SANS ANALYST PROGRAM

Sponsored by McAfee

Data Protection Prospective Vendor Checklist

A SANS Whitepaper – July 2009

Written by Barbara Filkins

Summary

Data-centric protections need to address data discovery and classification, incident workflow, policy creation/management and data movement detection. The breadth of technology required to accomplish all of this is broad, covering:

- Fully-integrated encryption for end points for data in use, in motion and at rest within applications (e-mail, file servers, etc.), including sensitive data transferred onto portable storage devices
- Host-based DLP for localized detection and prevention of data leakage for data in use, data in motion, and data at rest
- Network DLP with data discovery and analysis, network monitoring (with extensive protocol and application parsing support), and prevention capabilities for both inbound and outbound content

How should a management team go about evaluating today's encryption and emerging data leakage prevention (DLP) tools? What questions should they ask of the vendor provider(s)? How does a management team determine which solution being proposed will meet the most requirements for today—and in the future? How do they even set requirements without due diligence and discovery technologies to assist in locating and classifying what it is they need to protect? How do they weigh specific business requirements to product features? How do they gauge the stability of the vendor? How do they compare pricing models (per user, per server) and such additional factors as growth potential and integration with other vendor products to optimize their investments?

Organizations need a way to map business needs against all these challenges in procuring a technical solution. To help, SANS has developed the following Prospective Vendor Checklist. In it, requirements have been organized into broad categories to include:

- Host/network data leakage protection and encryption (how the product functions)
- Management and support (how the product can be managed)
- Company profile and pricing (how viable the vendor is, what services it offers, and product pricing)

This checklist can be sent to prospective vendors, and can be used in combination with our interactive Data Protection Requirements Worksheets to calculate ratings and compare vendors.

