DIGITAL GUARDIAN®

次世代型データプロテクション（データ定義不要型DLP）

2018年7月11日

デジタルガーディアン 株式会社

データ保護の方法

Action
(行動)

X

Classification
（保護データ指定）

日本におけるデータ保護対策の大きな課題

- データの重要性については日本も海外も変わらない
  - 個人情報、知的財産、 CAD等

- しかし、長らく日本では：
  - 守るべきデータの定義があいまい
  - アクションのみを禁止すると業務効率が落ちてしまう

  ことが理由でデータ保護対策が海外に比べ進んでいない状況

- ところが、ここ数年で環境は激変しつつある

適切なデータ分類が重要さを増してきている背景

General
Data
Protection
Regulation

次世代型データプロテクション

①パッケージ化による重要データ自動抽出

Action
(行動)

X

Classification
（保護データ指定）

DIGITAL GUARDIAN®

②UEBA：
ユーザー/端末ベースのプロテクション

Entity
（人、PC）

UEBA
（高リスクユーザ、PC等の検出、除外）

DIGITAL GUARDIAN®

次世代型データプロテクション

Action
(行動)

Entity
（人、PC）

DIGITAL GUARDIAN®

次世代型データプロテクション

デジタルガーディアン

重要データ自動抽出

- 実データのフローから自動判断
- 各産業毎のテンプレート
- コンテンツベース：キーワード、クレジットカード番号、氏名、電話番号等
- コンテキストベース：データ生成アプリ指定、ファイルの保存先、アプリケーション等

＋

ユーザー、端末ベースプロテクション

- 「何が重要データなのかは、悪い人やPCに聞け」、というアプローチ
- リスクの高い人物、エンティティの挙動を自動判定
  - （競合他社への転職を検討している社員、マルウェアに乗っ取られたPC等）
- コンテキストベース：各エンティティの振る舞いから、ハイリスクのファイルを抽出
（重要な情報である可能性があるため、保護対象とする）

重要データ自動抽出

データ解析型
アプローチ

- 実データのフローから自動判断
- 各産業毎のテンプレート
- コンテンツベース：キーワード、クレジットカード番号、氏名、電話番号等
- コンテキストベース：データ生成アプリ指定、ファイルの保存先、アプリケーション等

重要データの自動分類、定義

これまで

1. ポリシーの作成
2. 重要データの定義
3. 重要データの分類、探索
4. 方法論の検討
5. 製品検討
6. 実行

CISO、IT部門

デジタルガーディアン

これから

1. 重要データの定義
2. 重要データの探索、分類
3. ポリシーの作成
4. 方法論の検討
5. 製品選定
6. 実行

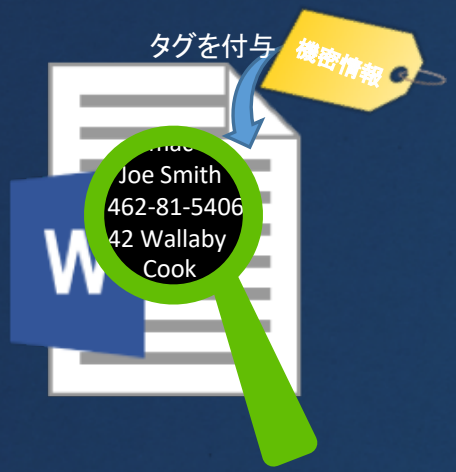
CISO、IT部門

DIGITAL GUARDIAN®

コンプライアンス型と知的財産型

コンプライアンス型分類法

1) コンテンツベース（キーワード検索）



- キーワード（正規表現含む）で定義した文字列を含むファイルを自動的に探索

知的財産型分類法

2) コンテキストベース（オペレーション駆動型）

- 重要なイベントとみなす行為が発生した場合、その行為で使用したファイルを識別
- ファイル形式には依存しない

重要データの判定例
～ 製造業 ～

- 機械メーカーのB社
  - 研究開発データや知財データをファイルサーバに集約し、ファイルサーバにあるすべてのデータを重要データとする
  - 他サーバやエンドポイント内をコンテンツベースで検索し、ファイルサーバへの集約を促す
  - 重要情報に対して、リスクがある、または、未承認のイベントをレポートとしてまとめ、部門長に毎週報告
- コンテンツベースとコンテキストベースを組み合わせて、重要データを識別

重要データの判定例
～ 部品メーカー ～

- 部品メーカーのC社
  - 研究開発データや知財データをファイルサーバに集約し、以下の条件に合致したファイルを重要データとする。
    - 特定のアプリケーションで作成したファイル
    - 特定のキーワードを含んだファイル（ファイル名を含む）
- コンテンツベースとコンテキストベースを組み合わせて、重要データを識別

重要データの判定例
～ 金融関連業 ～

- 投資管理会社D社は、コンテンツベースの重要データを識別
  - フィンガープリントや正規表現を使って、個人情報を識別
  - ユーザーが個人情報に対してリスクのある行為（例．メールに添付して外部へ送信等）を行なった場合は、リアルタイムでブロック

