エンドポイントで PCIデータを自動識別、PCI DSSに準拠した制御を提供

デジタルガーディアン株式会社
坂橋　晃司

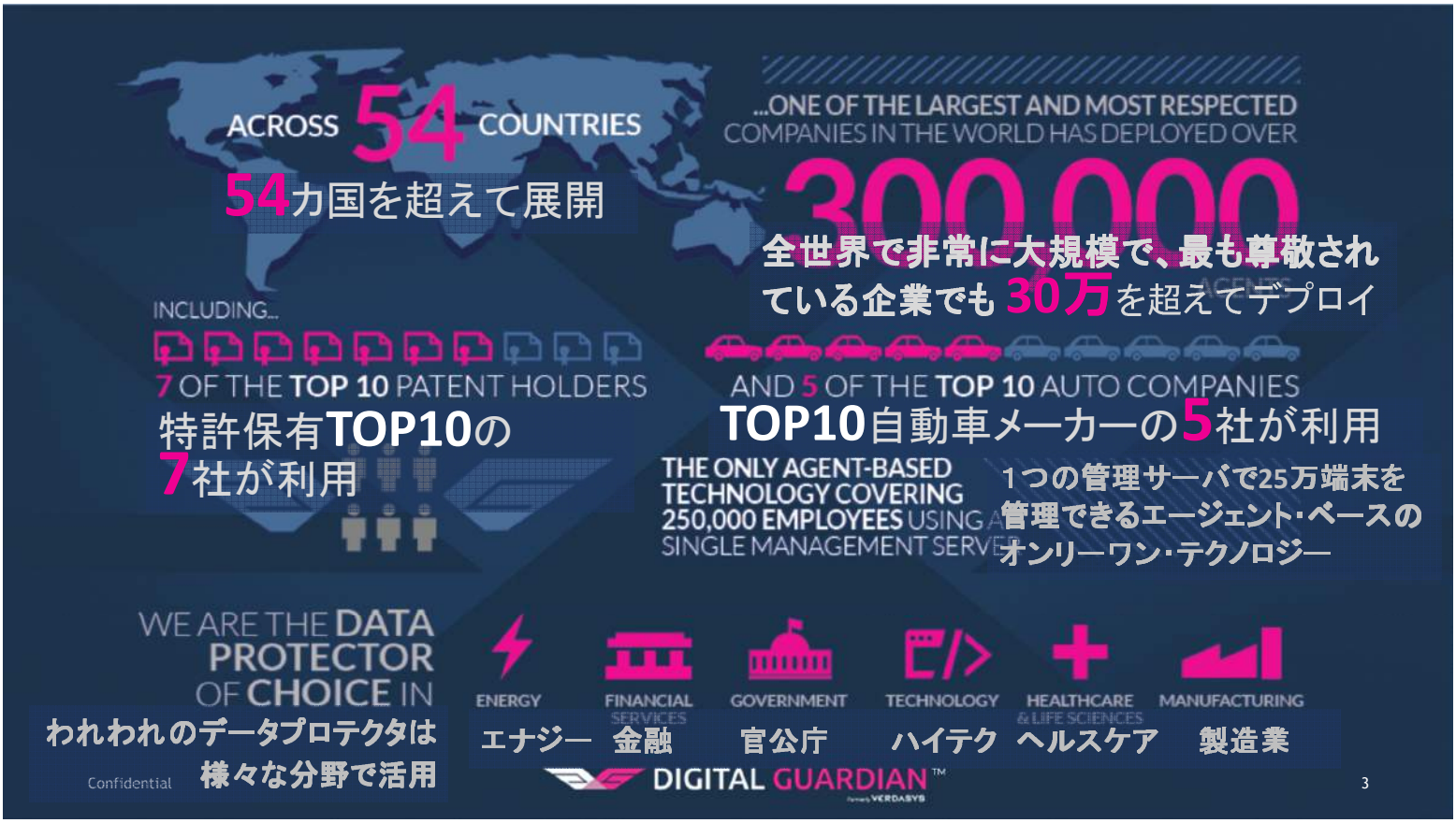
2015年7月28日

デジタルガーディアン

- 機密データ保護や情報漏洩対策のパイオニア
  - データ・セキュリティに特化したエンドポイント・ソフトウェア・ベンダー
  - Intellectual Property（知財）保護で高い評価
- ETDR（Endpoint Threat Detection & Response）のリーダー
- 設立：2003年（2006年、日本進出）
- 本社：Boston, MA
  - 他拠点：London、東京、他グローバルサポート体制（50カ国以上）
- 導入実績：250社+
- テクノロジー・パートナー：VDI、シンクライアント、SIEM、次世代ファイアウォールなど

SECURITY'S CHANGE AGENT DIGITAL GUARDIAN by VERDASYS

Gartner Magic Quadrant Leader



導入事例

当日後紹介します。

PCI DSS 3.0 概要とDG対応表

PCI DSS 3.0 安全なネットワークとシステムの構築と維持		Digital Guardian 対応状況
要件1	カード会員データを保護するために、ファイアウォールをインストールして維持する	-
要件2	システムパスワードおよびその他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない	-
カード会員データの保護		
要件3	保存されるカード会員データを保護する	◎
要件4	オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する	◎
脆弱性管理プログラムの維持		
要件5	すべてのシステムをマルウェアから保護し、ウィルス対策ソフトウェアまたはプログラムを定期的に更新する	◎
要件6	安全性の高いシステムとアプリケーションを開発し、保守する	-
強力なアクセス制御手法の導入		
要件7	カード会員データへのアクセスを、業務上必要な範囲内に制限する	○
要件8	システムコンポーネントへのアクセスを識別・認証する	-
要件9	カード会員データへの物理アクセスを制限する	○
ネットワークの定期的な監視およびテスト		
要件10	ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する	◎
要件11	セキュリティシステムおよびプロセスを定期的にテストする	-
情報セキュリティポリシーの維持		
要件12	すべての担当者の情報セキュリティに対応するポリシーを維持する	◎

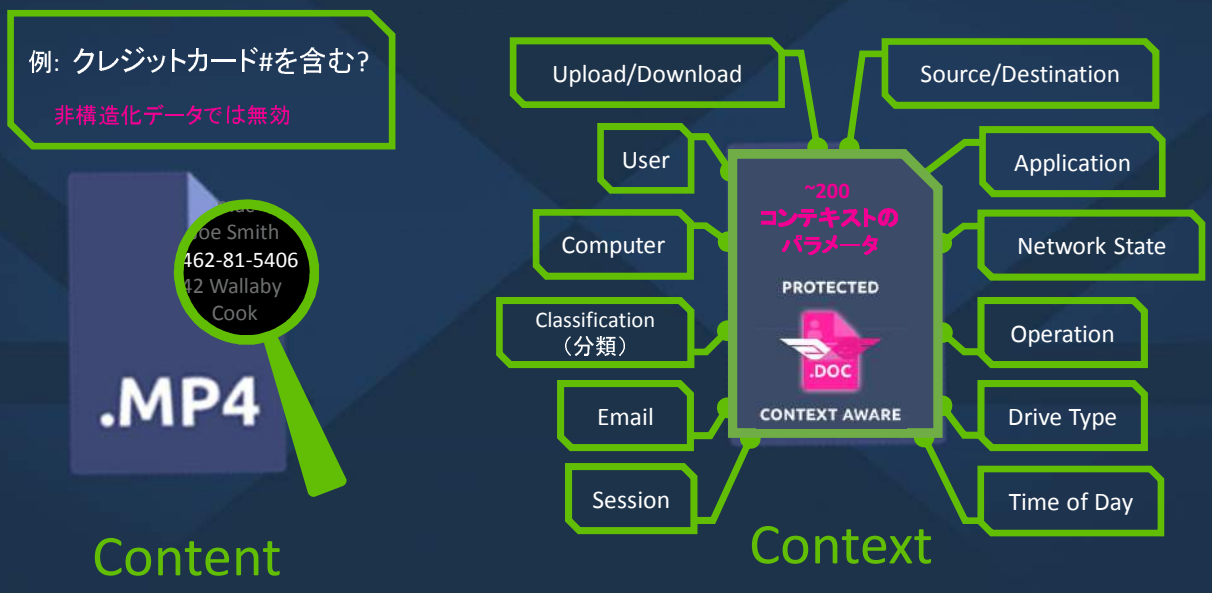
要件３の提唱

- **要件3: 保存されるカード会員データを保護する**
  1) カード会員情報データの検知および分類
  2) カード会員データのみ自動的にタグ付けして、漏洩に繋がる行為を常時監視し、社外へ出るような際に制御（警告、ブロック、暗号化など）する。