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
1	**Data Leakage Protection**			
1.1	**Discovery, Retention, Searching for Data at Rest (on end points, servers, file shares), In Use and In Motion (on the network over email and in Web traffic, being copied onto external devices, etc.)**			
1.1.1	**Discovery:** Ability to discover unmarked or unknown data			
	Marks, indexes, and securely retains:			
	Unfiltered data analyzed by network sensors			
	Unfiltered files that have been analyzed from end points and servers			
	Unfiltered files analyzed from Wiki, FTP and Web servers			
	Documents sent over unfiltered traffic			
1.1.2	**Retention**			
	Registration (fingerprinting a repository's files)			
	Provide inventory (i.e., full listing of files, fingerprinted or not)			
1.1.3	**Search**			
	Search based on specified time periods			
	Search for indexed content based on:			
	Keywords, expressions, content patterns, document type (Word, Excel, CAD, etc.)			
	Hash functions (i.e., MD5 hash)			
	Location, system/device type			
	File owner, port, path, age of file			
	Actions and tools related to the operating system (e.g., clipboard, screen capture)			
	Email and email attachments, based on specified sender/recipient			
	Applications, including Web applications Other (i.e., not covered by existing rules, client defined)			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
1.2	**Monitoring, Alerting, and Enforcement**			
1.2.1	**Monitoring:** Discover, identify, correlate, analyze and log every instance of sensitive data movement or use (e.g., removal, modification, or transmission attempt) to include:			
	Host			
	Data processed within application on host			
	Application being accessed (clipboard, printscreen, others that commonly capture data)			
	Content traversing endpoint by application access (including from clipboard, printscreen)			
	Over I/O channels (bus, Bluetooth, LPT, etc.)			
	Archive tools (winzip, tar)			
	External devices (data transferred to USB drives, CDs (CD-R))			
	Network (i.e., traffic between designated IP addresses, URLs, protocols, ports)			
	By location, IP address and protocol			
	According to URL source (Web application)			
	Identify protocols and applications operating on nonstandard ports (port agnostic)			
	Analyze SSL traffic (through proxies)			
	Analyze email traffic passing through Mail Transfer Agent			
	Save and index data for forensics, investigations and audit			
	Establish routine/scheduled scans for violations based on rules and policies			
	Identify/detect content using regular expressions, keywords, hash functions and pattern matching			
	Self-learning: Able to detect unclassified/untagged data and add to policies			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
1.2.2	**Alerting:** Define and implement actions to be taken when a violation or incident is detected based on the content (markers/registration), context (how data is behaving), application, user and location			
	Use historic information in DLP platform to tune alerting rules on the fly			
	Monitor tagged content for violations from management console			
	Alert end-user/administrator re: preventative actions			
	Alert end-user/administrator with customizable popup re: policy violation			
	Suppress end-user alerting/notification of violation in monitoring egress points			
	Remember past scan details so that new scans don't have to scan entire repository of data at rest			
	Support common notification formats (e.g., email, SMS, logs, SNMP)			
	Able to apply alerting rules to previously unclassified/untagged data			
1.2.3	**Enforcement:** Define and implement actions (i.e., allow, block, reject, quarantine, encrypt, drop, delete) to be taken for enforcement when a violation or incident is detected based on content (markers/registration), context (how data is behaving), application, user and location			
	Sensitive files during discovery: encrypt, quarantine, delete			
	Data in SMTP traffic: allow, block, reject, quarantine, encrypt			
	Sensitive data in Web traffic: allow, block, encrypt, drop attachment			
	Data over Wi-Fi: allow, block, quarantine, encrypt			
	PDF image writers: block, allow			
	Allow, encrypt, block based on:			
	Registered content and type of content			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
	Device or media being used			
	Data functions on mobile devices and phones (email, text messaging, etc.)			
	Enforce policies at endpoint and/or device:			
	While endpoint is disconnected from protected network			
	Block encrypted content from leaving endpoint (to prevent insiders from using unsanctioned encryption)			
	Encrypt sensitive files when copied to removable storage or network shares			
	Enforce policy specific to mobile devices and smartphones (i.e., encrypt to, remote shut down, secure wipe, etc. in case of lost device)			
	Permit rule/policy override by authorized administrator based on user justification			
	Allow administrative discretion over user-initiated data protection enforcement actions, such as encryption			
	Able to apply rules to previously unclassified/ untagged data			
1.3	**Forensics/Investigation**			
1.3.1	Capture event data with appropriate metadata (date/time, user, protocol)			
1.3.2	Store and index captured event data for search "after the fact"			
1.3.3	Large-scale storage capability such as SAN to hold metadata and raw data for investigators and regulators			
1.3.4	Provide chain of custody support			
1.3.5	Established partnerships with third-party forensics tools providers			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
1.4	**External Device Control**			
1.4.1	Define and implement controls on external device use by endpoint agent			
1.4.2	Allow/disallow device use by endpoint agent			
1.4.3	Encrypt data copying onto device			
1.4.4	Block copying of encrypted data onto device (to thwart misuse of encryption to conceal documents)			
1.4.4	Disable external devices based on type of data being copied (content-aware disabling)			
1.4.5	Disable external devices outright			
1.5	**DLP Rules Support**			
1.5.1	**Business/Regulation Support**			
	Compliance-specific policies (HIPAA, SARB-OX, PCI DSS, state/federal/international – Please state)			
	International compliance regulations (Please state)			
	International language document support (Please state)			
1.5.2	**Rules Creation, Extension, and Management**			
	Wide variety of flexible rules based on standard policies			
	Ability to easily create custom policies through cloning an existing policy			
	Tuning and testing of rules using historical information in DLP system			
	Rules exceptions easily tuned on the fly to reduce false positives			
	Signatures for sensitive documents can be uploaded through a Web interface			
	Ability to define and automate remediation actions based on policy violation			
	Flexible syntax to tie data to specific applications, file servers, network shares, printers, and unique content patterns			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
	Device rules to specify external devices like USB drives, with a large variety of unique identifiers			
	Rules centrally managed and deployed through a single console			
	Associates sensitive data through tagging rules			
	END DATA LEAKAGE PROTECTION			
2	**Encryption**			
2.1	**General**			
2.1.1	Maintains persistent encryption for data at rest and in use including:			
	Email (including attachments)			
	Files/folders with granular policy management for file, system and users			
	Full disk encryption			
	On client system pagefile (i.e., automatic)			
	Offline files			
	Mobile devices (Symbian, Windows Mobile, range of devices and versions)			
2.2	**Algorithms, Keys, Certificates**			
2.2.1	Supports FIPS 140-1/140-2 algorithms (AES, RC5)			
2.2.2	Supports strong key lengths (256-bit and up)			
2.2.3	Common Criteria Certification Level of EAL2 – EAL4			
2.2.4	Options of certificates, token and smart cards to protect keys (available for pre-boot and Windows)			
	Supports standards including ISO 7816-4 smart card scripting language			
2.3	**Key Management and Recovery**			
2.3.1	Centralized management for encryption policies and keys			
2.3.2	No superuser administrative key to unlock all data for separation of duties; original key required to decrypt			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
2.3.3	No storage of keys in plaintext at the server side			
2.3.4	Client-side key generation on PC/mobile computer			
2.3.5	Client-side key generation on mobile phones			
2.3.6	Authentication required to access keys			
2.3.7	Keys available when offline			