- コンテンツベース
  - 正規表現可能な個人情報（電話番号、クレジットカード番号等）や保持している個人情報が明確（フィンガープリントを利用）

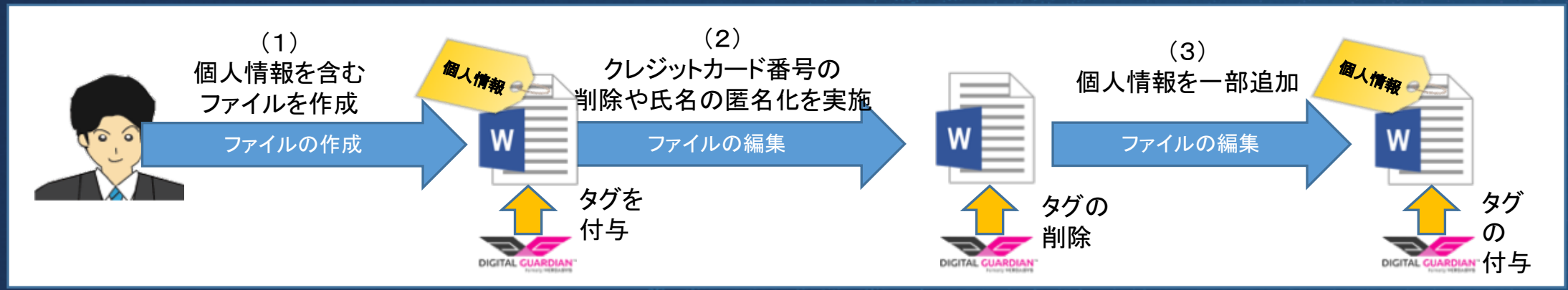
重要なのは、重要情報の判定の「正確さ」

複数の項目の組み合わせと件数で、重要情報を定義することが重要（下記は、個人情報の場合）。

No.	項目	内容
1	クレジットカード番号	正規表現＋チェックサムの検証
2	電話番号（固定及び携帯）	正規表現
3	住所	日本の全市区町村名を辞書として登録
4	氏名	日本人の姓の中で上位70%を辞書として登録（1文字の姓は除外）
5	メールアドレス	正規表現

