ゼロトラストと サイバーレジリエンスの強化

MICRO FOCUS is now opentext

ゼロトラストとサイバーレジリエンスによるセキュリティの強化

ゼロトラストは、従来のネットワーク境界防御の概念を捨て去り、システムにアクセスするものはすべて信用せず、その安全性を検証することで、情報資産への脅威を防ぐという、という考えですが、ゼロトラストは単一製品/ソリューションでの実現は難しく、製品/ソリューション間の連携が必須となります。
しかしながら、ゼロトラストを取り入れたセキュリティ対策を行っても、サイバー攻撃を完全に防ぐことは困難です。

一方で、サイバーレジリエンスは、サイバー攻撃を前提に、それを防御し攻撃による被害を低減しつつ、被害にあっても迅速に復旧を行い、ビジネスを継続する取り組みです。ゼロトラストは防御に重点を置いているのに対し、サイバーレジリエンスは、被害からの復旧に重点を置いています。

サイバー攻撃は日々巧妙に進化し続けており、完全に攻撃を防御することが難しくなってきている現状では、ゼロトラストの考えを取り入れ、攻撃に対する防御、なおかつ、サイバーレジリエンスの考えに基づき被害からの迅速な復旧、これらを行う事で、サイバー攻撃の脅威を最小化できます。

マイクロフォーカスは、4つのポートフォリオでお客様のサイバーレジリエンスの強化を支援します。

データプライバシー/プロテクション

- 個人情報・機密データの保護（暗号化、トークン化）
- カード情報保護、非保持化による監査範囲の縮小
- データクラウドとの連携によるセキュアな分析
- テスト用データの保護・管理

Voltage

The Forrester Wave™: Dynamic Data Masking Solutions, Q3, 2021においてリーダーに選出

デフォルト（標準仕様）でプライバシーを保護する80以上の
特許を取得しているパイオニア的な先進技術

アプリケーションセキュリティ

Fortify

- 最新の開発に対応したソフトウェアレジリエンス
- 包括的なAppSecプラットフォーム
- ソフトウェアサプライチェーンの保護
- 自社開発コードだけでなくOSS のライセンス違反や脆弱性発見も可能

Gartner®アプリケーション・セキュリティ・テストの Magic Quadrant™で、9年連続リーダーの1社に位置付け

業界をリードする精度とカバレッジの広さを
オンプレミスでもSaaSでも提供

MICRO FOCUS is now opentext

アイデンティティおよびアクセス管理

- インテリジェントアクセスガバナンスによるゼロトラスト
- アダプティブアクセスと自動化
- 不正アクセスからの非構造化データの保護
- セキュリティポリシー制御の一元管理

NetIQ

ヨーロッパを代表する情報セキュリティ専門アナリスト企業の Access Management 2022レポートでリーダーに選出

従業員や顧客を対象とした包括的なIDおよびアクセスサービスを提供し、
組織のセキュリティを確保することでゼロトラストを実現

セキュリティオペレーション

ArcSight

- 業界トップのリアルタイム相関分析
- ユーザー・エンティティの行動分析、SOARとの統合
- オープンでスケーラブルなデータプラットフォーム
- 脅威インテリジェンス（MITRE、MISP、GTAP+）

GigaOmのRader for SIEMにて、革新的なリーダーと アウトパフォーマーに選出

KuppingerCole のリーダーシップコンパス for インテリジェンス SIEMプラットフォームにて、Overallリーダーに選出

Voltage	継続的なデータの発見、洞察、および保護によりリスクを軽減し、デフォルトでプライバシーを保護することで、企業や組織の安全を確保します。Voltageの先進的なフォーマット保持型エンタープライズデータ保護技術には、暗号化、トークン化、ハッシュ化、およびマスキング機能が備わっており、プライバシーコンプライアンス、決済基準と規制、およびデータセキュリティに対応しています。日本語特設サイト
Fortify	オンプレミスでもSaaSでも、CI/CDパイプライン全体を通じてテストを自動化するアプリケーションセキュリティプラットフォームを提供します。また、自社開発コードだけではなく、 OSS のライセンス違反、脆弱性の発見も可能にします。（オプション） 日本語特設サイト
NetIQ	セキュリティの要であるIDを中心としたセキュリティ強化を実現します。ID登録から抹消までのライフサイクル管理に始まり、ID認証と承認の統合標準、ユーザーが自身でプロファイル管理するセルフサービスなど、あらゆるデバイスに対応した、いつ、どこからでも適切なリソースにアクセスするユーザーエクスペリエンスを提供し、個人情報も保護します。 リアルタイムの監視を容易にしアクセス権限を視覚化して役割のマイニングと分析、リスク スコアリング、監査制御のサポート、およびコンプライアンス レポートを提供し、意思決定の支援を行います。
ArcSight	すべてのセキュリティ監視業務をエンドツーエンドで包括する次世代SOC プラットフォーム。 ArcSight Intelligenceは、内部脅威、未知の脅威、情報漏洩の3つにフォーカスした製品で、教師なし学習を使って未知の脅威を検出します。ArcSight Intelligenceユーザーは、追加ライセンスや追加費用なしでSOAR（セキュリティ運用の自動化及び効率化の機能）が利用できます。日本語特設サイト

