

クラウドへの移行を保護するSplunk

最新のSOCでクラウドへの移行を加速する

主要なメリット

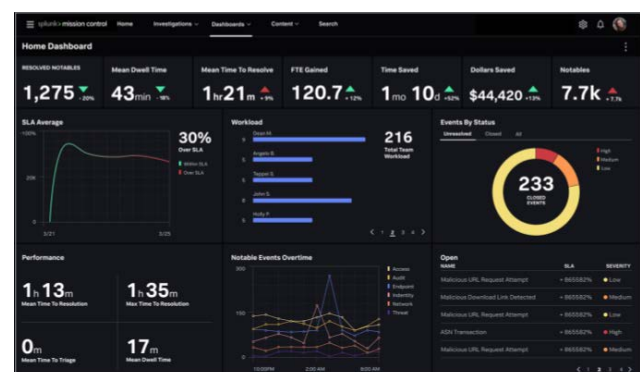
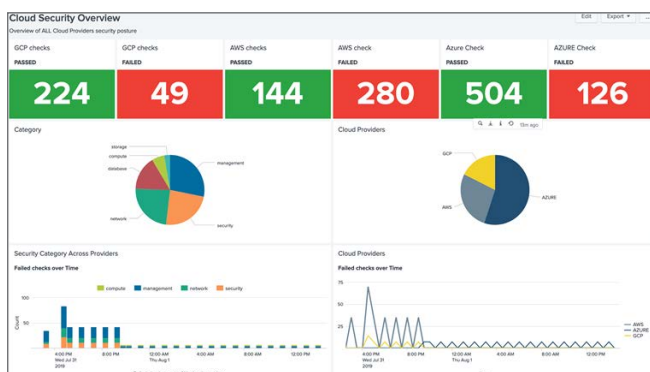
- 短期間で価値を実現 - クラウドへの移行中でも担当者はより付加価値の高いタスクに専念
- 総所有コストを削減 - インフラコストを不要にし、管理上のオーバーヘッドを削減
- リスクを低減し、サービスエクセレンスを維持 - 安全なSOC(セキュリティオペレーションセンター)プラットフォームで100%のアップタイムを実現
- SOCを迅速に拡張 - ビジネスの成長を実現



企業の94%がすでにクラウドテクノロジーを活用している今日、ハイブリッドインフラまたはマルチクラウドインフラへの移行は必然です。

しかし、クラウドへの移行は単純ではありません。移行の技術的な複雑さは、クラウドネイティブに移行する際に組織が直面する課題の1つに過ぎません。移行中はもちろん移行後も、組織の全システムにわたるセキュリティとコンプライアンスの維持は不可欠です。

ソリューションのエコシステムは絶えず流動しており、企業内の各グループはさまざまなタイミングとペースでテクノロジーを導入しています。これらの課題の根底には、ベンダーの独自システムに関する知識のギャップと、セキュリティの責任の細分化があります。SOCに関する課題は、クラウドへの大規模な移行の中断や遅延の原因になりかねません。



Splunk Data-to-Everythingプラットフォームのサンプルダッシュボード

Splunkのメリット

SplunkのクラウドベースのSIEMソリューションである **Splunk® Enterprise Security (ES)** は、SOCの役割を大きく拡大し、クラウドへの移行を加速できます。Splunk ESを導入すると、組織はクラウドを活用してSOCを迅速に構築して成熟させながら、加速的に成長するビジネスの要件に合わせてSOCを拡張できます。クラウドへの移行のあらゆる段階で問題を修正するための高い可視性と能力を備え、成熟を重ねたクラウドベースのSOCがあれば、多くの時間とリソースを解放できます。これにより、チームは付加価値の高いタスクに専念できるようになり、リスクを低減し、価値実現までの時間を短縮しながらクラウドへの移行を促進できます。

SplunkでSOCをクラウド向けに変革

Splunk ESをクラウドで活用すると、最新のSOCを構築するために最もコストと時間がかかる問題が解消されます。インフラ内のハードウェアの設置、監視、保守が不要であるため、セキュリティアナリストは、同じレベルのセキュリティを提供しながらも、組織をサポートするより付加価値の高いタスクに専念できます。コラボレーション型の統合環境では、自動化と脅威インテリジェンスにより、高度な脅威の識別、防御、対応に要する貴重な時間を節約できます。

ワークロードとアプリケーションをクラウドに移行する途中でも、セキュリティ担当者は、Splunk ESをクラウドで活用して、ハイブリッド、マルチクラウド、オンプレミスのインフラ全体をセキュリティで保護することで、セキュリティ運用とセキュリティインテリジェンスを強化することができます。Splunkのお客様は、Splunk Enterprise Securityを **Splunk® Cloud** と組み合わせて使用することで、高度なマルウェアを検出し、高度な脅威を調査して、迅速に対応することができます。また、多くの場合は数時間で価値を実感することができます。

さらに、この組み合わせによってSOCの拡張が容易になります。Splunk Cloudは、一時的なものであるか(アラートの増加など)、ビジネスの成長に応じた永続的なものであるかを問わず、変化に合わせて拡張できます。ハードウェアとソフトウェアのアップグレードはSplunkが行うため、余計な時間とリソースに投資せずに、最新のテクノロジーを活用できます。

責任の共有により 安全なコラボレーションを実現

クラウドでのSplunk ESは、すべての環境に関する単一の情報源を提供します。これにより、インフラが分散し攻撃対象が拡大する状況でも、チーム間のコラボレーションを簡単に行えます。Splunkは、クラウドサービスプロバイダーとして、重要なデータを保護する責任を共有します。Splunk Cloudは、世界の規制当局と標準化組織のすべての認定と標準の要件を満たしています(SOC2 Type II、FedRAMP、ISO 27001、[その他多く](#)を含みます)。

セキュリティの中核としてSplunkを導入すれば、ハイブリッドクラウド環境とマルチクラウド環境のサイバーセキュリティを強化しながら、クラウドへの移行を加速できます。また、Splunk CloudにSOCを構築すると、コストとリスクを低減し、俊敏性、信頼性、柔軟性に優れたセキュリティプラットフォームのメリットを活用できます。詳細については[こちら](#)をご覧ください。



営業へのお問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html
〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階

www.splunk.com/ja_jp
splunkjp@splunk.com