（例１） カード情報が入ったファイルをコピー、移動、ファイル名/拡張子変更、印刷、プリントスクリーンの行為を監視（ログ収集）し、その行為をブロックする。

（例２）1ファイルにカード情報が、5件以上入っていれば、警告のみ
〃 、50件以上入ってれば、暗号化
〃 、100件以上入っていれば、ブロック

データ自動分類する方法



データ自動分類

- 散在するデータの中からクレジットカード番号が入ったファイルを見付けて、タグ付け分類

1) **Context Classification**（**コンテキスト・クラシフィケーション**）：ファイル属性やメタデータ
   - ファイル拡張子　Ex) pdf, xls(x), doc(x)
   - ファイル・パス（ロケーション）　Ex) \\nas\開発\GL_A
   - ファイル名　Ex)社外秘_経理_2014.xlsx, confidential_finance.xlsx
   - ファイル容量　Ex)10MB以上

2) **Content Classification**（**コンテント・クラシフィケーション**）：ファイル内のテキストなどコンテンツ
   - キーワード　Ex) ファイル内のテキストに「社外秘」, “confidential”
   - 正規表現　Ex) 桁数：\d{10}|\d{11}→10桁or11桁の数字を検索（電話番号）
   - 辞書　Ex) 登録されているナンバー：SSN, CC#（Visa, Mastercard）など

タグとは？

- 「タグ」とは、ファイルに対して
そのファイルが保有するADS
（Alternate Data Streams：
代替データストリーム）領域
に任意で付けられる文字列

ADS領域を特殊なツールで閲覧した画面

Classification	
Classification	500
Rule IDs	{28911EBB-7229-48A7-BCC8-85A5B753D8FE} (partnerId=0) {B31B4229-1C3D-4C0D-A664-C6799421D8EE} (partnerId=0)
Policy IDs	{7081E4C4-56DF-478B-8FAA-562A760B8EE0} (partnerId=0) {18DDD82A-DEE0-4527-9B6B-32E955C5D651} (partnerId=0)
Policy Tags	フォルダー (partnerId=0) 社外秘 (partnerId=0) ← タグ

- タグそのものに機能*1はなく、コントロール・ルールでタグ付けされたファイルを制御管理
  - 1つのタグに複数のコントロール・ルールを適用可能
- 一旦、付いたタグは移動先がNTFS（ファイルシステム）であれば、移動後も継承される*2

*1 厳密には、ファイルの一部でもコピーなどした際にも継承される「Permanentタグ」と継承されない「Temporaryタグ」の2種類ある。
*2 但し、エキストポート先が、FATなどNTFS以外のファイルシステムの場合、タグは外れます。また、メールで添付、WinZIP以外でアーカイブしてZIP化した場合、その他フォークをサポートしないプログラムでUploadした場合、タグは外れる可能性があります。

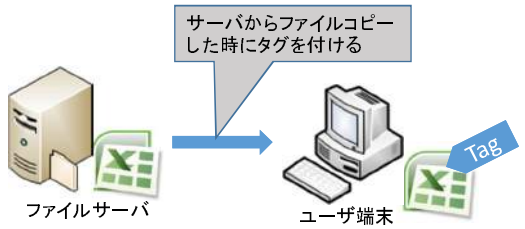
タグを付けるタイミング

- タイミングは2種類

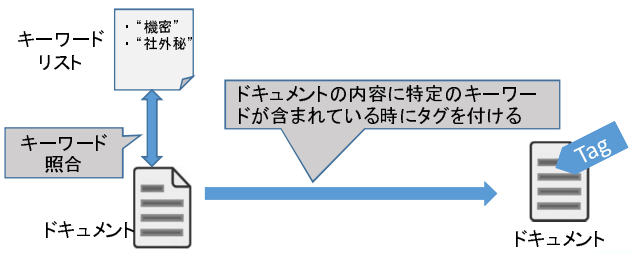
1) **Data-In-Motion（ファイル操作時）**：
   - タグを付けるべきファイル属性や、キーワードなどの条件をクラシフィケーション・ルールで定義し、各端末にポリシーとして適用する。ユーザが、ファイル操作を行った時点（data-in-motion）で、クラシフィケーション ルールに該当するファイルであればのそのルールのタグが付けられる。

2) **Data-At-Rest（静止ファイル）**：
   - ユーザが何も操作を行わなていないファイル（data-at-rest）が、DG Scannerによってクラシフィケーション ルールが定義する条件にあてはまるかどうかの評価を受ける。クラシフィケーション ルールに該当するファイルなら、そのルールのタグが付けられる。
   - 基本、DG Scannerは、決められた時刻に自動実行される。
   - スケジュールされた時刻に対象となる端末の電源が入っていないなどして、一定期間DG Scannerが実行されなかった場合、電源が入った時に自動的に実行する設定や、アイドル状態に実行させる設定などがある。

ファイルのコンテキスト（属性）情報による分類



ファイルのテキスト内容による分類



要件４の提唱

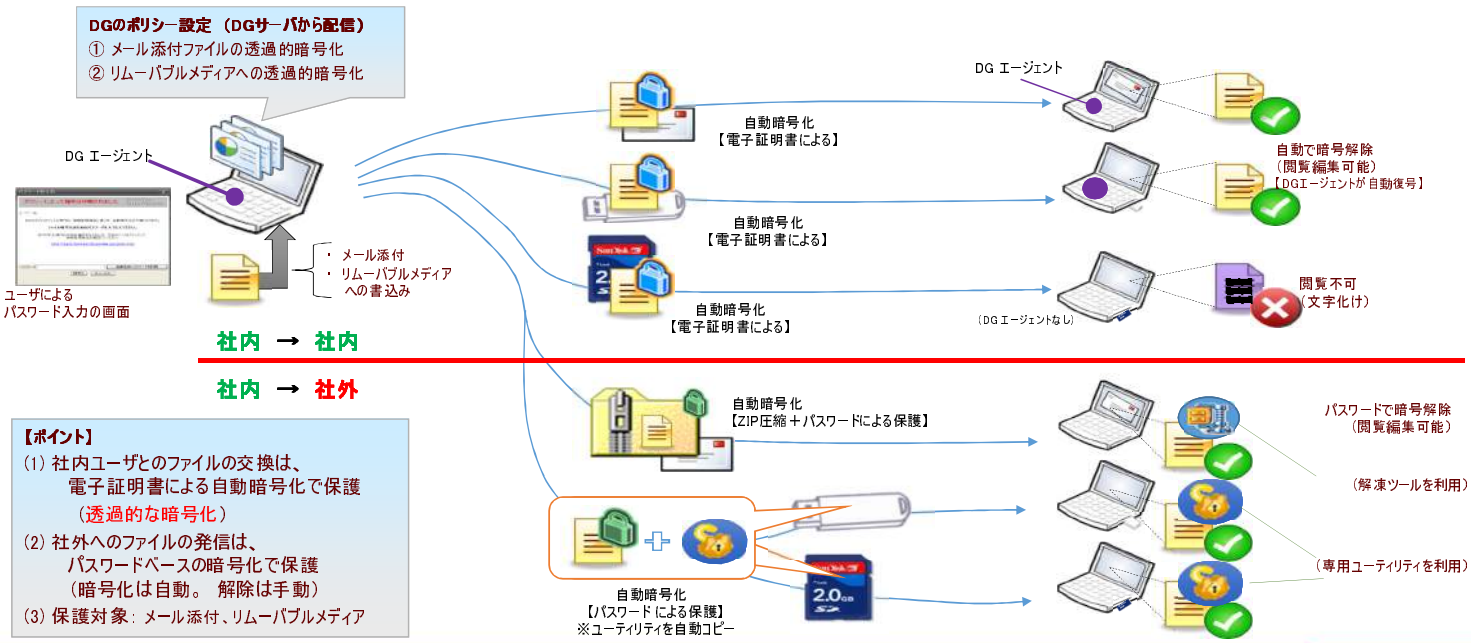
- **要件4:オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する**

