データセンターの保護とセキュリティの完全理解

Kyle Gaede (Associate Director, Segment Group at Microchip Technology)

このブログ記事では、データセンターのセキュリティの仕組みと Microchip 社がどのようにサイバー攻撃保護ソリューションを提供しているかについてご紹介します。

デジタル要塞の保護: データセンターとクラウド セキュリティの課題に取り組む

データセンターのセキュリティは言わば、リソースへの不正なアクセスと操作による被害を軽減するために考案されたポリシー、予防策、手法の集合体です。DoS(サービス拒否攻撃)、データの盗難、改ざん、紛失は、データセンターが直面している保護されたシステムへのアクセスを目的とした数多くのセキュリティ問題の中でもよく見られる攻撃です。データのセキュリティ問題は、企業にとって、特に個人情報と金融情報をホスティングする大規模データセンターに依存している企業にとっては悪夢となり得るものです。

Anixter 社によれば、企業の 39%が最近のデータ漏洩の主な要因は不注意であったと述べています。これに対し、悪意のある犯罪的攻撃は 37%を占めており、その平均コストは 550 万ドルに上ります。当然ながら、これはデータ保管をクラウドに切り替えるデータセンターと企業が増加している理由の 1 つですが、クラウドにデータを保存する場合であっても非常に大きなリスクを伴う可能性があります。

データセンターのセキュリティの仕組み

データセンターのセキュリティでは、アプリケーション、インフラストラクチャ、データ、知的財産等を保護するために物理的データセンターとマルチクラウド環境全体にわたってワークロードを追跡します。この手法は物理サー

バベースの従来型のデータセンターから、クラウドを含む仮想サーバベースの最新型のデータセンターまで適用されます。

従来型のデータセンターは共有アプリケーションおよびデータのデリバリを可能にするコンピューティング リソースとストレージ リソースのネットワークです。主なコンポーネントとして、ルータ、スイッチ、ファイアウォール、ストレージ システム、サーバ、アプリケーション デリバリ コントローラ等があります。

データセンターには数百～数千の物理サーバと仮想サーバが存在し、アプリケーション タイプ、データ分類ゾーン、その他の手法でセグメント化されています。このような多数のリソースへのアクセスとリソース間のアクセスを制御する適切なセキュリティ規則を作成して管理する事は非常に困難です。

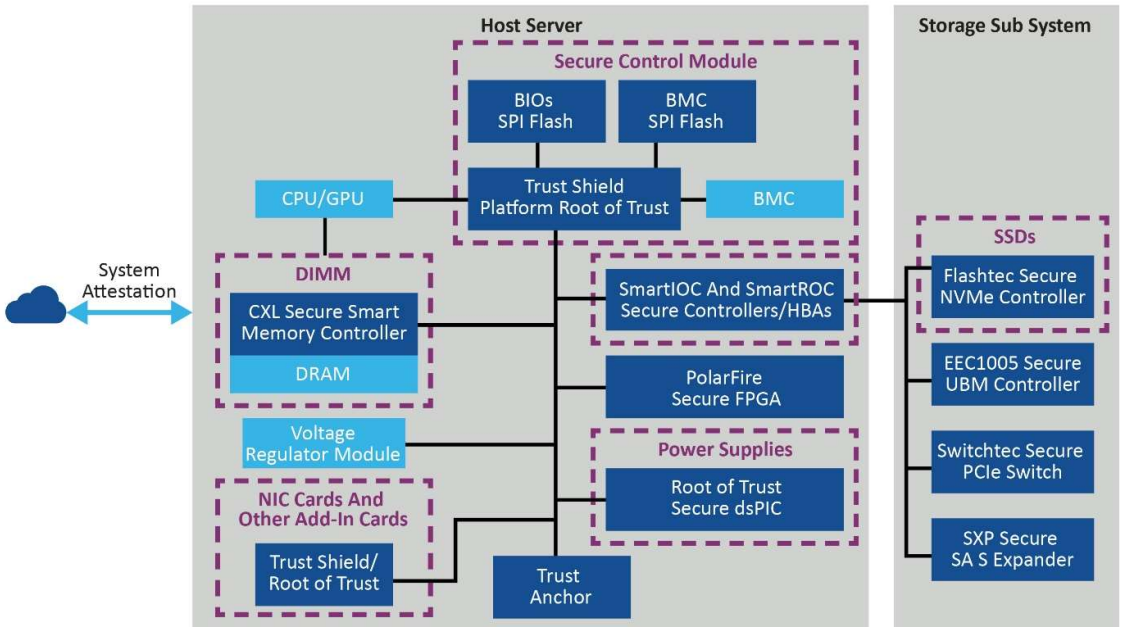
データセンターのセキュリティには重要なニーズが 3 つあります。その 1 つ目は可視性です。データセンターのセキュリティを保護する際は、ユーザー、デバイス、ネットワーク、ワークロード、アプリケーション、プロセスの可視性が求められます。可視性は性能ボトルネックの回避とキャパシティの計画およびアップグレードに役立ちます。また、攻撃の検出、悪意のあるユーザーの特定を素早く行えるようになるため、フォレンジックとインシデント事後の対応にかかる時間も短縮できます。

