reporting:**

* Hot Spots of data leakage included as part of the metrics to reports to management
* Audit loves it (as well as HR)
* ArcSight has many correlation rules within the product to raise visibility of threats.

**IDM / Vexa**

* Various data feeds are put in the reference database.

**2nd User Presentation: Citibank, Jeff Streelman**

**Point Number One:** Get a dedicated staff...

**Company Profile:**

* **Business Sector:** Financial
* Doing business in over 140 countries
* Number of worker: 350K
  + Located over 100 countries
* Amount of Data storage: 30+ PB
* Number of clients: 200+ million

**Core Businesses:**

* Regional Consumer Banking
* Institutional Clients Group
  + Securities and Banking
* Transaction Services

**Citi Holdings**

* Brokerage and Asset Management
* Local Consumer Lending

**DLP History Environment:**

* Network Monitor since November 2005 for Global usage of SMTP traffic only (for countries that allowed)
* Network Prevent in final testing phase. Network Prevent will be implemented by 1Q12 for Global usage of smtp traffic only
* Network Discover since December 2010. Currently only the US however will go global in 2012 and targeted for NAS and SharePoint
* Endpoint currently in pilot phase (250 people in pilot) with Global usage in January 2012 and scope is desktops, laptops, and thin clients (Citrix)
* Data Insight – we own some licenses but no plans yet for deployment. Potentially as a control around secure storage environment (i.e. secure SharePoint - more tightly controlled with DI) however there are no plans.

**DLP Environment:**

* VMWare Linux 64-bit boxes
* DLP 11.1 for all most of the servers
* IDM / HR systems feed into the Enforce
* All remediation is done through DLP system and not via ArcSight
* Repeat offender policy: 1st “detection” of a repeat offender goes to his manager; 2nd detection goes again to his manager and to HR. 3rd detection, for consultants, it’s a dismissal. For employees, a bigger discussion for HR (leak data via email substantial).
* Do not block emails yet.
  + Looking to blocking emails for only a very small subset.
  + Testing phase: blocking test timeframe started in September 2011. We will block where legally allowed.

**DLP Statistics:**

* Network Monitoring
  + Number of emails message processed per month > 25MM (more if application traffic is included 5:1)
  + Number of total incidents (manually reviewed): 10K per month (dedicated team of 8)
  + Number of events (not false positive): 1,100 per month
  + Number of countries: 91 Countries
  + Number of rules > 250
  + Type of monitoring rules:
    - A lot of EDM for US data
    - Data Identifiers, regular expressions
    - Blocking on EDM
* Network Discover (DAR)
  + Amount of data scanned at Citi > 30 PB
  + Sensitive data risk reduced by remediation of file containing instances with PII / PCI: 120,000,000 Files
  + Number of files scanned: 80 Billion
  + Number of SharePoint Sites: 80,000
  + Number of US Branches scanned: 2000
  + Number of Data Centers: 45

**Other Statistics / Notes:**

* 4 Data Centers are used for internet traffic with each site 1.5 Billion messages per month
* Highest false positives rates for Citi is based on User Security Classification
* Evolution of document can go from confidential to public and the business process needs to be developed to work with the DLP solution
* There is a team to determine if the data is sensitive by work with the ISOs
* Every business has an information security officer to look and verify if the information is sensitive or not with the business contacts.

**DAR Challenges:**

* Implementation
* Remediation
  + handling the flood of DAR incidents during initial scan is challenging
  + There is a lot to handle with large file systems – you need to look for hot spots.

**DAR Findings:**

* There is a lot of old data
* People do not encrypt the data
* Access to SharePoint is a challenge since people want to share.
* File shares are moved to different volumes around and consequently ownership info is lost.
* Windows Systems ID ownership is loss
* Did initial scan and only one incremental scan so far

**Governance**

* Country Clearance
  + Citi has centralized data privacy office which globally coordinates these efforts
  + Cross border implication (moving data across countries) with centralized Enforce server
  + Establishing strong defined roles and responsibilities to enforce segregation of duties (e.g. only someone from Switzerland can review Swiss data)

**Operation**

* DLP Product knowledge and training
* Citi has engaged an onsite Business Critical Engineer who assist with all technical activities around the Symantec DLP products (dedicated DLP resource)

**Database Design**

* Challenges when purging unused records

**Upgrades:**

* Synchronized of data between non-production and production environment is only semi-automated (sometimes you just have to manually key in the information)