  - カード会員情報の入ったファイルをメールする際には、すべて暗号化
    ➔AFE（Adaptive File Encryption）機能
  - カード会員情報の入ったファイルをアップロードさせない。

  または、暗号化されていないファイルはアップロードできなくする。

  ＊外部記憶装置や外部メディアへ書き出し、コピー、移動も当然暗号化すべき

活用シーン



活用シーンの事例

- **社内ユーザ間での情報流通**:
  - ① XLSX形式のメール添付ファイルは自動暗号化する。
    ファイルを開くには、DGエージェントが動作している端末でなくてはならない。DGエージェントで保護されていない端末ではファイルを開くことができない。**【監査の徹底、情報の保護】**
  - ② XLSX, PPTX, PDF 形式のメール添付ファイルは、ユーザに警告画面を表示(TO, CC, BCCを自動識別)する。
    ユーザがパスワードを入力し「暗号化」ボタンを押すと、添付ファイルは自動で暗号化され、メールが送信される。
    警告画面で送信を「キャンセル」することも可能。**【セキュリティ意識の向上、教育・啓蒙効果】**
  - ③ USBメモリなどのリムーバブルメディアにファイルを書き込むと、自動で暗号化する。
    社外にUSBメモリを持ち出しても、DGエージェントがインストールされていないのでファイルを開くことができない。
    【情報保護の徹底と、ビジネス継続性の維持】
- **社外ユーザへのメール発信**:
  - ① メール添付の場合、XLSX, PPTX形式の添付ファイルを添付して送信する時に警告を表示する。
    パスワードを入力すると、自動的に添付ファイルをZIP圧縮＋パスワード保護で暗号化する。
    【監査の徹底、情報の保護】
  - ② USBメモリを利用する場合、PDF形式のファイルをUSBメモリなどのリムーバブルメディアにコピーすると、パスワードベースで自動暗号化する。同時に、復号用のユーティリティもコピーされるので、これを利用して、社外ユーザはファイルを開くことができる。ユーティリティを利用すると、ファイルを閉じる際に、再度、暗号化されるので、USBメモリ上では常に情報は暗号化される。**【情報の保護】**

要件５の提唱

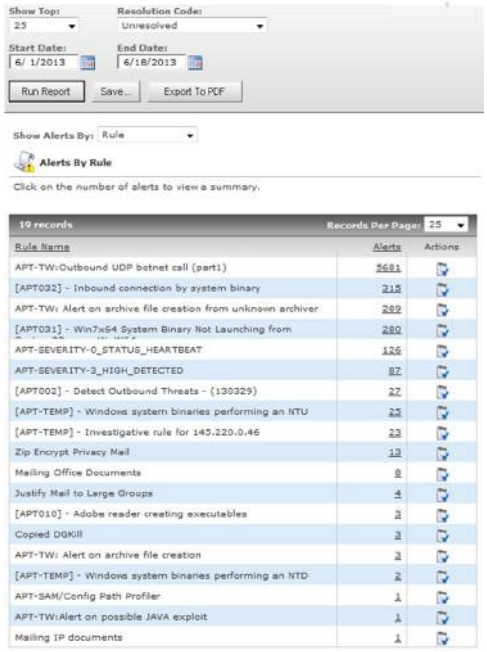
- すべてのシステムをマルウェアから保護し、ウィルス対策ソフトウェアまたはプログラムを定期的に更新する
  - 既知のマルウェアは、NWセキュリティおよびA/Vソフトウェアで随時更新
  - 未知のマルウェアは、次世代FWおよびエンドポイントで振る舞い検知

➔ATP(Advanced Threat Protection)機能

未知のマルウェアの検知

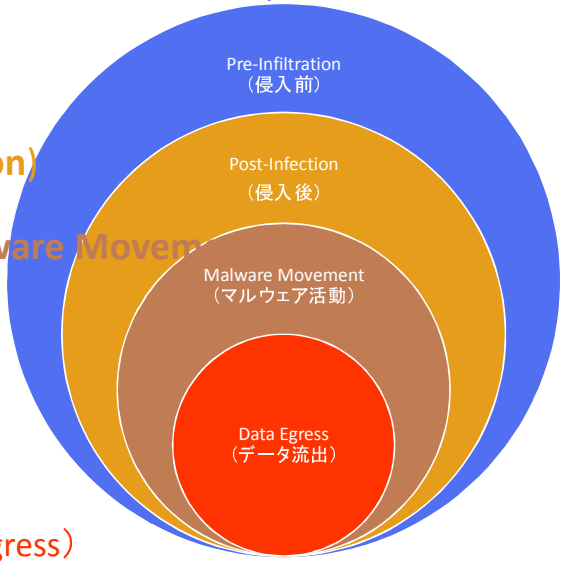
- マルウェア特有の典型的な振る舞いを追跡して検知
  - **サイバーパック・(外部攻撃対策用)ポリシー**に基づいて、マルウェア特有の振る舞いを追跡しながら、それらサイバー攻撃の一連の活動として有機的に結びつけ、特定・検知する
    ➔**振る舞い追跡検知型**
  - 例えば・・・今までに一度も起動したことがない(未知の)アプリケーションが起動し、大量のデータを分割しながらアーカイブ化する。それらの分割ファイルを定期的に外部(中国や取引のない国などのIPアドレス)へ繰り返し送信する一連の振る舞い

シグネチャーベースではないので未知の攻撃も検知。
出張中などオフラインでもポリシーが有効



多層防御のサイバー・パック・ポリシー

- 侵入フェーズでマルウェアを特定or検知 (右図: **Pre-Infiltration**)
  - OS (Windows XP/7/8)
  - アプリケーション
    - Adobe Reader, Office 2007/2010, Browser
  - その他: Java, add-onツール
- 侵入後にマルウェアを特定or検知 (**Post-Infection**)
  - 許可されていないまたは異常なプロセスや子プロセス
- マルウェア侵入拡大の動きの特定or検知 (**Malware Movem**
  - マルウェア内部拡散
    - バックドア開設、ポートスキャン、脆弱性の発見など
    - 他エンドポイントへの感染行為
    - 機密データの収集
  - ピボットポイント – 再度外部から攻撃できるようにしておく
  - 統合されたと分業を組み合わせる
    - 機密データの検索と閲覧およびコピーなど
    - 機密データのアーカイブ化
- 機密データが流出する動きを検知または阻止(Data Egress)