× 件数

重要データの判定は、ファイルに対してイベント（編集、コピー等）が発生する毎に行います。

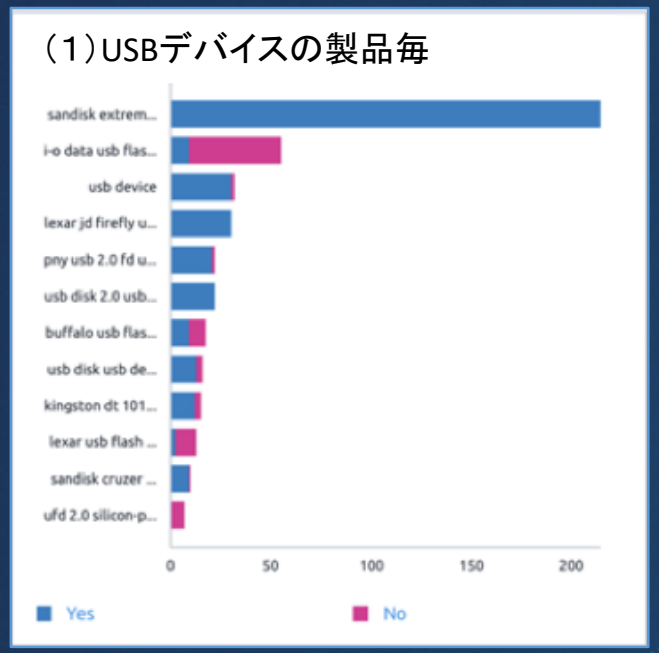


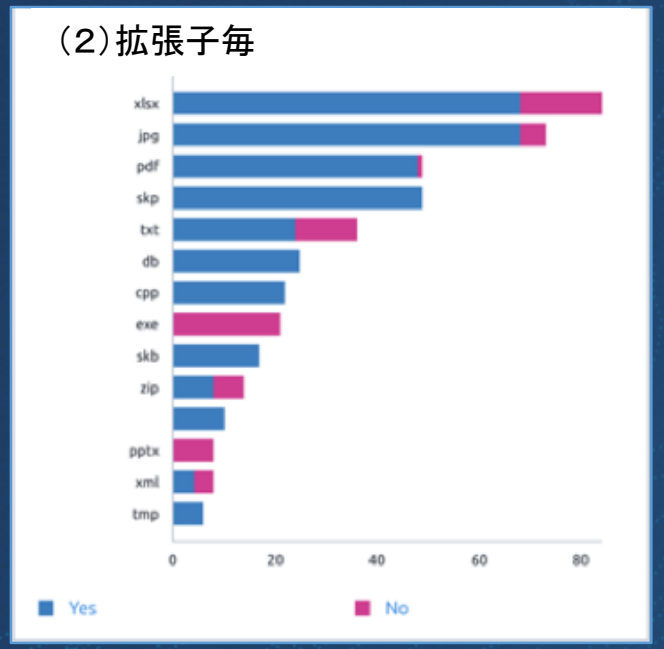
重要情報定義、分類パッケージ

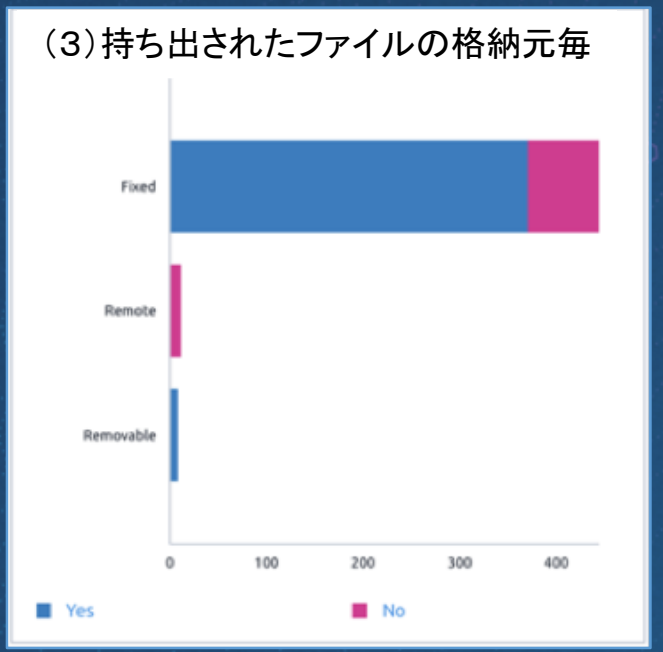
- コンテンツベース
  規制対応した個人情報定義をライブラリとして用意
  - **PCI-DSS**
  - **HIPPA**
  - **GDPR 等**
- コンテキスト
  IP（知的財産）を含む機密データ保護も業界ごとにパッケージ化可能
  （例）
  - 製造業（CADデータ）
  - リテール（個人情報）
  - 金融（信用情報）

Visibility Study」

- ファイル持ち出し状況
  - 持ち出されたファイルを様々な切り口で集計
  - 「どのようなデータが、どこへ持ち出されている」のか を特定していくための材料を提供





