ORACLE

エンタープライズを保護するための クラウド・セキュリティの傾向

クラウドによって組織のセキュリティ態勢を
強化する方法

クラウドの支援により、組織は変化するセキュリティの懸念事項に対処

ITおよびセキュリティのリーダーは、サイバー攻撃が増加し、ITインフラストラクチャが複雑化するにつれて進化し続けるセキュリティ面の課題に直面しています[1]。マルチクラウドの導入、リモート・ワーク、デジタル顧客エンゲージメント、およびデータとデバイスの増加により、組織では攻撃対象領域が拡大し、コストのかかる非効率性や不要なリスクを発生させる可能性があるツールが過剰になっています。

組織は、これらの課題に対処する方法を評価するにあたり、セキュリティ態勢を強化する、よりシンプルで効率的な方法を求めてクラウドに移行しています。多くの組織では、クラウド・インフラストラクチャはオンプレミス・データセンターよりもセキュアなプラットフォームを提供でき、システム・セキュリティのタスクを自動化し、リスクの軽減に役立つサービスによってサイバーセキュリティを簡素化できます。

このEブックでは、組織がセキュリティ面の課題に対処するためにクラウド・サービスをどのように使用しているかについて傾向を説明し、セキュリティの複雑さを軽減しようとしているITおよびセキュリティ部門のリーダーにアイデアを提供して、Oracle Cloud Security Servicesが貴社のセキュリティ戦略の一部になり得る方法を示します。

1.“Is your organization too complex to secure?,” PwC, 2022

クラウド・セキュリティの傾向

01 統合されたIDおよびアクセス管理システム

02 クラウド・サービスによる脅威の検出

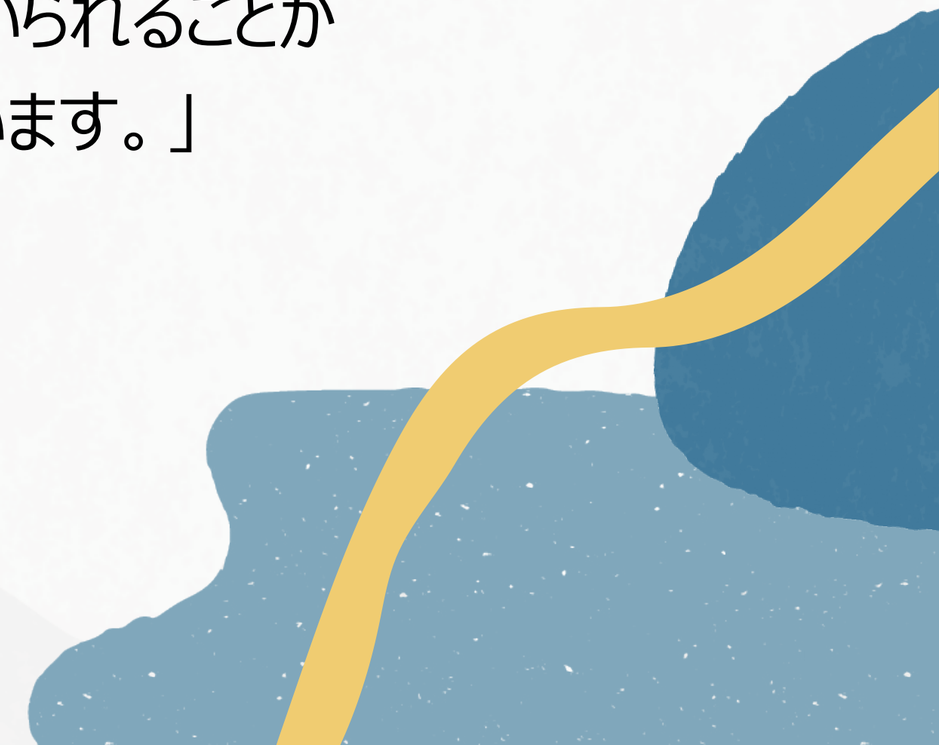
03 自動化の使用によるデータ損失のリスクの軽減

04 マルチクラウド・アプローチをサポートする階層化されたセキュリティ戦略

05 サイバーセキュリティの知識を備えた企業役員

「長年にわたり、セキュリティはOracle Cloud全体の設計面での重要な考慮事項です。セキュリティは基盤として組み込まれるべきものであり、お客様がセキュリティとコストの間で妥協を強いられることがあってはならないと当社では考えています。」