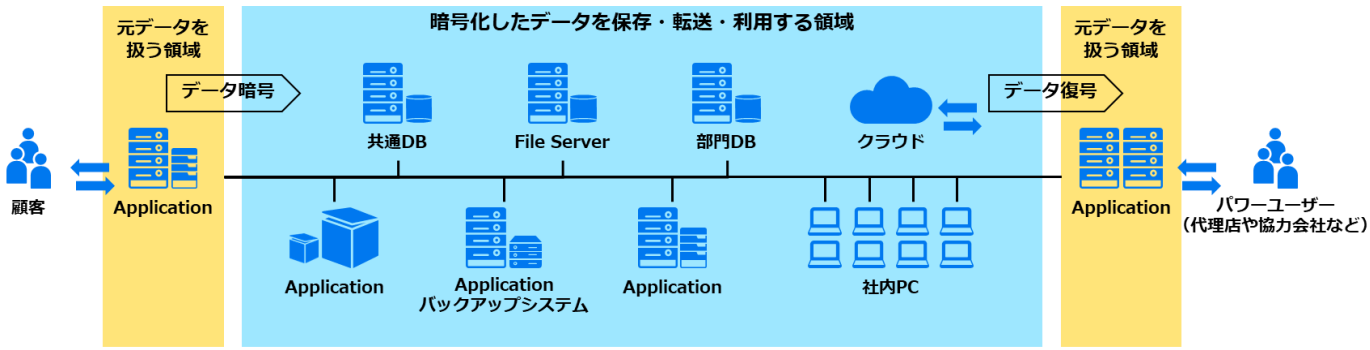
マイクロフォーカスエンタープライズ株式会社
jp-info-enterprise@microfocus.com
microfocus-enterprise.co.jp

Voltage

デフォルト（標準仕様）でプライバシーを保護する80以上の特許を取得しているパイオニア的な先進技術で、入力時にデータの暗号化を行い、生データが必要な業務以外は、暗号化した状態で保存・転送・利用します。

データ自体を暗号化するデータセキュリティ

データが入力された時点から暗号化を行うことで、本当に生データが必要な業務以外は暗号化状態で保存・転送・利用が出来るようになります。アプリケーションやネットワーク、データベースなど、レイヤーごとのセキュリティ対策では、レイヤー間でセキュリティギャップが生じますが、Voltage SecureDataは、End-to-Endで情報を保護することでギャップをなくします。



Voltage SecureData　主な機能

- フォーマット保持型暗号（FPE：Format Preserving Encryption）
- フォーマット保持型ハッシュ（FPH：Format Preserving Hash）
- セキュア・ステートレス・トークナイゼーション (SST)

FPEで暗号化した例

変換例	生データ	暗号化データ （日本語に対応）
氏名	庄司　まゆみ	禽騨　ひろま
郵便番号	123-4567	814-6811
住所	東京千代田区丸の内１－２－３ 丸の内ビルズA-1001	姥蒂遠凭拉湧鑓ご癌５－０－５ 杏そ課ペノキM-1874
電話番号	010-2345-6789	631-8723-5075