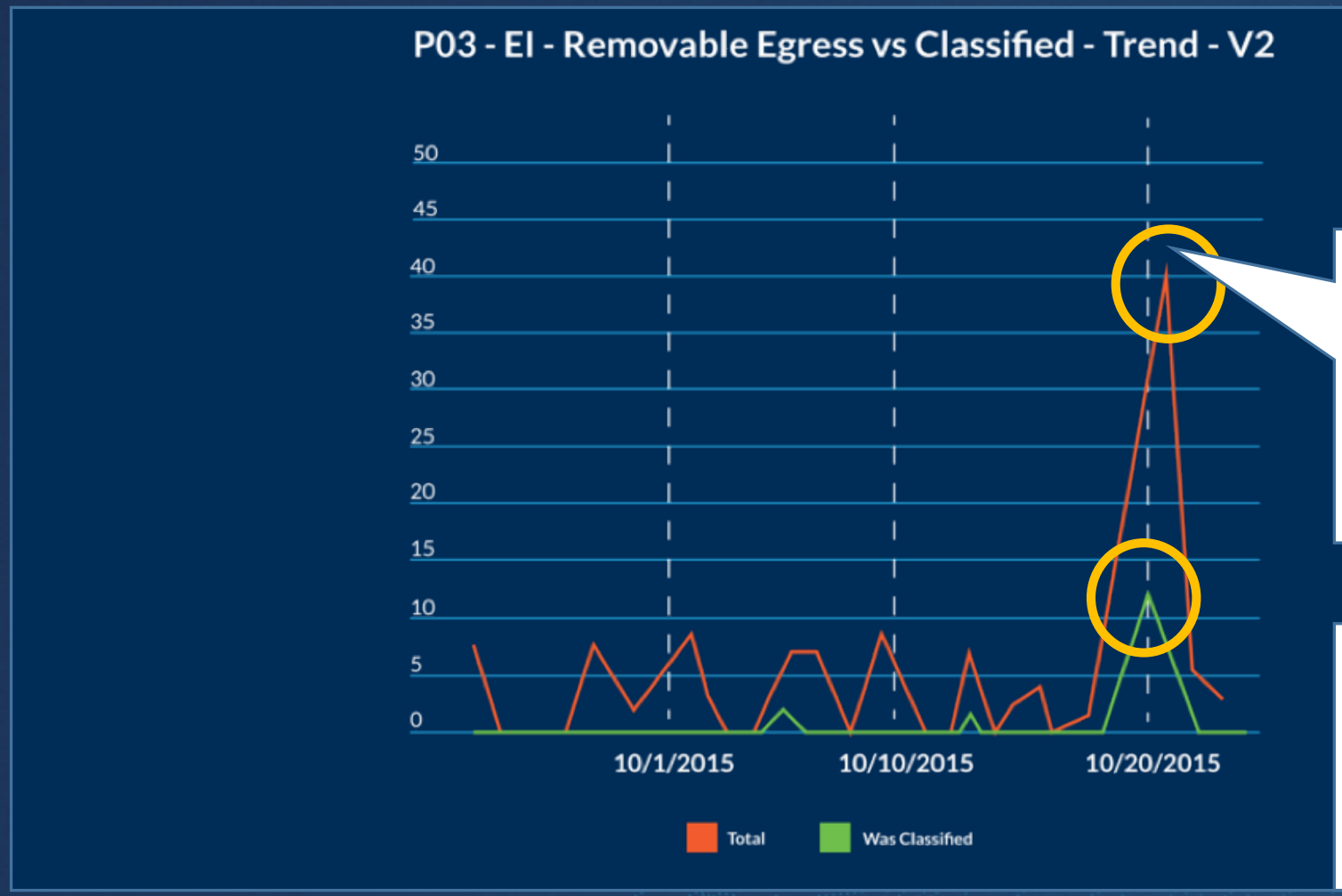


ユーザー、端末ベースプロテクション

リスク人物、端末
追跡型
アプローチ

- 「何が重要データなのかは、悪い人やPCに聞け」、というアプローチ
- リスクの高い人物、エンティティの挙動を自動判定
  - （競合他社への転職を検討している社員、マルウェアに乗っ取られたPC等）
- コンテキストベース：各エンティティの振る舞いから、ハイリスクのファイルを抽出
（重要な情報である可能性があるため、保護対象とする）

リスク行動の典型例（退職）

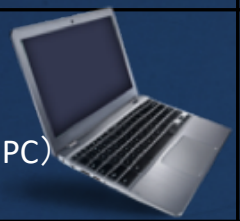
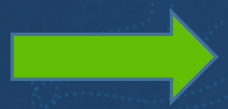


異常値

退職願を出す2週間前に、データをリムーバブルメディアへ大量にコピー

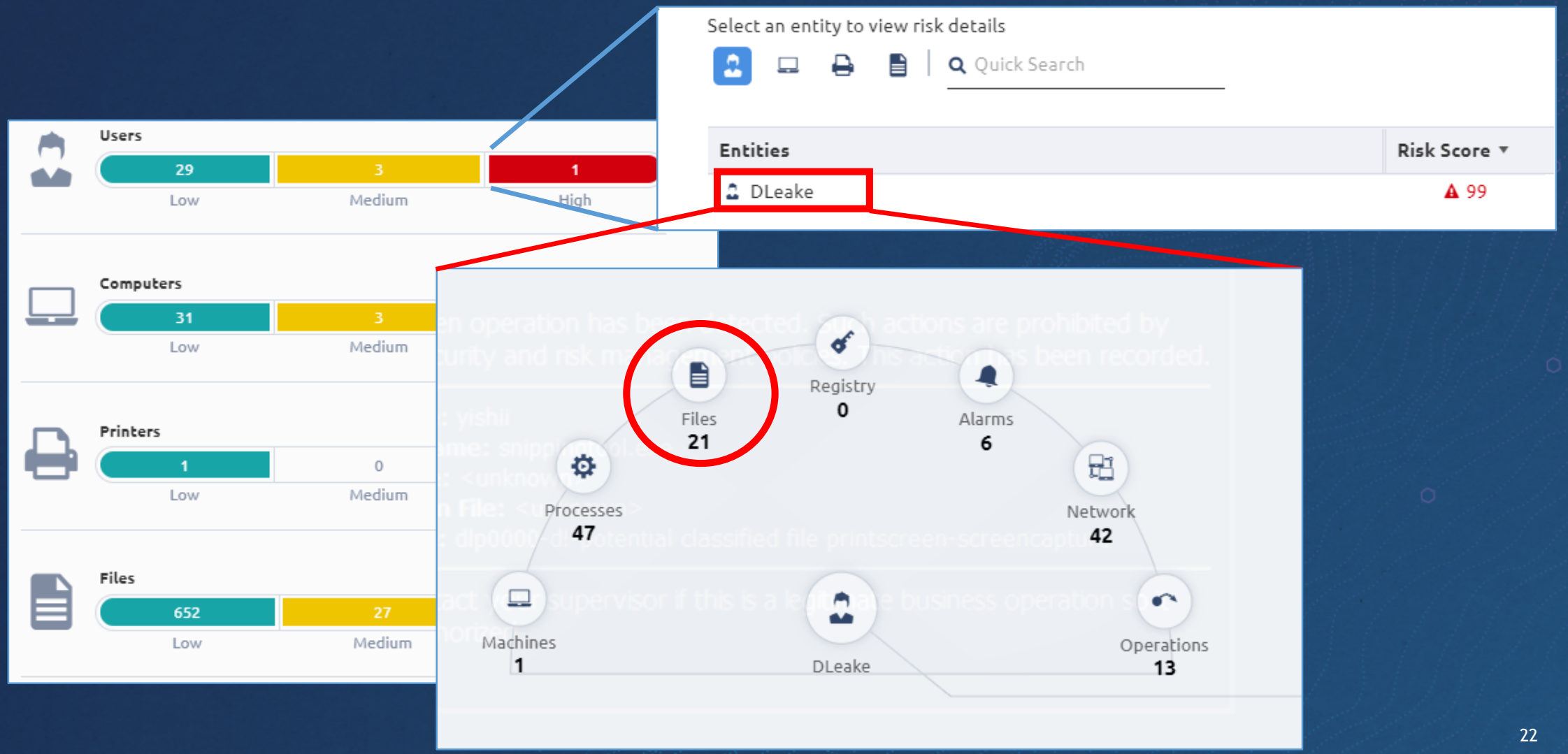
このレポートにより、退職希望者にデータを返すことを要求し、退職時のデータ漏えいを防止できた。