簡略化したサイバーパックポリシーの例

- javaが許可されていないリソースやオブジェクトをダウンロードする際に警告または阻止 App
- 未知の実行ファイル形式を検知および実行制限 App Sys
- 外部へ許可されていないコミュニケーションを警告または遮断 NW
- 子プロセスとして実行ファイルやスクリプトを作成すると警告または阻止 Sys App
- 未知のアプリケーションによるファイル暗号化を検知または制限 App
- データを.rar/.zipなどのファイル圧縮形式でアーカイブ化するのを警告または制限 App Sys
- 許可されていないチャネルからネットワーク経由のデータ送信をブロック NW

App Sys NW または、これらの組み合わせから構成されているが、
お客様のネットワークやシステム構成およびセキュリティ・ポリシーに応じて、
カスタマイズとチューニングすることにより最適な検知と防御を実現します。

サイバーパック・ポリシー 例1

Critical, High, Medium, Low, Informational

[APT001] - Outbound connection by system binary and filtered bad list
ホワイトリストにない、および危険リストの外部ネットワークへの接続を監視
[APT002] - Adobe Acrobat or Reader spawning processes
Adobe AcrobatやReaderが、許可された子プロセス以外のプロセスを起動したら違反
[APT003] - Dynamic DNS Sites
リストアップされているダイナミックDNSサービスを使うサイトに接続したら違反
[APT004] - Hosts file modification
Hostsファイルへの書き込みがあったら違反
[APT005] - Alert on autorun.ini write at root directory
ファイル名、”autorun.ini”がルートディレクトリーに書き込まれたら警告
[APT006] - Process bypassing DNS and filtered known bad
URLのIPアドレスにDNSを迂回してアウトバウンドのセッションを開くと違反
[APT007] - LSASS not child process of WININIT
LSASSがwininit.exe以外のプロセスからオープンされると違反
[APT008] - Outbound connection by rundll32
Windowsシステムリソース、”rundll32.exe”がアウトバウンドのネットワークを張ったら違反
[APT009] - Outbound TCP connection by system binary
Windowsシステムリソースが、アウトバウンドのネットワークに接続を行ったら違反
[APT010] - Adobe reader creating executables
Adobe製品がスクリプトや実行ファイルを作成すると違反
[APT011] - MS Office Processes Creating Executables
MSOffice製品がスクリプトや実行ファイルを作成すると違反
[APT012] - Svchost.exe child process NOT from services.exe
Services.exe以外のプロセスがsvchost.exeを作成すると違反

サイバーパック・ポリシー 例2

Critical, High, Medium, Low, Informational

[APT013] -Alert on Archive creation from unknown archiver
ホワイトリスト化されたアーカイブツール以外でファイルアーカイブされたら警告
[APT014] -Alert on Archive from unknown archiver with sensitive data
ホワイトリスト化されたアーカイブツール以外で、重要ファイルがアーカイブされたら警告
[APT015] -Alert on multipart rar creation or access
分割されたrarファイルの作成の場合、警告
[APT016] -Alert on multipart rar creation from unknown archiver
不明なアーカイブツールが分割されたrarファイルを作成した場合、警告
[APT017] -Alert on multipart rar from unknown archiver with sensitive data
不明なアーカイブツールが重要ファイルに対して分割rarファイルを作成した場合、警告
[APT018] -Alert on JAVA usage from unauthorized site
javaが許可されていないリソースやオブジェクトをダウンロードすると警告

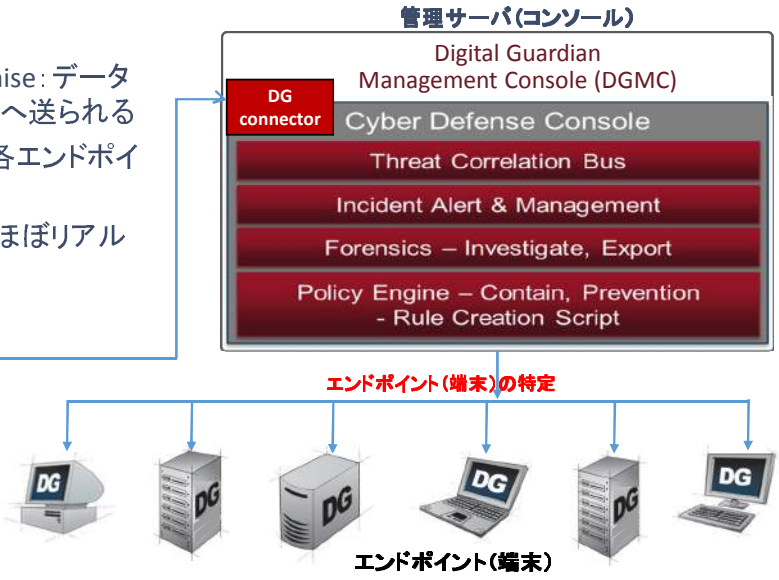
[APT019] - Suspicious outbound UDP call
不明なアウトバウンドのUDPコールを行うと違反
[APT020] - Suspicious outbound UDP threshold trigger
閾値を超える不明なアウトバウンドのUDPコールを行うと違反
[APT021] - Inbound connection by system binary
ブラックリスト化されたリモートアドレスからローカルのプロセスへインバウンドにコールバック接続すると違反
[APT022] - Outbound HTTP connection by system binary
特定のディレクトリーやシステムバイナリーから、任意のプロセスがHTTP接続を行うと違反
[APT-TEST23] - Process launch from root directory
プロセスがルートディレクトリから実行されると違反

最新の多層防御

- 次世代FWとの連携で検知

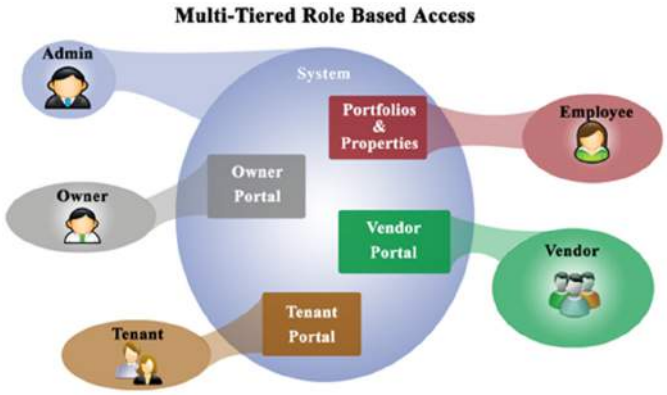
1. 各ネットワーク装置からIOC(Indicator Of Compromise：データ侵害の脅威/インジケータ)がDGMC（管理サーバ）へ送られる
2. DGMCは、それをルールに変換して追加登録し、各エンドポイント（端末）へポリシーとして配信
3. 捕捉したIOCがどのエンドポイントに到達したかをほぼリアルタイムに特定または検知