**DLP Architecture:**

* Endpoint Systems uses separate Enforce Server
* Network monitor also uses separate Enforce server
* DAR again also uses separate Enforce serer

**Note:** Total of 3 separate Enforce Servers.

* Realities of Handling Multiple Enforce servers:
  + This is required for Citi due to the initial DAR volumes (Scaling required for global organization
  + There is no single console to combine / correlate incidents
  + MOM Console

**Enhancements:**

* Network monitoring
  + Generate count of items found during scan (do not generate incidents)
* Network discover (DAR)
  + Capture source and destination paths during network operations (Whitney candidate)
* EndPoint
  + Remove persistent network connections (Whitney Candidate v12)
  + Enhanced use pop-ups (HTML formatting > 300 chars,
  + Use windows local AD cache for LDAP groups
  + Support use of "counters" at agent
* Overall Improvements
  + White listing for policy exceptions (TLS)
  + Reclaim database space

**EndPoint (EP) Testing and Deployment Methodology:**

* Structured approach ensure success
* Risk analysis: what problems are you looking to solve?
* Product evaluation, selection and lab testing
* User acceptance testing with internal group
* Pilot testing with limited users globally
* Production deployment (staged and starting 2012)
* Performed evaluation based on real world use cases in partnership with businesses
* Brought in external vendor (Verizon Business Services)
* Performed rigorous side by side testing

**Open Discussion with Jeff Streelman**

* Integration between DLP and other products
  + PGP
  + Encryption DLP

**Question:** How do you handle remediation of the endpoint incidents?

**Response:**  Through pop-up and also analyze results of data leaked and classified business process. There are very limited use cases for blocking - laptop is offline and move data will be blocked.

* Big thing next year: push endpoints out to 350K and mine data to come up with ideas. Use the Endpoint as a training tool.
* DLP endpoint will be on any Citi owned devices including Citrix thin clients and vendor machines.

**Symantec DLP for Tablets Presentation:**

Enterprise Mobility and Consumerization of IT is driving the need for mobile content-aware DLP:

* Mobile devices, specifically tablets, are causing security headaches
* 47% said mobile computing is making cyber security more difficult
* 45% cited the consumerization of IT as a further complication
* 29% of enterprises use tablets today
* 67% Monitor, block, remove content

**DLP for Tablets: Solution Benefits**

* Balances protection with usability
* Reduce data loss risk
* Preserve access to confidential data
* Supports consumerization with coverage for personal and corporate use cases
* Preserves iPad app performance with common apps working as expected
* Works with any MDM solution: customer use their preferred solution

Question: What is the compatibility with a sandbox technology or MDM? DLP for Tablets should work better with MDM.

**Competitive Advantages:**

* Websense
  + No actual on-table coverage; the solution merely prevents email of confidential data to table using reverse proxy
* Verdasys
  + Leverages agents on Activesync and BlackBerry Enterprise server to protect
* Zenprise
  + Protect access to SharePoint / Ofice365

**Understanding Data Loss Risk on the iPad:**

* The iPad has multiple channels for data loss:
  + Default email client (corporate and personal mail)
  + Safari web browser (web uploads, social apps, webmail)
  + Apps (cloud storage, social apps, etc)
* Apple provide native capabilities to secure device and communication:
  + Secured app store, passwords, encryption, remote wipe, vpn server (MDM api)
  + Leverage the MDM API using the Symantec Mobile Management (SMM) product

**Solution Overview:**

* Agentless deployment for Symantec DLP Tablet Prevent Server
* Reduce risk of data loss from iPad with user’s having access to sensitive data
* Leverage the web prevent server capabilities for the following:
  + VPN - can be Apple or SSL (Juniper or Cisco VPN)
  + You have to have VPN access
  + Direct access to the internet is prevented
  + Proxy to Symantec tablet prevent server
* Architecture Flow:
  + DLP Enforce -> DLP Tablet Server -> Transparent Web Proxy -> VPN (not acting as a reverse proxy) -> iPad
  + Currently certified for Bluecoat for proxy.
  + DLP for Tablets routes iPad traffic through corporate VPN to DLP at all times.
  + -VPN is in the DMZ
  + iPad SMM Agent
    - Activesync had to be built in the app.
    - Apps on the iPad work different when blocking traffic.
  + ICAP traffic between the Prevent server and the iPad.
  + Certify Bluecoat and 2 most common VPNs; IPSEC and SSL requirements.
* AirWatch traffic to iPad
* Tablet for Prevent is complement to MDM
* Only works with Certificate based authentication to the VPN for the tablet Prevent server (e.g. VeriSign , MS certificates)
* The certificate has to be installed on the iPad.
* You can also have a password to the device
* Dual factor authentication cannot be enabled with the Tablet Prevent
* The MDM solution will need to be place in case the iPad is loss, etc to bolster the security
* Having only certificate based authentication for the VPN to Prevent negates password prompts and provides seamless access.
* Activesync in the DMZ to allow the corporate email access (internal) to the iPad (remote user)
* When you connect to an external site (e.g. Facebook), the VPN on Demand feature will be activated to monitor traffic, remove, etc