データセキュリティの主なユースケース

PCI監査対応

- 監査対応範囲の縮小
- Point-to-Point Encryption (P2PE)による暗号化、カード情報非保持化

例えば…

クレジットカード情報保護に関する課題

・PCI DSS対応のため、トークンを使って、クレジットカード情報の非保持化を進めたい

・ PCI DSS対応費用削減のため、監査対象範囲をできる限り狭めたい

・各加盟店でのPCI DSS対応は困難なので、加盟店側には生のクレジットカード情報が残らないようにしたい。

データの秘匿化

- 運用環境での包括的なデータ保護
- クラウドへのセキュアなデータ移行
- セキュアなビッグデータ解析
- 秘匿化によるテスト用データの作成

例えば…

個人情報保護に関する課題

・改正個人情報保護法の報告義務の例外となるよう、個人情報は、万が一に備え、高度な暗号化を行いたい

・個人情報をクラウドに移行する際には、オンプレもクラウドも共通した方式で暗号化したい

・個人情報を含む大量のデータをデータレークに保存して、サービス利用履歴や購買履歴の解析に利用しているが、漏洩が心配

テストデータに関する課題

・テスト品質をあげるためには、本番と同じデータを利用したいが、特に開発やテストをアウトソースしている場合にデータの漏洩が心配

・人工的に作成したデータでのテストでは、データが偏ってしまって、十分なテストができないことも多い

・本番環境と同じ特性を持つデータでないと、不具合が再現しないことが多い

Secure Stateless Tokenization (SST)によるトークン化

生のクレジットカード番号を保持するシステムを必要最小限とし、PCI DSSの監査対象システムを削減

- クレジットカード番号を数学的な関係性を持たないセキュアステートレストークン化 への変換でクレジットカード情報の 非保持化を実現
- 置換には静的なテーブルを利用するためトークンを管理するデータベースが不要

Format Preserving Encryption (FPE)による暗号化

元の機密情報を保持するシステムは必要最小限にし、万が一の漏洩時に備えて、機密情報を無害化しておく

- 入力時点からデータ自体を暗号化すると、本当に生データが必要な業務以外は暗号化状態でデータを保存・転送・利用
- 仮に保護されたデータが漏洩してもデータ自体が暗号化されているため、ビジネスへのインパクトは最小化される

Voltage 特設サイト

日本語のデータシートや事例資料、過去の講演動画などを掲載しています。
https://www.microfocus-enterprise.co.jp/products/voltage/

Fortify

Fortifyは、オンプレミスでもSaaSでも、CI/CDパイプライン全体を通じてテストを自動化するアプリケーションセキュリティプラットフォームを提供します。

包括的でスケーラブルなポートフォリオで、最新のDevOpsと既存SDLCをサポートする広範囲の統合に対応します。

Fortifyは幅広いポートフォリオで業界をリードする精度とカバレッジの広さを持ち合わせています

幅広いポートフォリオ

Static Code Analyzer (SCA): ソースコードのセキュリティ脆弱性を分析します (静的テスト：SAST)。

ソフトウェアコンポジション解析: SonatypeやDebrickedを使用してオープンソースコンポーネントの脆弱性をスキャンします。

WebInspect: 動的テスト:DAST は、実行中のアプリケーションを分析し、アプリケーションに対する攻撃をシミュレートすることで 脆弱性を発見します。IASTエージェントが含まれます。

	統合管理	SAST	ソフトウェア コンポジション解析	DAST	MAST
オンプレミス	✓ SSC	✓ SCA	✓ Sonatype / Debricked	✓ WebInspect	–
SaaS (FoD)	✓ 独自	✓ SCA	✓ Debricked	✓ WebInspect	✓ 独自

Software Security Center (SSC): オンプレミスソリューションに付属する総合的なアプリケーションセキュリティプラットフォームで、アプリケーションセキュリティリスクに関する包括的な可視性を実現します。

Fortify on Demand (FoD): サービス型（SaaS）のアプリケーションセキュリティ。SAST、DAST、MAST（モバイル診断）を含みます。

スキャンの精度

100%
OWASP 1.2bベンチマークでの
Fortify SCAの真陽性率

95%
Fortify SCAは、検出漏れを最小化した上で、機械学習を使用して誤検出を削減

脆弱性を見逃す方が、誤検知の確認にかかる 時間よりもコストが高い可能性がある

Fortifyソフトウェアセキュリティリサーチによる裏付け (2021年12月時点)

カバレッジの広さ

1,286
検出された脆弱性カテゴリ

30
サポートされるプログラミング言語

1,000,000以上
対応しているアプリケーション
プログラミングインターフェイス

幅広いコンプライアンスに対応

- OWASP Top 10
- OWASP Mobile Top 10
- SANS Top 25
- DISA STIGs
- GDPR
(General Data Protection Regulation)
- FISMA Compliance

2,000社以上のグローバル導入実績

「Micro Focus Fortifyは、開発者のニーズに間違いなく応えてくれます。ニーズをよくわかっています。」
- Damien Suggs氏 (AppSecディレクター)