イベントとエンティティとリスク

エンティティ ＼ イベント	いつものファイルサーバ（JP-FileSV01）へログイン	いつもアクセスしないファイルサーバ（JP-FileSV31）へログイン	ファイルサーバ（JP-FileSV31）からファイル（新製品企画書.docx）をコピー	ファイル（新製品企画書.docx）を普段とは異なる先に保存
田中氏 				
jp-tanaka（田中氏のPC） 				
新製品企画書.docx 				

注）Inetrset社「Advanced Threat Detction With the Interset Platform」を参考に作成

リスクの高いユーザーから重要データの特定



UEBA：分析～対応自動化フロー

分析	✓ DG Endpointから送信されたイベントログを、予め定義された50以上のモデルを使って分析します。 ✓ 分析は、DG ARCが休みなく行います（24時間365日）。
検知	✓ 上記分析の結果、異常値を検知します。 ✓ イベントと各エンティティの紐付け、及び、リスクのスコアリングを行います。
優先順位付け	✓ エンティティ毎にリスクを集計します。 ✓ リスクの高い順にエンティティを並べ替えます。
対応	✓ ハイリスクと判断した根拠となるイベントをタイムラインで表示。 ✓ ここ1ヵ月間に、ハイリスクのユーザーが外部へ持ち出したデータをダッシュボードとして表示。

まとめ

- データ漏洩対策は引き続きクリティカルな検討課題
  - **GDPR**
  - 知的財産
  - 内部脅威、外部脅威
- リスク定義は今後ますます重要に
  - 企業成長を妨げない
  - 実行が容易であること
- データ解析テンプレート＋UEBAが重要データ定義の最適解
  - 正確性
  - 自動化
  - 簡素化
- デジタルガーディアン はデータプロテクションにフォーカス

DIGITAL GUARDIAN®

A New Dawn for Data Loss Prevention.

A New Day for Digital Guardian.

デジタルガーディアン 会社概要 “データプロテクション”

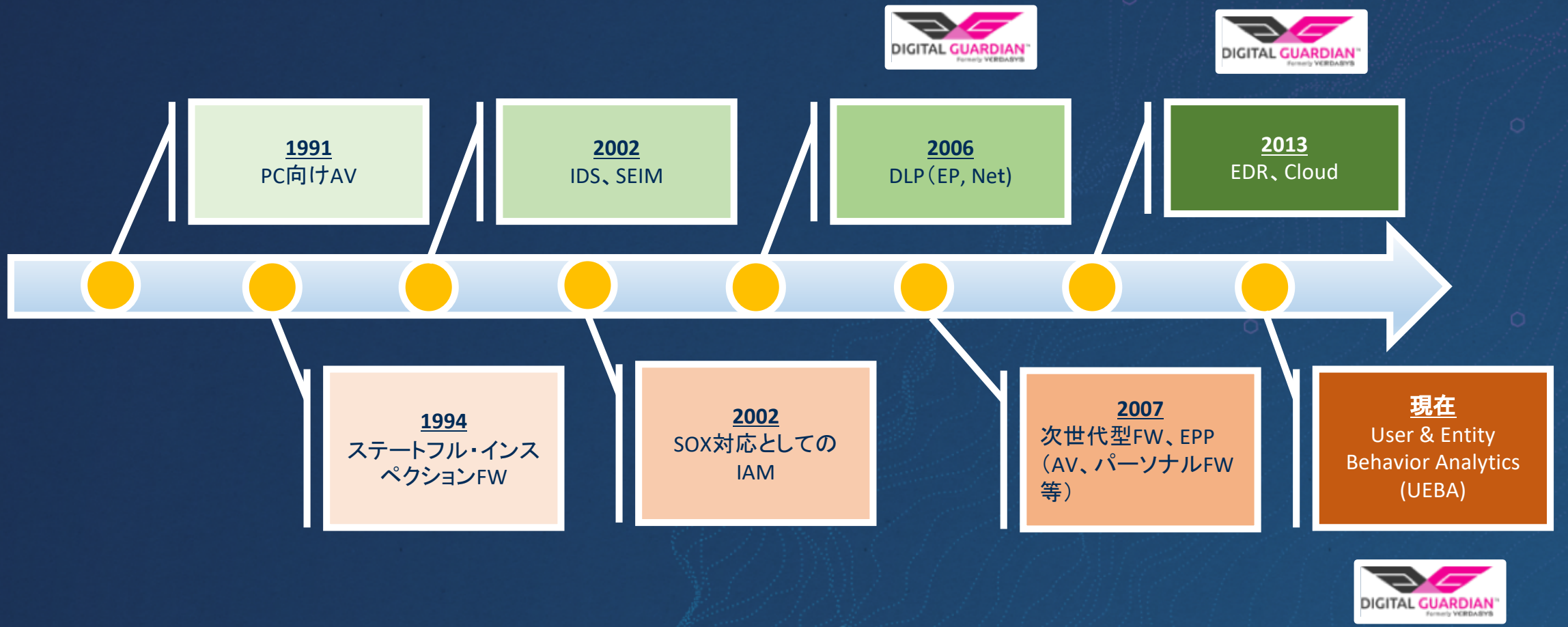
DATA IS THE TARGET.