IOCs:
- App name / MD5
- Domain Name / IP
- URL
- Registry



要件７と９の提唱

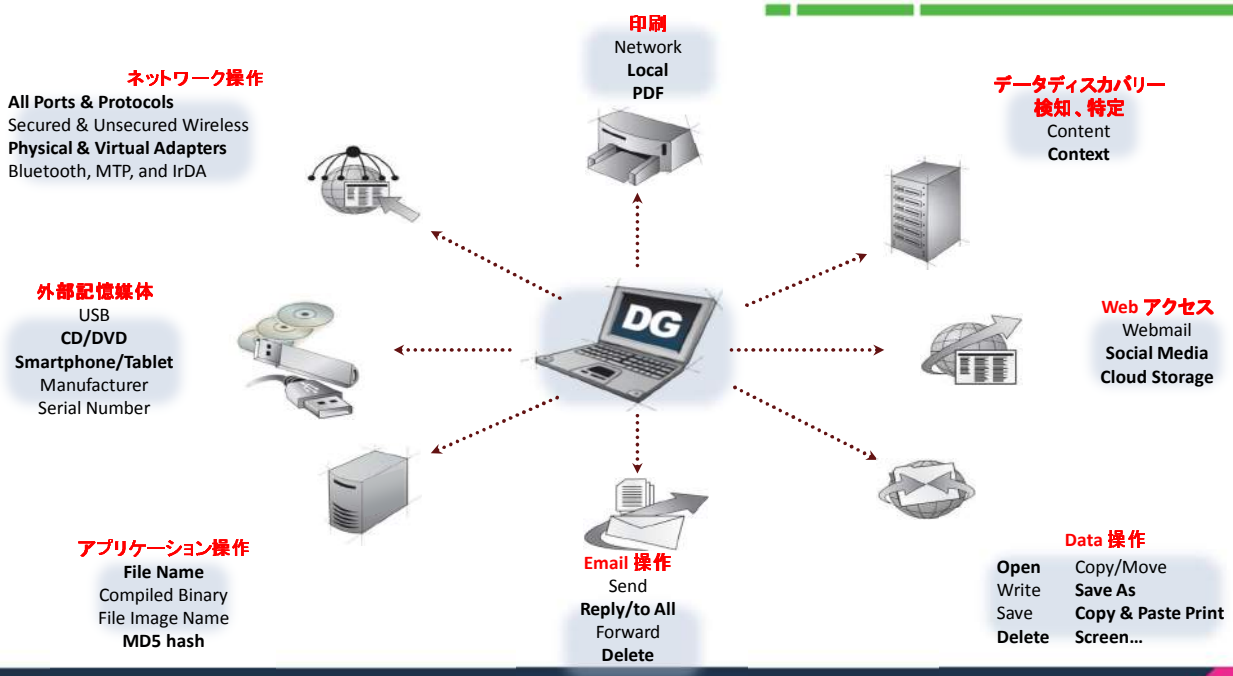
- 要件7：カード会員データへのアクセスを、業務上必要な範囲内に制限する
- 要件9：カード会員データへの物理アクセスを制限する
  - Active Directoryと連携して、アクセス権を有さないユーザには、データにアクセスさせない。



要件１０の提唱

- ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する
  - ログ収集（フォレンジック）
    - ネットワーク
    - エンドポイント
  - リスク評価、傾向分析

エンドポイント（端末）の可視化



エンドポイントにおける収集可能なログ一覧

	データ操作（日本語）	Eng	補足説明/description
1	ADE スクリーンキャプチャ	ADE Screen Capture	Windowsのクリップボードを使った操作
2	ADE プリントスクリーン	ADE Print Screen	Windowsのクリップボードを使った操作
3	ADE プリントプロセス	ADE Print Process	Windowsのクリップボードを使った操作 アクティブになっているウィンドウのスクリーンショット。(Alt+Prt Scrn)
4	ADE 新規オブジェクト挿入	ADE Insert New Object	Windowsのクリップボードを使った操作 まだ保存されていないオブジェクトのOLE挿入
5	ADE 新規ファイル挿入	ADE Insert File	Windowsのクリップボードを使った操作 保存されているファイルのOLE挿入
6	ADE 切り取り	ADE Cut	Windowsのクリップボードを使った操作 ファイル本文の一部の切り取り(Ctr+XやCtrl+C)
7	データ交換	Application Data Exchange	Windowsのクリップボードを介してコンテンツをドラッグ＆ドロップ。 Windowsのバッファを使った操作全般で上記1～7を含む
8	CD/DVD焼き付け	CD/DVD Burn	
9	デバイス 追加	Device Added	
10	デバイス検出	Device Detected	
11	デバイス削除	Device Removed	
12	デバイス所在 不明	Device Missing	端末が起動された時に端末に接続されていたデバイスが確認できなくなったときに記録
13	ネットワークからダウンロード	Network Transfer Download	ダウンロード元と先の両方
14	ネットワークへアップロード	Network Transfer Upload	アップロード元と先の両方
15	ネットワーク操作	Network Operation	TCPおよびUDPによるネットワーク操作
16	ファイルアーカイブ	File Archive	
17	ファイルオープン	File Open	通常のファイルオープンではなく、システムやアプリケーションがファイルを開く操作
18	ファイルクローズ	File Close	
19	ファイルコピー	File Copy	ファイル丸ごとコピー
20	ファイルリサイクル	File Recycle	ごみ箱にファイルをいれたときに記録(Del)
21	ファイルリストア	File Restore	ごみ箱からファイルを元に戻した時に記録
22	ファイルリネーム	File Rename	拡張子やファイル名の変更
23	ファイル移動	File Move	
24	ファイル解読(復号)	File Decrypt	Windows Exploreで、DGによって暗号化されたファイルを手動で復号化したときに記録
25	ファイル作成	File Create	
26	ファイル削除	File Delete	ファイルシステムからファイルが削除されたときに記録(Shift+Del)。ファイルリサイクルではない+D51。
27	ファイル書き込み	File Write	
28	ファイル読込	File Read	
29	ファイル表示	File View	
30	ファイル編集	File Edit	ファイルが開かれる、読み込まれる、書き込まれる、最終変更時刻が変更される、上書き保存を含むイベント
31	メール送信	Send Mail	Webメールはネットワーク操作(13)
32	メール添付	Attach Mail	Webメールはネットワーク操作(13)
33	ログオフ	User Logoff	
34	ログオン	User Logon	
35	印刷	Print	
36	文書リポジトリ	Document Repository	ドキュメタムの操作
37	名前を付けて保存	File Save As	

総合的なログを相関分析してシステム全体を可視化

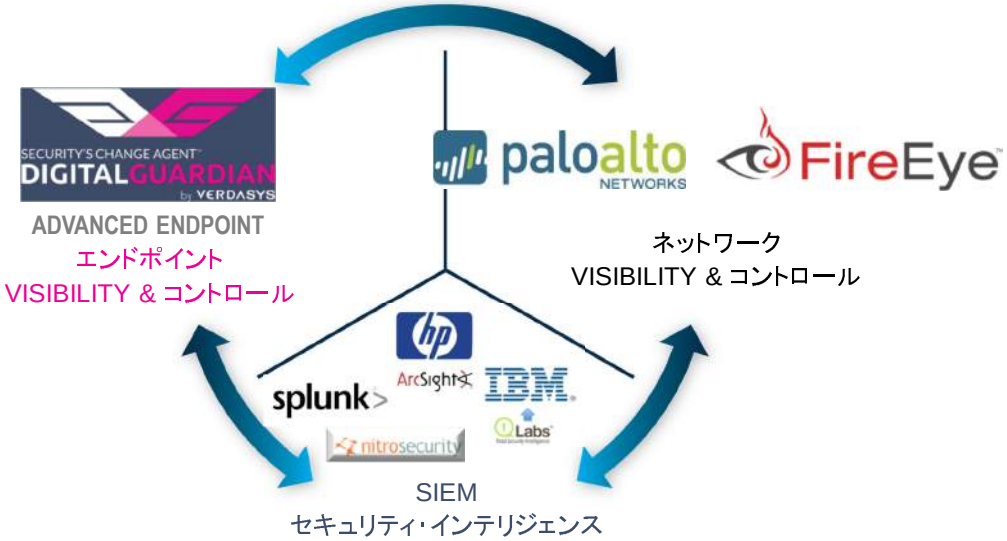
エンドポイントおよび コンテキスト
Data Usage, Application & System Events, User & Malware Behavior

ネットワークおよびセキュリティ・アプライアンス
LDAP, IPS/IDS, Vulnerability Mgmt., OS, DB, URL filtering, WAF and Application logs. 外部脅威のData