2.3.8	Temporary reset option for those who lose passwords, smart cards or tokens			
2.3.9	Secure recovery of lost/forgotten tokens, even if system is offline			
2.3.10	Encryption of all key transfer communication			
2.3.11	Retrieval of critical user data from client in case of system damage			
2.3.12	System repair possible without decrypting hard drive			
2.3.13	Creation of "recovery admins" with no additional privileges (Help Desk/Support, etc.)			
2.3.14	Maintenance of encrypted state even after sudden power loss			
2.4	**Encryption Management**			
2.4.1	Centralized management for encryption policies, keys, recovery and administration			
2.4.2	Management support for file, folder and full disk encryption			
2.4.3	Flexible policy development and update processes			
2.4.4	Rules can be set based on document types and file types			
2.4.5	Rules can be set based on user and group			
2.4.6	Administrator can state a UNC path on the device/ device group to auto encrypt by policy			
2.4.7	Default blocking of users from changing an applied encryption policy			
2.4.8	Variety of administrator notification options (email, phone, SMS messages)			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
2.4.9	Notification on specified device, even in sleep/ suspend mode			
2.4.10	Configurable preauthentication screen with customized warning/instruction fields to alert users			
2.4.11	Policy synchronization "configurable over the air" for mobile devices and phones			
2.4.12	Encryption policy changes/updates automatically fetched from the clients without administrative intervention			
2.4.13	Rules can be set based on user and group			
2.4.14	Password protect and administrator control over uninstall at the client			
2.4.15	Support for multiple two-factor authentication types like smart cards and hardware tokens, as well as certificates			
	END ENCRYPTION			
3	**Management and Support**			
3.1	**Implementation, Deployment, and Management**			
3.1.1	Supports centralized deployment, administration, management, and reporting for DLP and encryption			
3.1.2	Manages all security products (e.g., software, appliances) from one administration console (regardless of vendor)			
	Deploys agent using common software methods like GPO, SMS, etc.			
	Supports foreign language for client and administrator software			
	Encrypts software updates			
3.1.3	Provides intuitive and easy installation, setup, deployment, population of policies, and ongoing support for:			
	DLP and encryption rules "out-of-the-box"			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
	Creation of encryption installation packages for clients that support a variety of installation options (e.g., removable media, centralized console, SMS, other software distribution tools)			
	Creation of user/system specific policies			
	Custom authentication methods			
	Multiple deployment options			
3.1.4	Documentation that's useful and easy to follow			
3.2	**Administrative Access (Rule- and Role-Based Access)**			
3.2.1	Individual account for each named administrator (required by regulators)			
3.2.2	Worfklow engine that supports business process owners (non IT) requiring access to their data			
3.2.3	Configuration and management of multiple administrative roles, each role being assigned specific permissions and access according to business unit (e.g., branch or department), machine groups, etc.			
3.2.5	Separation of duties by assigning specific roles for different administrators (e.g., "encryption admins" responsible for key management, "user and machine admins" responsible for user/group and machine administration)			
3.2.6	Administrator accounts with similar security settings as client accounts (passwords, timeouts, tokens, etc.)			
3.3	**Rule and Policy Development/Management (General)**			
3.3.1	Provides central management across data protection and encryption policies			
3.3.2	Presents intuitive interface for customizing rules and policies (e.g., Will it require vendor services? Does it require learning a complex, proprietary scripting language?)			
3.3.3	Allows dynamic, real-time tuning of rules and policies			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
3.3.4	Provides hierarchical management of rules, including higher-level groupings that map to business objectives			
3.3.5	Allows powerful rule construction, using keywords and/or regular expressions in standard Boolean logic			
3.3.6	Allows reuse existing rules to construct new rules and templates			
3.3.7	Allows detection of non-textual elements such as binary fingerprints or image color patterns			
3.3.8	Supports granular application and device control			
3.3.9	Allows disabling of system ports			
3.3.10	Allows definition of what applications are trusted/ untrusted and granting them their associated rights			
3.4	**Incident Workflow**			
3.4.1	Allows investigation of incidents involving data at rest, data in use, and data in motion from within a centralized management console			
3.4.2	Allows definition and establishment of specific workflows (i.e., add all three event types to cases), assigns cases to individual users/owners, allows users to document cases (e.g., notes), and document management			
3.4.3	Supports monitoring and management of critical aspects and phases of each incident/case until resolution, involving specified authorized administrators and role-specific users as required throughout the process			
3.4.4	Creation of cases (i.e., groups of incidents) and population into management system			
3.4.5	User dashboard provides information to guide user in remediation of discovered problem			
3.4.6	Classifies incidents/cases into user-defined categories			
3.4.7	Assigns incidents/cases to users for data at rest, in use, and in motion			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
3.4.8	Provides security and access controls around case/ incident (user and group)			
3.5	**Reporting, Auditing, and Compliance**			
3.5.1	Central monitoring for all HDLP, NDLP, and Encryption alerts from within management console			
3.5.2	"Dashboard" presentation that provides immediate visibility into data at rest, data in use and data in motion violations broken down by severity, types of event, etc.			
3.5.3	Ability to tailor dashboard presentation to client needs			
3.5.4	Ability to launch individual components from central management console			
3.5.5	Variety of standard reports that can be tailored for client needs			
3.5.6	Support of development of ad-hoc (i.e., custom) reports			
3.5.7	Availability of all reports from within a single management console			
3.5.8	Ability to meet all regulatory requirements that apply			
3.5.9	Flexibility in determining what events to log			
3.5.10	Ability to log all boot and logon events			
3.5.11	Central logging			
3.5.12	Ability to secure logs against tampering			
3.5.13	Availability of logs in numerous export formats to suit audit purposes			
3.6	**Identity Management**			
3.6.1	Integration with user identity repositories and/or user management at the repository:			
	Active Directory			
	Novell			
	LDAP			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
3.7	**Performance**			
3.7.1	Reasonable size of deployment package (i.e., less than user-specified size)			
3.7.2	Less than 5% impact on CPU/memory for encryption/decryption process			
3.7.3	Solid, proven recoverability that includes recovery from crashes during encryption/decryption process			
3.7.4	Reliable network throughput without dropping packets or affecting traffic sampling			
3.7.5	Minimal impact to network/system resources when performing endpoint- or network-based discovery tasks			
3.7.6	Optimized rule tuning to help shorten required time to deploy and tune policies			
3.7.7	Seamless enforcement of policies and policy updates in the background			
	Integration with Existing/Planned Infrastructure			
	Supports current O/S for servers and clients			
3.8	Windows 2000, XP, Vista (32/64 bit), and Windows Server 2003			
3.8.1	Mac OS X/Linux			
	Mobile clients (Windows Mobile, Symbian, other)			
	Allows integration with other security monitoring tools through extensible architecture			
	Integrates with network services/technical infrastructure			
3.8.2	Directory services (e.g., Active Directory) to block sensitive content leakage			
3.8.3	MTA (e.g., Exchange) to block sensitive content leakage			
	DHCP for incident correlation			
	Policy update via TCP/IP in a "firewall friendly" manner on configurable ports (applies to endpoint encryption for PC agents)			
	Supports configuration options for other standard products			
	END MANAGEMENT AND SUPPORT			