セキュリティで重要な要素の 2 つ目はセグメンテーションです。攻撃の範囲を狭め、攻撃がリソース間で飛び火してデータセンター全体に広がるのを防ぐ事ができます。これはパッチの適用サイクルが遅れているサーバにとっては救いの一手となり、パッチ適用前に脆弱性が悪用される可能性を減らせます。ただし、セグメンテーションを適用したからといって不本意な侵入を防げる訳ではありません。それでもハッカーの動きを鈍らせてセキュリティ担当者がパッチを導入するのに必要な時間を稼ぐ事は可能です。

ワークロードは物理データセンターとマルチクラウド環境全体を常に移動しているため、脅威からのワークロード保護は攻撃を防ぐための主要な鍵となります。これらの基本的なセキュリティ ポリシーは、動的に変更する事でポリシーのリアルタイム適用とワークロードをあらゆる場所で追跡するセキュリティ オーケストレーションを可能にする必要があります。例えば、複数の顧客を抱えるデータセンターを考えてみてください。ある顧客が別の顧客のサーバに侵入してデータや独自の知的財産を盗み出そうする可能性があります。悪意のあるハッカーは、エンドポイント デバイスにマルウェアを感染させ、フィッシングの手法を使ってだます事で従業員の認証情報にアクセスしようとする事がよくあります。

企業とデータセンターは、脅威からの保護、脅威の軽減や検出を効率化する包括的な統合セキュリティ デバイスまたは組み込みシステムを導入する事でこのような混乱を軽減できます。

ハードウェアと組み込みシステムによる不正な攻撃の軽減



データセンター統合ハードウェアおよびソフトウェアはホストサーバとストレージ サブシステムへの不正な攻撃を軽減できます。(画像出典: Microchip 社)

一部の企業とデータセンターは、ハードウェアと組み込みシステムを利用する事で不正な攻撃を軽減しています。これらはホストサーバとストレージ システムの両方に実装でき、データ保護システムを追跡して脅威の概要を包括的に把握するのに役立ちます。ホスト側では、スマートメモリ コントローラ等のソリューションを実装する事で CPU と DRAM の間にバッファを提供するセキュアな EEC メモリを使って侵入を特定して防止できます。

Trust Shield ソリューションとルートオブ トラスト(信頼の基点)ソリューションはハードウェアとファームウェア レベルでシステムを保護します。これらのソリューションは、システムのプラットフォームに対して全体的なチェーンオブ トラスト(信頼の連鎖)を確立しながらセキュアブート プロセスの土台となるランタイム ファームウェア保護を提供します。SCM(セキュア制御モジュール)も同様で、ファームウェアと重要なシステム コンポーネントを不正な攻撃から保護するセキュアな BIOS と SPI フラッシュ機能を提供します。

SmartIOC および SmartROC セキュア コントローラも、コントローラ ベースの暗号化機能を実装する事でセキュリティを強化すると共にストレージ アプリケーションのシステム性能を向上させます。セキュアな FPGA(フィールド プログラマブル ゲートアレイ)と SoC(システム オンチップ) FPGA はサーバおよびストレージ アーキテクチャ内でセキュリティ強化アプリケーションを提供するその他のソリューションです。これらはセキュリティの 3 つの層であるデータレベル、設計レベル、ハードウェア レベルを組み合わせたものです。データを安全に管理する暗号コプロセッサを含むものもあります。

意外にも、電源がサイバー攻撃の標的となる可能性があります。とりわけ DoS 攻撃に対しては最も脆弱です。これは、正規品の電源、適切なファームウェア、セキュアな dsPIC® DSC(デジタルシグナル コントローラ)を含むルートオブ トラスト コンポーネントを使う事で攻撃を軽減できます。

攻撃の防止または軽減はストレージ サブシステム側でも行えます。これは PCIe®リンク暗号化、QoS (Quality of Service)、セキュアブートおよびデータ暗号化機能を利用したセキュアな NVMe®および SSD コントローラを使う事で可能です。セキュアな UBM コントローラとスマートな PCIe®スイッチもサーバ側で役立ちます。これらを使う事でストレージ エンクロージャ管理用のセキュアなバックプレーン、セキュアブート、セキュアなファームウェア機能を実現できます。

ここで重要なのは、全ての企業とデータセンターが最新のサイバー セキュリティ保護を採用していたとしても、データが完全に保護される訳では決してないという事です。何としても侵入しようとするハッカーは侵入のためにあらゆる手段を講じてきます。ここで紹介したソリューションは、最新の脅威による侵入を遅らせ、現在利用可能な最高の脅威軽減策を提供するよう設計されています。