(SIEM) Security Information and Event Management

エンドポイントとネットワークの総合的なログを相関分析して全体像を把握

次世代セキュリティ・エコシステム



ADVANCED ENDPOINT
エンドポイント
VISIBILITY & コントロール

ネットワーク
VISIBILITY & コントロール

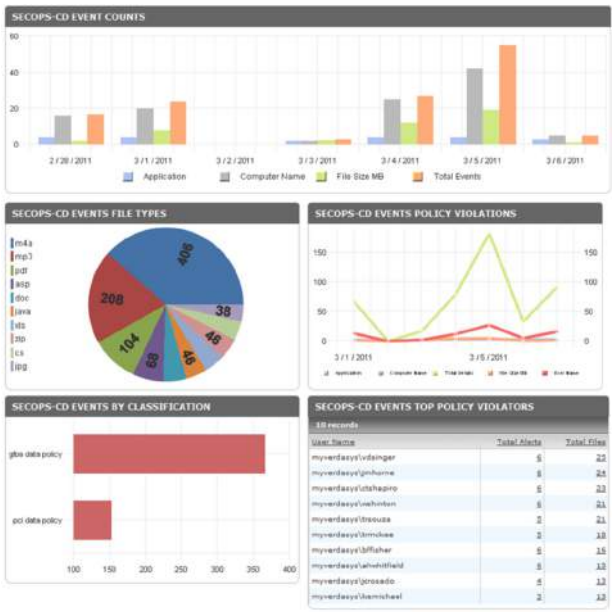
SIEM
セキュリティ・インテリジェンス

要件１２の提唱

- すべての担当者の情報セキュリティに対応するポリシーを維持する
  - 拠点・事業所/部門/部署/課などに応じて、セキュリティ・ポリシーを適用し、運用管理する

➔ADとの連携、フェデレーション、ダイナミック・グループで任意のグループを作成し、細かい貴社固有の業務に沿った運用ポリシーにカスタマイズ

  - MSP（マネージド・サービス）で煩雑な運用をお任せも可能



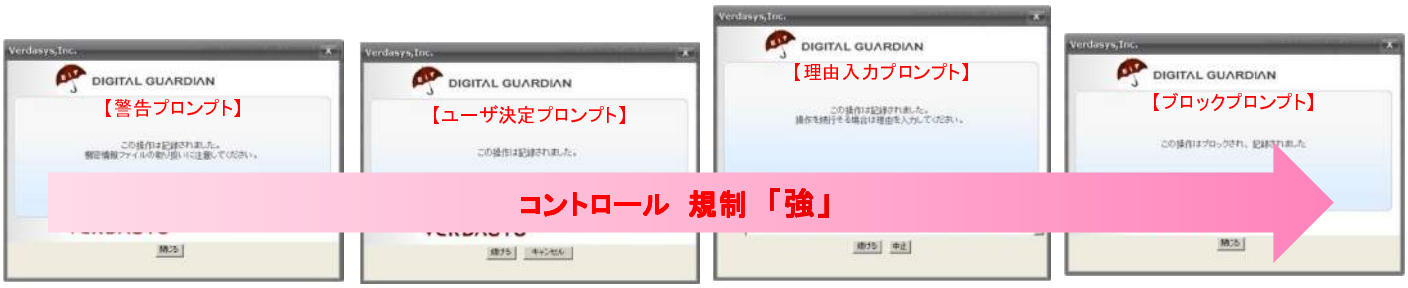
タグ付きのデータに対してポリシーを適用

何を？ What? Which data?	どういったユーザ操作やイベント？ Which operation, event and user activities? How?	いつ？ どういう時？ When ?	どこへ？ Where? From to?	誰（適用端末は）？ Whom? Which machines?	どう制御管理？ Plolicy Control how?
特定ファイル（機密ファイル） ・ファイルパス（保存場所） ・ファイル・タイプ/拡張子 ・ファイル名 ・属性情報 ファイル内のテキスト ・特定文字列や英数字 ・正規表現 上記の組み合わせ	【ファイル操作】 ・開く ・閉じる ・上書き保存 ・名前を付けて保存 ・切り取り **・コピー** **・貼り付け** **・プリントスクリーン** ・書き込み **・移動** ・削除 **・アップ/ダウンロード** ・イン/**エキスポート** 【Eメール】 **・メール添付** ・コピー＆ペースト ・新規作成 **・送受信** 【アプリケーション】 ・閲覧、修正、削除 ・イン/**エキスポート**	終日 就業時間帯 就業時間外 特定時間帯 特定曜日 休祭日 オン/オフライン 上記の組み合せ	**ローカル** **社外（WAN）** **社内（LAN）** **サーバ** **モバイルデバイス** **外部記憶メディア/装置** **・USBメモリ** **・SDカード** **・DVD/Blue lay** **プリンタ** **IPアドレス** 上記の組み合わせ	【ユーザタイプ】 ユーザ/管理者 部署・グループ 役職別 役員 本社・支店・事業所 日本法人 リージョン 協力関連会社 派遣・契約社員 子会社 【環境】 Win, Mac, Linux ネットワーク 仮想 IPアドレス 端末 Time zone 上記の組み合わせ	監視 警告 ユーザ選択 理由入力 暗号化 **ブロック** 上記の組み合わせ

これらの条件を組み合わせて、どうコントロールするか

コントロール（制御）ポリシーの種類

- どう制御管理したいか？
  - 監視（ログは取得）
  - 警告
  - 理由入力
  - 暗号化
  - ブロック（阻止）
  - または、上記の組み合わせ



上記プロンプトは、HTML形式で作成されているため、ロゴやテキストは、カスタマイズが可能です。

コンテキスト・アウェアについて

データに付随する属性およびメタデータ、ならびにデータの状態を示す関連情報、およびそれら付随する背景情報を感知・把握できるのがContext Aware（コンテキスト・アフェア）。 コンテント・アウェアはデータの内容（中身）で管理しますが、コンテキスト・アウェアは、それに加えて、下記のようなデータに付随する様々な情報や要素を考慮した管理が可能で、柔軟で厳格な運用やリスク管理ができます。

User Awareness	Point of Risk	Data Awareness	Event Awareness		Policy
Executive	Desktops	# Strings（文字列）	Network Drive	Local Drive	Monitor
Engineer	- Win	Key Words	Online storage	Copy	Block
Admin	- Linux	CAD Files	Paste	Web	Warn
Finance	- Mac	Source Code	Archive	Email	Justify（理由入力）
Contractor	Servers	Video/Images	Move	Rename	Encrypt
Supplier	Network	Customer	USB Device	Print	Allow
IT	Offline	Classification（分類）	Executable	Create	Classify
Sales	Virtual	Application	Screen Cap	CD/DVD	Contain

Digital Guardian (DG)
ソフトウェア・ソリューション

- **エージェント型エンドポイント**・ソフトウェア
- エンドポイントにおける**プロセス（データ/ユーザ操作のイベント等）**と**出口経路**（Egress points）を可視化し、単一エージェントで**内外部の脅威**から機密データを守る情報漏洩対策のプラットフォーム
- DGエージェントがインストールされた端末で、何が起こっているかを把握：
  when, who, what, how, where (from, to) ➔ Forensic（フォレンジック）