Prospective Vendor Checklist

SECTION	DATA PROTECTION REQUIREMENTS	MEETS? YES	MEETS? NO	COMMENTS
4	**Company Profile and Pricing**			
4.1	**Company Profile**			
4.1.1	Comparable/compatible customer base			
4.1.2	Comprehensive technology partnerships (relevance to larger frameworks as well as smaller individual points)			
4.1.3	Sound financial standing			
4.1.4	Market direction of company aligned with client technology roadmap			
4.1.5	Track record of adapting to market critical requirements			
4.1.6	Established value and approach			
4.2	**Maintenance and Support**			
4.2.1	Breadth of professional services (e.g., training, installation, configuration)			
4.2.2	Software upgrade policy (maintenance only, maintenance and major releases)			
4.2.3	Web-enabled access to upgrades and patches			
4.2.4	Breadth of support services (on-site, helpdesk for end-users)			
4.2.5	Accessible knowledge base			
	SCORE SUBTOTAL: MAINTENANCE AND SUPPORT			
4.3	**Pricing**			
4.3.1	Pricing model (per user, group, device)			
4.3.2	Value add (integration, manageability, etc.)			
	END COMPANY PROFILE AND PRICING			

About the Author

Barbara Filkins has done extensive work in system procurement, vendor selection and vendor negotiations in her career as a systems engineering and infrastructure design consultant. Based in Southern California, she sees security as a process that she calls "policy, process, platforms, pipes, AND people." Most recently she has been involved with HIPAA security issues in the health and human services industry. She has clients ranging from federal agencies (DoD and VA) to municipalities and commercial businesses. Her interest in information security comes from its impact on all aspects of the system lifecycle as well as its relation to many of the issues faced by modern society that are dependent on automation—privacy, identity theft, exposure to fraud, and the legal aspects of enforcing information security. She holds the SANS GSEC (Gold), GCIH (Silver, working towards Gold), and GHSC certifications.

SANS would like to thank this paper's sponsor