- デジタルガーディアン
  - 2003年設立
  - CEO：Ken Levin
  - 本社：アメリカ マサチューセッツ州 ウォルサム
  - 従業員数：約500名
- 製品
  - DLP（エンドポイント、ネットワーク）, EDR, クラウドセキュリティ, 脅威分析、レポーティング
- 導入実績業界
  - 製造、建築、金融、小売、流通、ヘルスケア、公共、エネルギー、プロフェッショナルサービス、コールセンター、等

Gartner® Magic Quadrant Leader

FORRESTER® Wave Leader

デジタルガーディアン 会社概要
ソリューションヒストリー



最後に

DIGITALGUARDIAN®

Digital Guardian is a **LEADER** in the Forrester Wave™: Endpoint Detection And Response, Q3 2018

DIGITALGUARDIAN®

OPTi Secure

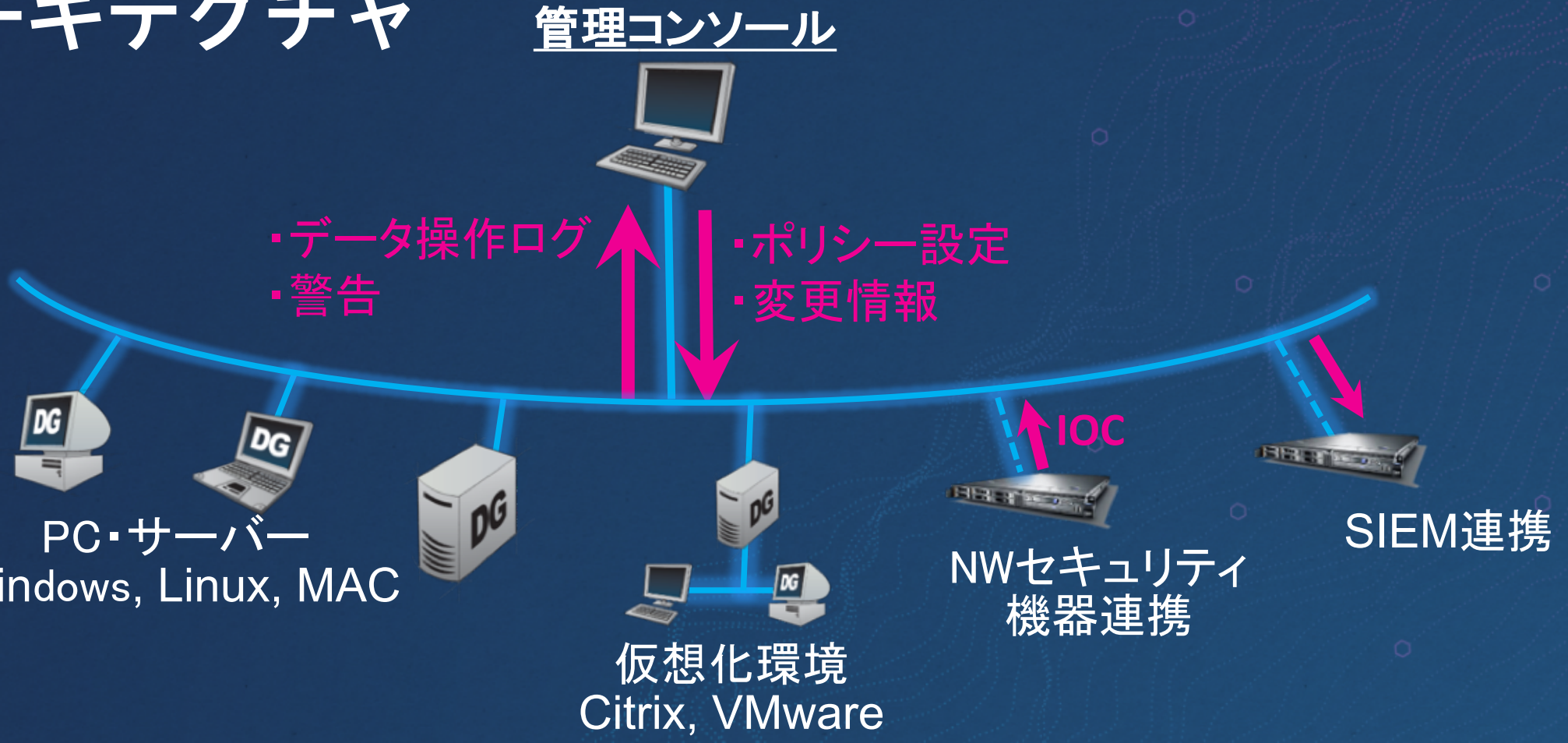
DG・マネージドサービス
「データプロテクションサービス」のご紹介

2018年7月11日

高橋真哉
ＪＢサービス 株式会社

DGについてのおさらい

アーキテクチャ


管理コンソール
・データ操作ログ
・警告
・ポリシー設定
・変更情報
DG
PC・サーバー
Windows, Linux, MAC
仮想化環境
Citrix, VMware
IOC
NWセキュリティ
機器連携
SIEM連携

