Digital Guardian

リスクを可視化し、あらゆる脅威から重要データを守る 次世代エンドポイントセキュリティ Digital Guardian

昨今の標的型攻撃や内部不正を防ぐ為には、次世代ファイヤーウォールやサンドボックスといった入口・出口対策だけでは難しくなってきているのが実情です。
Digital Guardianは最終的に守らなければならない”データ”に着目して、守ることに特化した次世代エンドポイントソリューションです。

Digital Guardianでの内部不正、標的型攻撃対策

内部不正

データの漏えいをあらゆる方法で防ぎます

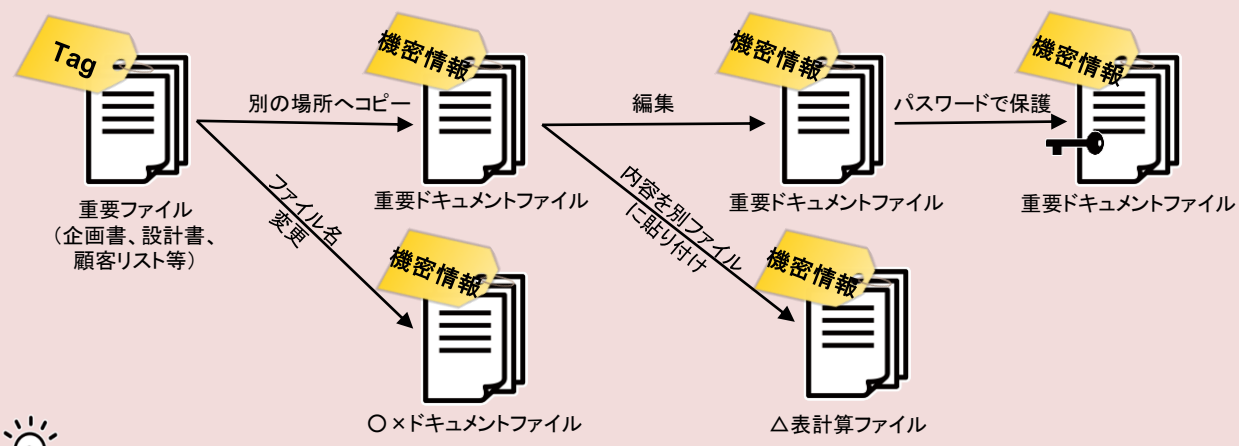
- 社外に持ち出したオフライン端末でもポリシーは有効
- スクリーンショットや印刷も制御して漏えいを防止
- 怪しい行動に対しては抑止効果のある警告も可能

標的型攻撃対策

データ漏えいの検知に加えてマルウェアの検知も可能です

- PC上でプロセスを監視し、怪しい振る舞いを時系列に検出
- マルウェアに感染した状態であってもデータの漏えいはガード
- 暗号化やファイル名を変更した外部送信も検知可能

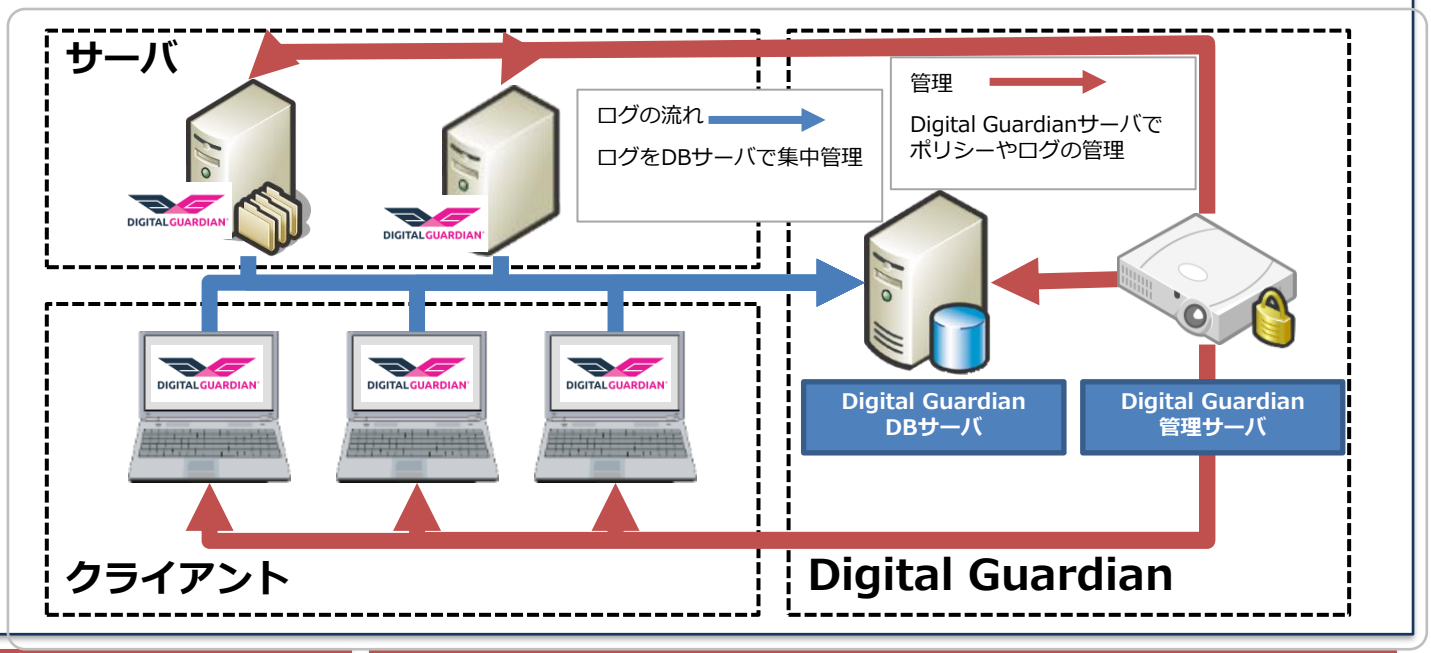
データ漏えいを防止するファイルのタグ付けと追跡機能



ファイルを変更・操作しても重要データのタグは引き継がれ、追跡が可能！

システム構成と主要機能

システム構成



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どんなファイルもアップロードさせない。また、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	マイナンバーやクレジットカードNo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	機密ファイルを外部記憶メディアへ書き込む際に暗号化させる。
ログ収集	あらゆる操作ログを記録するとともに、バックグラウンドで起動しているプロセスやセーフモード起動してもログ収集が可能。
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。
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。

お問い合わせ

ニッセイ情報テクノロジー株式会社
クラウドサービス事業部
TEL：03-5714-5029　Mail：security_info@nissay-it.co.jp

文書審査承認番号：NIT2023-008(ク002)04