「このパートナーシップの目的は、Fortify on Demandで AppSecを最新化することで、実用的なデータ主導の結果を得ることです。」- Rajan Gupta氏 (製品セキュリティ担当VP)

Fortify特設サイト

最新情報を含む製品関連資料や事例、アプリケーションセキュリティに関するレポートなどをご紹介しています。
https://www.microfocus-enterprise.co.jp/products/static-code-analysis-sast/

ID&アクセス管理（IAM）

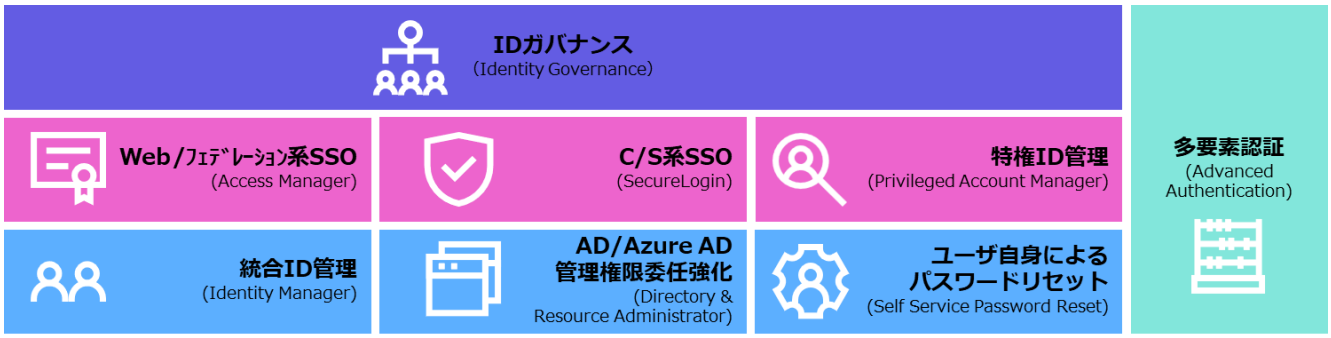
ID登録から抹消までのライフサイクル管理に始まり、ID認証と承認の統合標準、ユーザーが自身でプロファイル管理するセルフサービスなど、あらゆるデバイスに対応した、いつ、どこからでも適切なリソースにアクセスするユーザーエクスペリエンスを提供し、個人情報も保護します。

ゼロトラストにおけるIAMの重要性

「ゼロトラスト」は、調査会社Forrester Researchのアナリストが2009年に発案した概念です。何も信頼せず、全てのアクセスに対して全てを疑い検証することを意味しています。
ゼロトラストの概念を取り入れたセキュリティ対策では、システムやデータへアクセスするためのIDがセキュリティ境界となりますが、IDのみならずデータ・アプリ・デバイスもそれぞれ保護する必要があります。
なお、ゼロトラストは単一製品やソリューションでの実現は難しく、これら製品やソリューション間の連携が必須です。
例えば、クラウド・アクセス・セキュリティ・ブローカー（CASB）、セキュア Web ゲートウェイ（SWG）、セキュリティ情報とイベント管理（SIEM）やエンドポイントにおける検知と対応（EDR）、情報漏洩対策（DLP）などが関連しますが、それぞれが見ているIDは本当に正しいと言い切れるのでしょうか。
IDの管理が正しく行われない限り、関連製品によるゼロトラスト対策も信頼性が揺らぐことになります。
これら関連機能が本人確認に利用するIDは、IAMにより管理されるため、ゼロトラストの中でもIAMが最も重要な機能であると言えます。

NetIQ 製品ポートフォリオ

IDを中心としたNetIQ IAMは、以下に代表される製品で構成されています。



ソリューション	目的
IDガバナンス	ユーザが持つ各種アクセス権限を収集して、リスク値等を使い不適切な権限が付与されていないか監査することを目的としています。 統合ID管理と組み合わせることで、監査に加えて自動反映させることも可能となります。
Web/フェデレーション系SSO	WebサイトやSaaS利用時のID/パスワード入力の手間を軽減します。
C/S系SSO	Web化されていないツール、例えば、ESXクライアントやターミナルソフトへのID/パスワード入力の手間を軽減します。
特権ID管理	共有して利用されることが多いroot/administratorといった特権IDの、利用制限、ならびに、操作内容の監査を目的としています。
統合ID管理	冗長的なID管理作業をシステムで自動化して、管理作業の負荷を軽減します。
AD/Azure AD管理権限委任強化	AD管理ツールで不足する最小権限管理を強化します。
ユーザ自身によるパスワードリセット	ユーザ自身でパスワードリセットが可能となるため、ヘルプデスクの作業負荷を軽減します。
多要素認証	ID/パスワードでは不足する個人特定化情報を、他の要素、例えばOTPやスマートフォン等を使い個人特定化を強化します。