**Tablet options for Incidents:**

* There is a need to identity information in the incident for the tablet. Currently, we trying to query the VPN server to get additional information for the incident. DLP for Tablets is only in beta and currently working only with the Cisco VPN
* Get the information from the MDM server to get the information for the incident.
* Tablet Prevent server works very much like the Network Prevent box.

**VPN Settings and Tamper Protection:**

- DLP for Tablets relies for iOS VPN on Demand capability

- VPN setting can be deployed via the Symantec Mobile Management (SMM)

- SMM agent monitor changes the VPN setting and provides notifications

- An administrator can configure profile removal or device wipe in case of repeat offender. **Note:** This feature is unique to the Symantec MDM.

**DLP For Tablet Timelines:**

* Fuji - Advanced Reporting and analytics via SPC Q4 11 - Q1 12; report offline and report on different variables.
* Everest - Tablet Support Q1 CY12
* Diablo - Tablet v2 mid cy12 -more app support, performance metrics

**Symantec DLP v12 (Whitney) Presentation:**

* Whitney full DLP suite in Q4 Cy12
* Mac OS Support 1H CY13
* Some will like the support of Firefox beyond version 3 for Enforce.

**Aside:** Endpoint agent can use application control to monitor internet clients (Skype) however does not support EDM block.

**B. Core Product Enhancements - Strategic**

1. Reduce time-to-value - speed up hardware acquisition / deployment

2. Identity-centric DLP - common identity visibility and nomenclature; allow customer to see and act across individuals and groups; easily pull identity info ***without services***

3. Malicious insider protection - see and take action on repeat offenders; forensic investigation support - can have different rules for remediation

4. Symantec cross-product integration - encryption insight for full visibility into encrypted files; improving / expanding API

**Mail Quarantine**

* DLP / SMG quarantine management integration
* Do the management of the quarantine of the SMG from Enforce
* Enforce release, delete, encrypt.
* User self-remediation (note: like the pop-up for endpoint to self remediate the use).
* User receives notification with 1-time override.

**Core Product Enhancements - Strategic**

2. Identity-Centric DLP

* Phase 1 - Better visibility to actors behind DLP events (customer value) - Universal Feature candidates
* Phase 2 - More actionable data for user education, HR actions, etc
* Phase 3 - Unified policy and enforcement for access and use of confidential data across organization

**Question:** Will a web services capability help to query your systems?

**Response:** Yes, however web services for real-time transaction is slow and some customers are not ready.

**Content Visibility for Encrypted Files**

1. DLP synchronizes keys with Key Management Server (KMS)

2. Receive encrypted documents

3. Decrypts documents using cached keys

4. Evaluate DLP Policies on the decrypted document

**Note:** For Citi, password protected documents is also an issue.

**Workaround:** block password encrypted customer tools (WinZip) and allow corporate approved encrypted tools.

**Note:** There is a difference between Gateway encryption vs. traditional document encryption (Files shares, SharePoint)

* MS office plug-in to facilitate transparency to password protected files

**Direct Protect For Storage with Discover Server:**

1. Storage DLP finds sensitive files on shared storage

2. Data owners determined via Data Insight

3. Data owner key and corporate ADK retrieved (universal server)

4. File encrypted with data owner key and ADK.

**Information Protection - Different Protections Based on the Information's Value**

* Crown Jewels - Control with DLP +Encryption +IDentity+Content
* Company Confidential- Control with DLP + Encryption
* Sensitive Information - Control with DLP + encryption

**Question:** DLP deployment with VDI: is it scalable and is the performance acceptable?

**Response:** Yes, taken a 2nd look at VDI to leverage hypervisor

Support Citric to 10.5 agent on the Citrix sever or client image - 60 concurrent sessions with Windows 2008 r2 on one Citrix server for best practices

**Follow-up Meetings:**

There will be a follow-up Technical Advisory Board for Whitney release. There will be a webex invite for repeat offender.