特徴

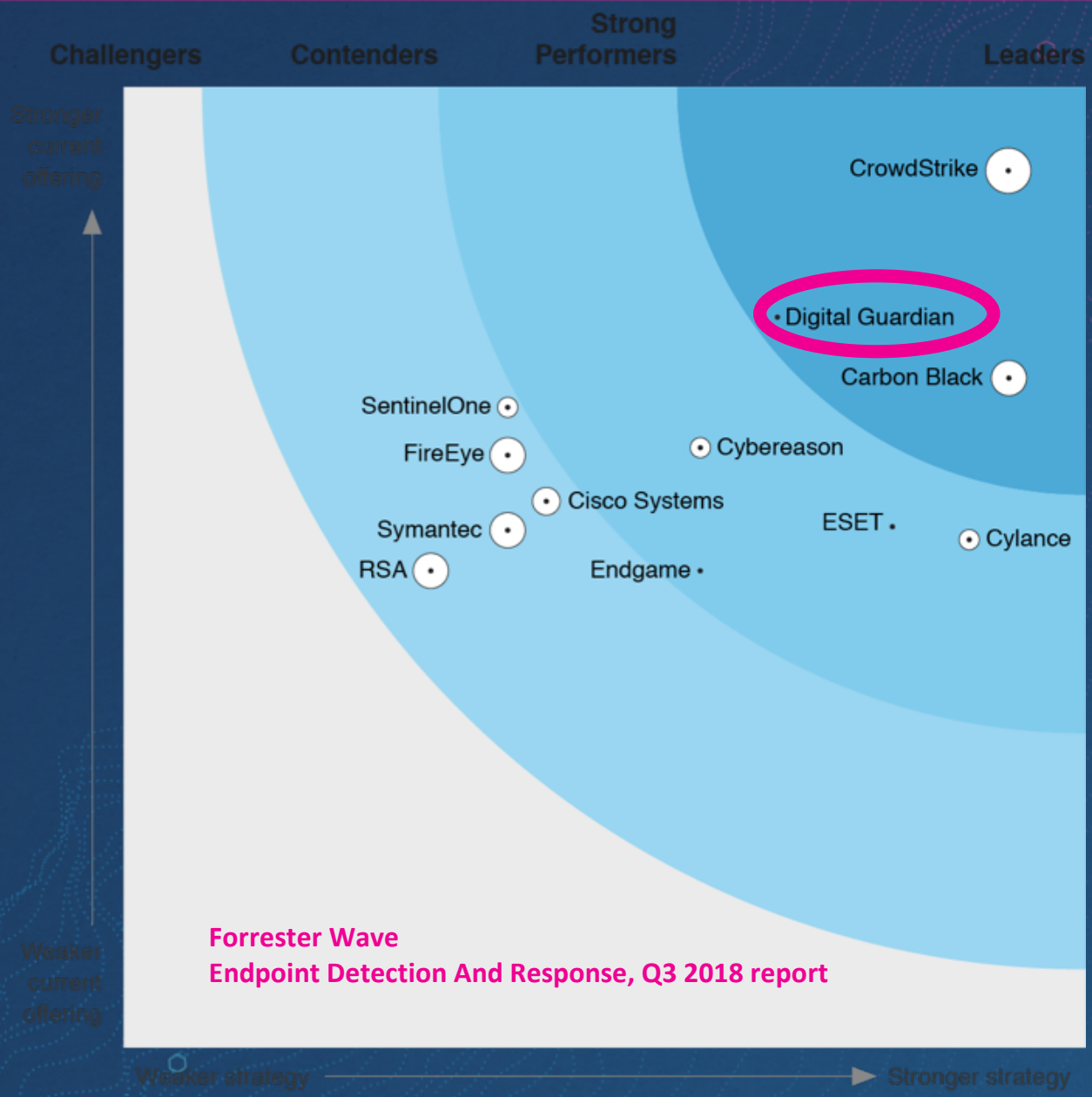
1. 重要データを自動で定義
2. 攻撃ではなく、データを見る
3. 人の操作ではなく、データの動きを見る