- **データ・セントリック/アウェアネス**で、機密データにタグ付け分類(Classification)し、ポリシーで一元管理

主な機能

主な機能	具体例
デバイス制御	特定のシリアルNo.のUSBデバイスだけ使用可能にする。
印刷制御	土日祝祭日や業務時間外は、社内にあるプリンタを使わせない。
ネットワーク制御	FacebookなどソーシャルメディアやDropboxなどオンラインストレージへ社内のファイルをアップロードさせない。FTP経由で機密ファイルをアップロードさせない。
アプリ制御	Skypeなどブラックリストのアプリケーションを起動させない。
データ操作制御	ソースコードの拡張子やファイル名を勝手に変更させない。
Eメール制御	マイナンバーの入った機密ファイル添付をメールに添付させない。
暗号化	CADファイルなど機密ファイルを外部記憶メディアにコピーや移動させる際には、暗号化させる。
ログ収集	セーフモードで起動した際にもログを収集する。
通知・制御	Facebookにアクセスする際には、理由を入力させる。
データ分類	クレジットカード番号が10個以上入ったファイルは、社内にあるファイルすべてに機密扱いのタグを自動的に付与する。
レポート	退職予定者が、退職するまでの期間に、機密ファイルの持ち出しやポリシー違反など異常がないかをダッシュボードで分析する。
ダイナミックグループ	ADとは別に、新入社員のグループを作成して、そのグループに厳格なポリシーを適用する。
サイバー攻撃対策	社内の各エンドポイントに未知のマルウェアに感染していないかを調べて、検知する。

デリバリー・モデル

- フレキシブルな下記3つのデプロイメント

Option 1
オンプレミス
On Premise

- 貴社の環境での展開

Infrastructure hosted in your environment

- 貴社で運用：Self-administration
- ポリシー、ルール、レポートを貴社で運用

Policies, rules and reports managed by you

- 必要であれば、弊社PSを利用

Engage with our Pro Services as needed

Option 2
マネージド・サービス
Managed Service

- 弊社のプライベート・クラウドで展開

Infrastructure hosted in our private cloud

- 弊社のPSが運用管理

Administered by our Pro Services

- ログイン画面よりポリシー、ルール、レポートの確認が可能
- Access to policies, rules, and reports
- 週1回の状況をフィードバック
- Weekly status meetings

Option 3
ハイブリッド（Option 1 + 2）
Managed Service On Premise

- 貴社の環境での展開

Infrastructure hosted in your environment.

- 弊社のPSがリモートにより運用管理

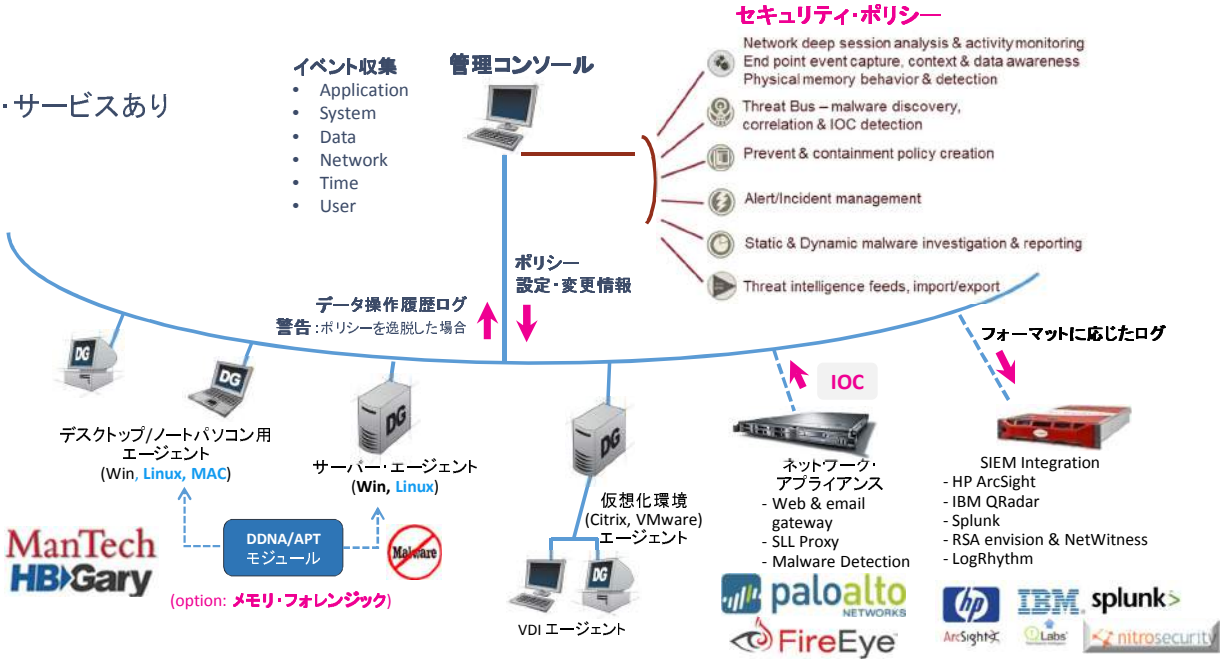
Administered remotely by our Pro Services

- ログ等のデータは貴社の環境内で保持

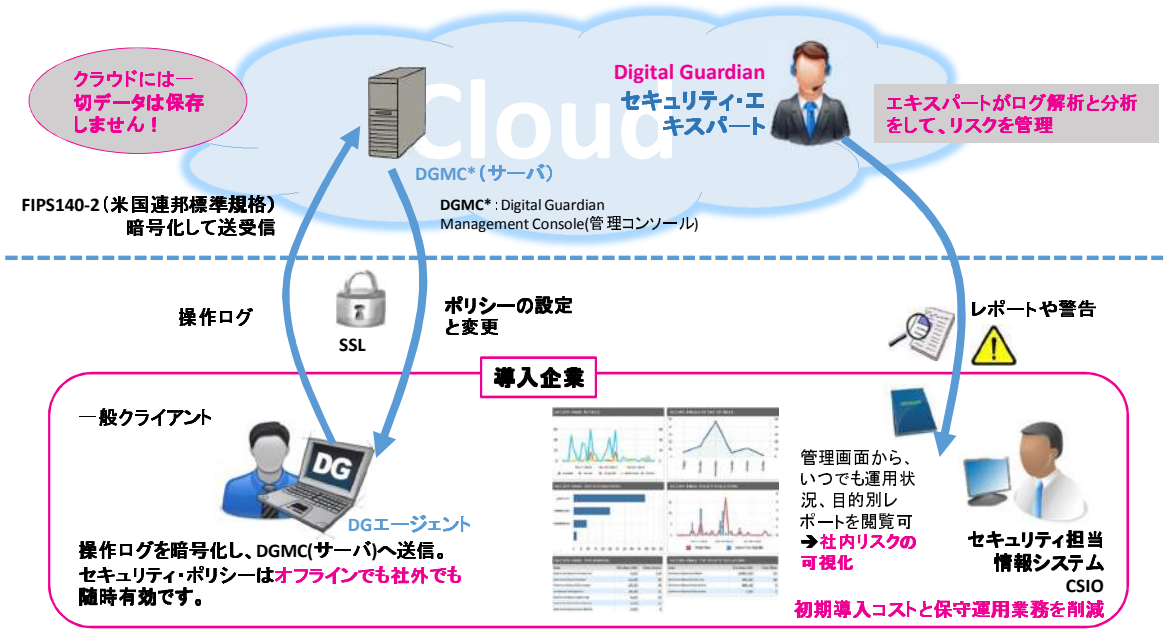
Data remains within your IT environment.

