インフラにセキュリティ機能を組み込み 高度化されたサイバー攻撃への防御を強化

Nutanix Cloud Platformで脆弱性対策からデータ保護まで包括的な対策を実現する

サイバー攻撃の脅威は、もはや防御だけでは防ぎきれない時代に突入している。ランサムウェアやゼロデイ攻撃、サプライチェーン攻撃などの多様な脅威に対して、企業システムのあらゆる箇所がリスクとなる中で、「止まらないIT基盤」をどう実現するかが重要な課題となっている。一方で、仮想化・コンテナ・クラウドのさまざまな技術の活用が拡大することで、セキュリティ設定や運用管理は複雑化の一途をたどっている。こうした背景から注目されているのが、「インフラそのものに強力なセキュリティ機能を組み込む」という視点だ。

管理が複雑化するIT環境では 高度化する脅威への対応が困難に

企業を取り巻くサイバー脅威は近年ますます高度化・巧妙化している。情報処理推進機構(IPA)の「情報セキュリティ10大脅威 2025 [組織]」でも1位「ランサム攻撃による被害」は、10年連続10回目の選出となっている。典型的なランサムウェアは、システムの脆弱性を突いて社内ネットワークに侵入し、複数のシステムやデバイスに横展開（ラテラルムーブメント）して拡大し、データの暗号化や破壊を行う。このランサムウェア攻撃における企業の課題を整理すると、主に以下の観点が挙げられる。

- システムの脆弱性を突いた侵入や、ラテラルムーブメントを防ぎきれない
- 仮想化やコンテナ化によって複雑化した環境で、セキュリティ設定や運用管理が追いつかない
- ランサムウェアによるデータ暗号化・改ざんで、業務停止や長期的な復旧遅延が発生する
- データ保護や復旧プロセスが分断され、事業継続性に不安を抱えている
- セキュリティポリシーがシステムごとに分散し、全体を俯瞰できない

ランサムウェア攻撃に対抗する「Nutanix Cloud Platform」

先述した課題を単一のプラットフォームで解決するのが「Nutanix Cloud Platform（NCP）」である。高度化されたサイバー攻撃からシステムを保護するその特徴として「脆弱性対策」「ラテラルムーブメント対策」「データ保護」が挙げられる。

1．脆弱性対策

この対策では仮想化基盤である「Nutanix AHV Virtualization（AHV）」とコンテナ基盤である「Nutanix Kubernetes Platform（NKP）」が中核を担う。AHVは、米国国防総省が定めたSecurity Technical Implementation Guide（STIG）をはじめとする国際標準に準拠しており、常にセキュアな設定状態を保つことができる。

さらに、Life Cycle Manager（LCM）によってセキュリティパッチやファームウェアを自動的に更新し、ハードウェアからソフトウェアまで最新の状態を維持する。設定に逸脱があった場合も、Security Configuration Management Automation（SCMA）が自動的に検知・修復を行うため、脆弱性を放置するリスクを低減できる。

一方のNKPについても、NSA/CISA Kubernetes Hardening Guidanceに準拠するほか、コンテナアプリの脆弱性管理の「Trivy」、監視診断の「NKP Insights」などの機能で安全性を確保している。

2．ラテラルムーブメント対策

脅威の侵入を完全に防ぐことが困難な現在では、万が一侵入されても被害が拡大しないような仕組みが不可欠だ。Nutanixはこの課題に対して、アプリケーション単位で通信を制御する「マイクロセグメンテーション」機能を提供している。

まずNKPにおけるマイクロセグメンテーション機能としては、アプリごとに「ラベル」を割り当てアクセス制御を行う

方式を採用しているため、アプリが別サーバーに移動した場合でも、ポリシーは自動的に追従する。一方、仮想マシン間のマイクロセグメンテーションについては、「Flow Network Security」と呼ばれる機能で実現する。こちらも先述のラベルと同様に「カテゴリ」というものを設定してアクセス制御のポリシーを設定する。