出来ること①

データの保護
（DLP）

出来ること②

脅威の可視化（EDR）



Forrester Wave
Endpoint Detection And Response, Q3 2018 report

マネージドサービスのご紹介

重要データはテクノロジーが見つける時代へ

これまで

1. ポリシーの作成
2. 重要データの定義
3. 重要データの分類、探索
4. 方法論の検討
5. 製品検討
6. 実行

CISO、IT部門

テクノロジー

これから

1. 重要データの定義
2. 重要データの探索、分類
3. ポリシーの作成
4. 方法論の検討
5. 製品選定
6. 実行

テクノロジー

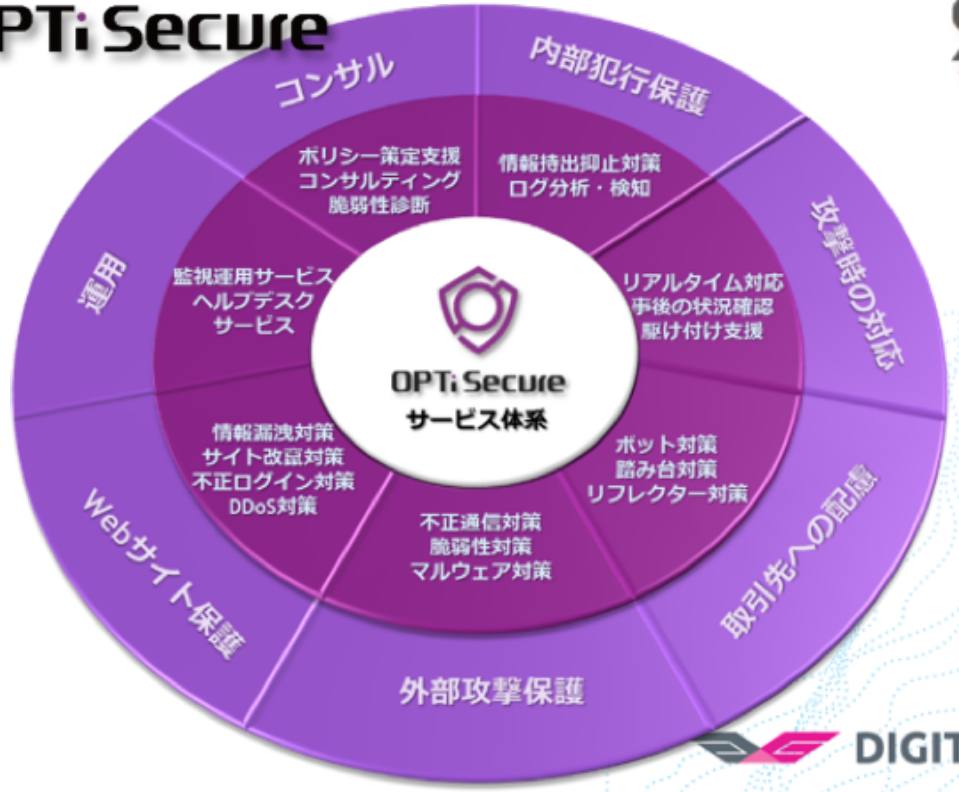
CISO、IT部門

マネージドサービス

● 社名	ＪＢサービス株式会社
● 代表者	代表取締役社長　三星義明
● 設立	2007年4月2日（日本ビジネスコンピューターのサービス事業部門を分社）
● 資本金	4億8千万円
● 社員数	467名
● 拠点数	44拠点

（2018年2月1日時点）

OPTi Secure



SMAC
Solution Management and Access Center

DIGITALGUARDIAN®

世界最高水準の情報漏洩対策ソリューション

中堅以下の組織では

- 導入構築の難易度が高い
- 機能が豊富過ぎる
- ログが取れすぎる

DIGITAL GUARDIAN®

マネージドサービス

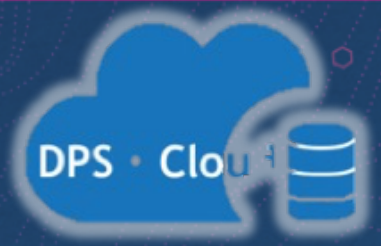
気軽にご利用頂く

しっかり使いこなす

データプロテクションサービス　主な違い

DPS・Cloud		DPS Enterprise
簡単・迅速	サービスコンセプト	詳細・じっくり
SaaS	提供形態	オンプレミス
推奨ルール利用	ルール	オーダーメイド

データプロテクションサービス・クラウド



SMAC

DIGITAL GUARDIAN

・管理
・ログの保管
・アラート分析
・ライセンス提供

・重要アラートご連絡
・分析結果とアドバイス
・月次の可視化レポート

・ルールの配信
・ログのアップロード

システム部門

エンドユーザー様

クラウドサービス利用のメリット

✓インフラ不要

✓専任者不要

✓クイックスタート

データプロテクションサービス　主な違い

DPS・Clou		DPS Enterprise
簡単・迅速	サービスコンセプト	詳細・じっくり
SaaS	提供形態	オンプレミス
推奨ルール利用	ルール	オーダーメイド

DPS・エンタープライズ　サービス概要

SMAC

・管理コンソール管理
・カスタムルール作成
・インシデント調査

・重要アラートご連絡
・分析結果とアドバイス
・月次レポート

システム部門

・ルールの配信
・ログのアップロード

エンドユーザー様

マネージドサービス利用のメリット

✓容易な使いこなし

✓専任者不要

✓クイックスタート


DIGITAL GUARDIAN®


OPTi Secure