アーキテクチャ(オンプレミス)

*マネージド・サービスあり



マネージドサービス（MSP: Managed Service Program）



初期導入フェーズ

評価検証（1ヶ月）
PoC/PoV

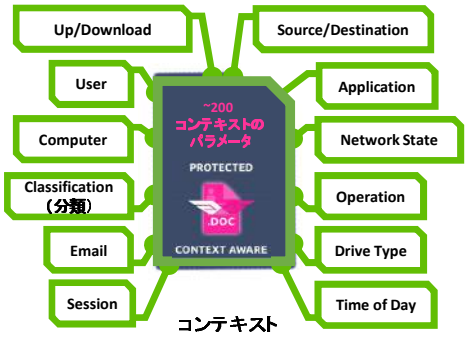
可視化（～1ヶ月）
ログ収集、正常値/異常値の蓄積

分類、リスク評価（RA）及び分析（～2週間）
データ分類、リスク分析と優先順位化

制御・管理（～2週間）
ルール作成・ポリシー配信などリスク管理

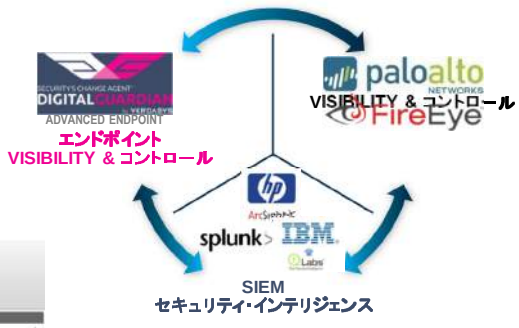
差別化のポイント

- **データ・セントリック/アウェアネス**でデータに**タグ付け分類**し、機密データの漏洩を阻止
- **状況に応じたきめ細かいリスク制御**
- **カーネル・レベル**で動くエージェントは、バックグラウンドで動くシステム系プロセスの検知やマルウェア等の怪しい挙動も制御可能➔**Context Aware** (vs. Content Aware)
- 単一エージェントで、**内部脅威および外部脅威からデータを保護**



差別化のポイント

- 次世代FW、SIEM、メモリー・フォレンジックとの連携で未知の最新脅威にも対応 ➔ **多層防御**
- 1つの管理サーバで**25万**のエージェントを管理可能
➔**スケールアウト容易**



DG Cloud ARMOR 5

クラウドサービス用セキュリティゲートウェイ。企業向けクラウドサービスを1つのゲートウェイに集約し、シームレスでセキュアなクラウド環境を提供します。

デバイスや端末環境に依存せず、クラウドサービスへのアクセスはすべてバーチャルブラウザ経由でセキュアなクラウド環境を実現。SSOにも対応

【特長】

- エージェントレスで、マルチ・デバイス/プラットフォーム
- BYODにも最適
- デプロイ(ゼロタッチ)、運用が容易

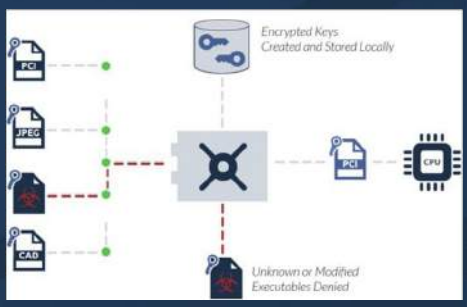
DG Application Whitelisting

savant PROTECTION

POS端末や業務用端末のアプリケーションをホワイトリスト化。既存のアンチ・マルウェア製品で検知できないゼロデイ攻撃や未知のアプリケーション起動を許さずに業務用端末をエンドポイントで守ります。

【特長】

- 暗号化されたホワイトリストをエンドポイント(端末)側で暗号化して保持
- デプロイおよび運用が容易



エージェントは、起動する正規アプリ毎に見えないキーを適用して、ホワイトリストにマッチしたキーを保持していれば、そのアプリは起動可となり、アンマッチの場合は起動させない仕組み。

BECAUSE WE'RE FOCUSED ON PROTECTING ONE THING

われわれは、1つのものだけを
プロテクトすることにフォーカスしている・・・

それは・・・

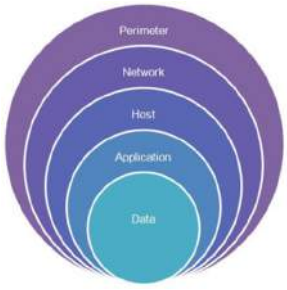
DATA

DIGITAL GUARDIAN™

Appendix 補足資料

データ・セントリック/アウェアネスとは？

- データ・セントリック・セキュリティへ
  - データそのものに着眼して、データの機密性や価値に応じてデータ中心に一元的に管理
  - データの状態（data at rest/in use/in motion)にかかわらず、あらゆる局面で**データ**を保護する
- 大切なデータを保護
  - 内部および外部脅威の攻撃ターゲットは大切な「**データそのもの**」、その大切な機密データだけを守る



データを中心に考える

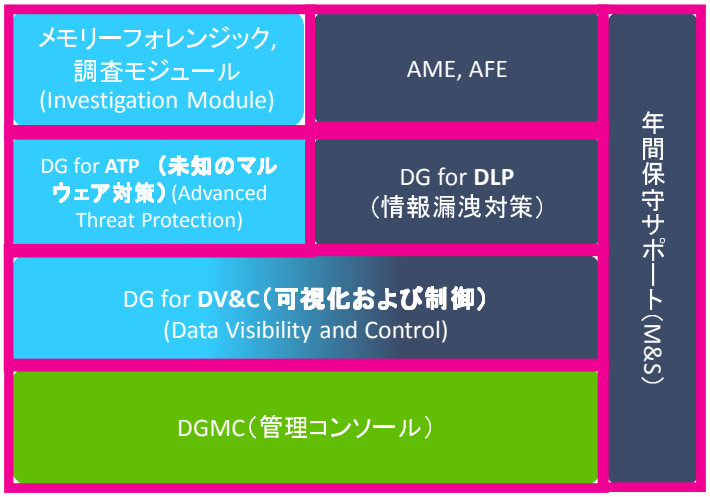
データセントリック/データアウェアネス

VS

✓**デバイスセントリック**:
ホスト機器、デバイスを守る
✓**ヒューマンセントリック**:
人（部門、職位、地位権限）に紐付いてデータのアクセス管理で守る。人に依存。
✓**ネットワークセキュリティ**:
境界線を設けてNWの内側だけ守る

プロダクト基本構成

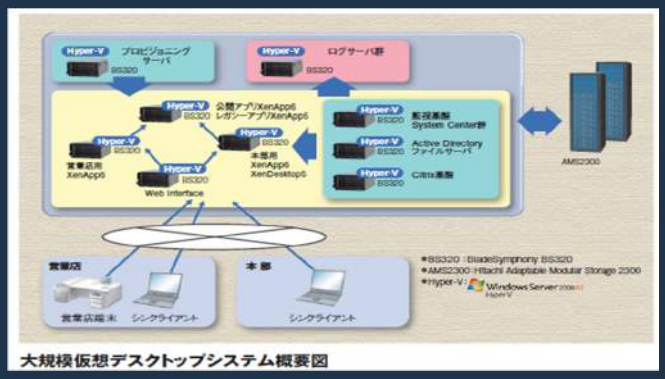
オンプレミス



MSP（マネージド・サービス）

Case Study: 金融セクター

- 導入理由（Business Drivers）
  - コンプライアンス、証跡監査
- 課題（Challenges）
  - CS向上（顧客へワンストップ・サービス提供）
  - 端末種類および数による業務遅延
- 要件・要望（Needs）
  - 全本支店端末のログ収集、監視および追跡
  - 端末およびサーバ集約
  - 新旧アプリ/システムの共存
  - 業務の迅速化
- 提案（Solution）
  - サーバ仮想化：Microsoft Hyper-V
  - 仮想デスクトップ化：Citrix XenDesktop, XenApp
  - 製品：DLP VDI（6240台），DLP Win（520台）DVC Win Server（240台），DGMC（3台）
- 結果（Result/benefit）
  - ✓ 運用コスト➔60%削減
  - ✓ OSライセンス➔50%削減
  - ✓ メンテナンス（バージョンUP等）コストの削減（TCO削減）



大規模仮想デスクトップシステム概要図