NetIQ 選ばれる理由

ゼロトラストの要であるID/アクセス/ガバナンス管理まで単一ベンダーで完結

一般的にこれらの管理機能は、別ベンダー製品を組み合わせて構成されるため、以下の様な問題が発生します。

- 製品間の親和性の低さ
- カスタマイズ工数/運用コストの増大
- 障害発生時対応時間の増加

NetIQ製品では、これらすべての管理機能を一括提供しているため、上述する問題点は最小化され、適切な管理基盤を実現できます。

高機能

NetIQ製品は、管理の容易性を高める数多くの機能に対応しています。
統合ID管理では、役職や兼務等の管理に適したロール機能、ロールを応用したワークフロー・職務分掌・レポート等に対応しています。
Web/フェデレーション系SSOでは、ID/パスワード以外の個人特定化情報やユーザ行動分析リスクスコアを用いたリスクベース認証、リスクスコアが高いユーザに対する多要素認証による本人確認強化に対応しています。
その他製品も各製品に求められる数多くの機能を有しています。

グローバル対応

NetIQ製品は、日本語対応だけでなく多くの諸外国言語に対応しています。
国内のITエンジニア不足に伴う外国人ユーザの採用、海外展開に伴う現地法人のM&A等が行われた場合でも
外国人ユーザが必要とする言語を使ってシステムをご利用いただく事が可能です。
また、システム構築やサポートにおいても海外連携を行っておりグローバル体制での支援が可能です。