3. データ保護対策

Nutanix Cloud Platform ではあらゆるデータが、スケールアウトストレージ「AOS Storage(AOS)」のもとで Nutanix クラスター上にある SSD やハードディスク上に格納される。AOS では保存データを AES256 で暗号化する「Data-at-Rest Encryption（DARE)」を標準で搭載している。

次に、仮想マシンのバックアップには「セキュアスナップショット」が有効だ。これは複数の承認者の合意なしにスナップショットを削除できない仕組みを採用しており、仮に攻撃者に管理者権限を乗っ取られたとしても改ざんを防止できる。

さらに、「Nutanix Disaster Recovery（DR)」を利用すれば、本番サイトが停止してもスナップショットを用いて、事前に定義したリカバリプランに基づいてリモートサイトでの業務継続を可能にする。ネットワーク接続先や起動順序、スクリプトなども設定可能だ。

次にファイル / オブジェクトデータの保護について言及しよう。後述する脅威の検出機能のほか、Nutanix Cloud Platform では一度記録したデータを消去・変更できない WORM（Write Once Read Many）機能を活用することでランサムウェアなどによるデータ侵害を防止する。そのほか、ファイルサーバー全体をフェイルオーバーする DR 機能である「SmartDR」やコンテナの永続ボリュームの DR を実現する「Nutanix Data Services for Kubernetes（NDK)」 など多彩な方法によるデータ保護が可能となっている。

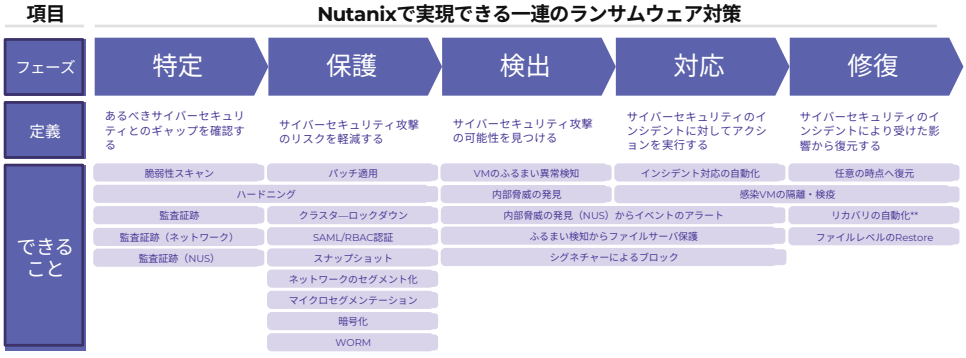
検知・対応や統合管理と可視化でセキュリティをさらに強化

ここまで中核となる脆弱性対策、ラテラルムーブメント対策、データ保護を紹介したが、最後に「脅威検知と対応」と「統合管理と可視化」の 2 つの特徴にも言及したい。

まず前者については SaaS 型のセキュリティ分析サービス「Nutanix Data Lens」が役立つ。これは、「Nutanix Unified Storage（NUS)」上のアクティビティデータを継続的に監視し、異常を検出すると自動で該当クライアントのアクセスを遮断する仕組みだ。つまり、ランサムウェアによるデータ破壊を防止するのに役立つ。

後者は「Nutanix Prism Central」や「Security Central」が有用だ。Prism Central は、クラスター全体のセキュリティ設定や脆弱性リスト、アップグレード状況を一元管理できるダッシュボードを提供するため、冒頭で指摘した管理の複雑化の課題解消に役立つ。一方、Security Central はセキュリティ監視機能を提供することで例えば先述のマイクロセグメンテーションによる仮想マシン間の通信での異常検知や推奨対策の自動提案も可能だ。

以上のように、NCP は多彩な機能を有機的に連携させることで、インフラ層そのものにセキュリティを埋め込み「守る・見つける・復旧する」を単一のプラットフォームで完結する「真のサイバーレジリエンス」を実現していく。



NIST サイバーセキュリティフレームワークに即したセキュリティ対策を一元化

Nutanix Japan 合同会社

E-mail:contact-jp@nutanix.com
https://www.nutanix.com/ja/contact-us

NUTANIX