ヨーロッパを代表する情報セキュリティ専門アナリスト企業のAccess Management 2022レポートでリーダーに選出

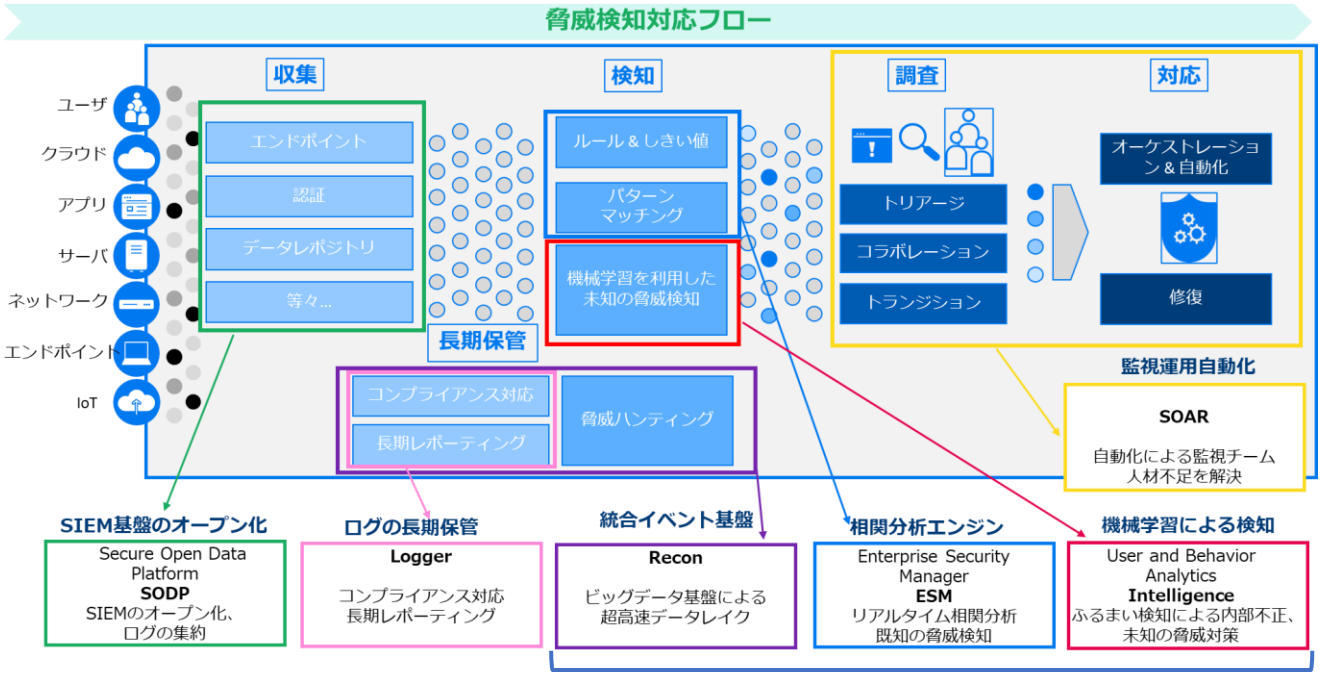
ArcSight

すべてのセキュリティ監視業務をエンドツーエンドで包括する次世代 SOC プラットフォーム

包括的なセキュリティ分析、ネイティブSOAR、インテリジェントな自動化により、脅威の検知と対応を迅速化します。

脅威検知対応プロセスとArcSightソリューションマッピング

ArcSightは、さまざまなソースからのデータの自動収集、多層アナリティクスによる高度な脅威の検出、迅速かつ効率的な調査、そして被害が発生する前に対応する能力を備えた、次世代SOC構築の実現を支援します。



- リアルタイム相関と仮説および分析ベースの脅威ハンティングで、コンテキストの豊富なインサイトを提供する多層アナリティクス
- 多層アナリティクスと脅威モニタリングのコンテンツパッケージにより、MITRE ATT&CKの手法と戦術を広範囲にカバーします。

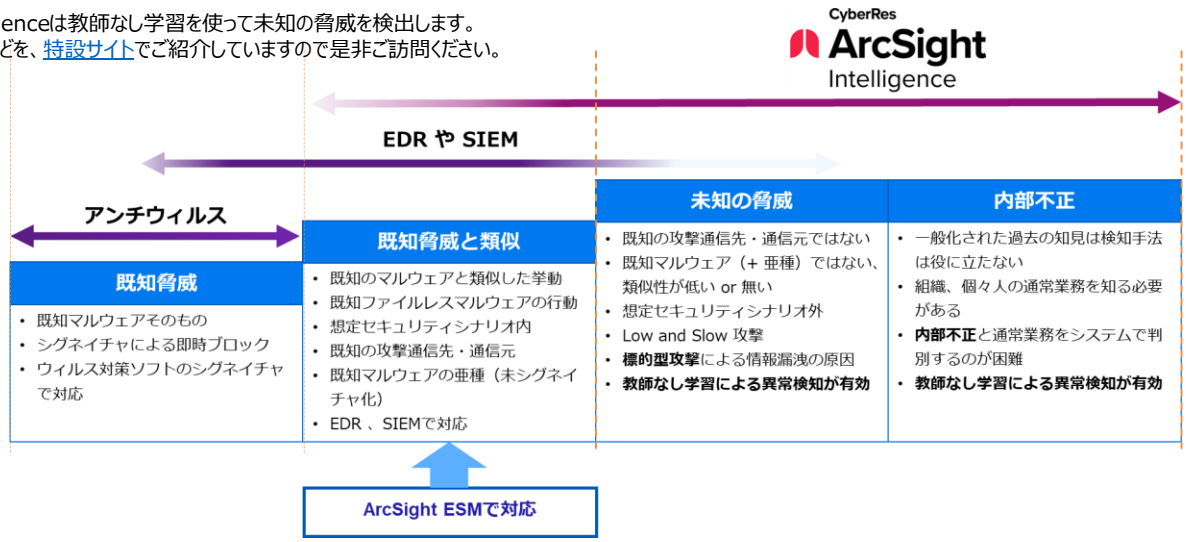
Recon・ESM・Intelligenceで実現する多層アナリティクス

監視の現場で、この3種類の分析ツールを自在に使えることが重要

高速検索・統計処理	リアルタイム相関分析	教師なし学習・機械学習
原因究明 予兆調査	既知脅威の検知	未知脅威の発見 内部脅威の発見

内部不正、未知の脅威にフォーカスしたArcSight Intelligence

ArcSight Intelligenceは教師なし学習を使って未知の脅威を検出します。
特長や関連資料などを、特設サイトでご紹介していますので是非ご訪問ください。



CyberRes
ArcSight 特設サイト
Intelligence

日本語のデータシートや事例資料、過去の講演動画などを掲載しています。
https://www.microfocus-enterprise.co.jp/products/interset-ueba/