Oracle Cloud Infrastructure、Executive Vice President、Clay Magouyrk



傾向

統合されたIDおよびアクセス管理システム

IDのスプロール化を制御するため、組織は、顧客、従業員、およびマシンの相互作用を1か所で把握できる統一されたIDおよびアクセス管理（IAM）プラットフォームに移行しています。

Enterprise Strategy Groupの最近の調査によると、85 %のIT組織でパンデミックが理由でクラウドの使用が加速しています[2]。クラウド・フットプリントが拡張して、より多くのアプリケーションとサービスが含まれるにつれ、新しいサイロが出現する可能性があります。
アプリケーションとサービスには、おのおのに独自のプロビジョニング・メカニズムやID管理のためのシステムがあるため、新たに採用することで、アクセス・ポリシーおよびガバナンス・ポリシーが適用される方法に不整合が生じる可能性があります。組織全体でセキュリティを1か所で把握できないと、“IDのスプロール化”により、過剰特権が与えられたアカウントに気づけない可能性があります。

IDのスプロール化により、ユーザーの迅速なプロビジョニングとデプロビジョニングがより困難になり、一貫性のないエンタイトルメントやゴースト・アカウントが発生して、データ損失や侵害のリスクが増す可能性があります。また、一貫性のないユーザー・エクスペリエンスが生じる可能性もあります。Gartnerによると、侵害で最多の方法は資格証明の乱用によるもので、これはIDのスプロール化に対処するための戦略を持たない組織は侵害のリスクが高まることを示唆しています[3]。

IAMは、企業とそのユーザーおよびデバイスとの相互作用の中心に位置し、組織のデータおよびアプリケーションの“フロント・ドア”として機能します。しかし、クラウドおよびオンプレミス環境全体でID主導のポリシーの使用を拡張すると、IDの管理やエンド・ツー・エンドのガバナンスの達成が困難になります。

組織は、IDをITアーキテクチャの拡張のためのセキュリティ制御として位置付ける、統合されたIAMプラットフォームに移行しつつあります[4]。これらのプラットフォームは、セキュリティに対する一元管理されたアプローチを提供し、クラウドおよびオンプレミス・アプリケーション全体でのエンタイトルメントを管理することで、組織がIDのスプロール化を防止する支援をします。

[2] “2021 Technology Trends to Watch,” Enterprise Strategy Group, 2021 (PDF)
[3] Kasey Panetta, “The Top 8 Security and Risk Trends We’re Watching,” Gartner, November 15, 2021.
[4] 上記を参照

オラクルが他と異なる点

IDのスプロール化の制御を支援する統合されたIDプラットフォーム

オラクルは、ユーザーIDをセキュリティ境界として位置付け、組織がゼロ・トラスト・セキュリティ・アプローチを実行する支援を行う、統合されたクラウドIDソリューションを提供します。

適応型の多要素認証、アクセス管理、シングル・サインオン、IDライフサイクル管理を含むIAMソリューションおよび機能を使用して、人間および人間以外のIDの一般的なユースケースに対処します。

リスクに対応したエンド・ツー・エンドのユーザー認証とシングル・サインオンを提供することで、IDとシステムを統合し、いつでもどこからでもどんな方法でもアクセスを保護します。

エンタープライズ規模のIDサイロを統合型プラットフォームに統合することで、IDのスプロール化への対処に役立つクラウドベースのワークフローを用いた、IDおよびアクセス管理への統合型アプローチを実現します。

組織全体の可視化を向上させ、高度な認証を提供するIAMサービスにより、ライフサイクル管理を簡素化して、侵害のリスクを軽減します。

ポリシー管理を1か所で把握することで効率を向上させ、手動によるプロビジョニング・プロセスを、一貫性を向上させながら迅速かつ簡単に新しいアプリケーション、ユーザー、およびデバイスをオンボードするための管理しやすい単一のワークフローに置き換えます。

従来のソフトウェア提供のIAMソリューションや、ERPや人事管理システムなどの中核的なビジネス・アプリケーションからの既存のエンタイトルメントを使用して、新しいアプリケーション、ユーザー、およびデバイスを迅速にオンボードします。

「私たちは、Oracle Identity and Access Managementに多くの価値を見出しています。このセキュアでコスト効率に優れレジリエンスがあるソリューションにより、ユーザー・エクスペリエンスが向上した可用性の高いIDプラットフォームを提供できます。」

City and County of San Francisco、IAM and Directory Services Technical Director、Chinna Subramaniam氏

傾向

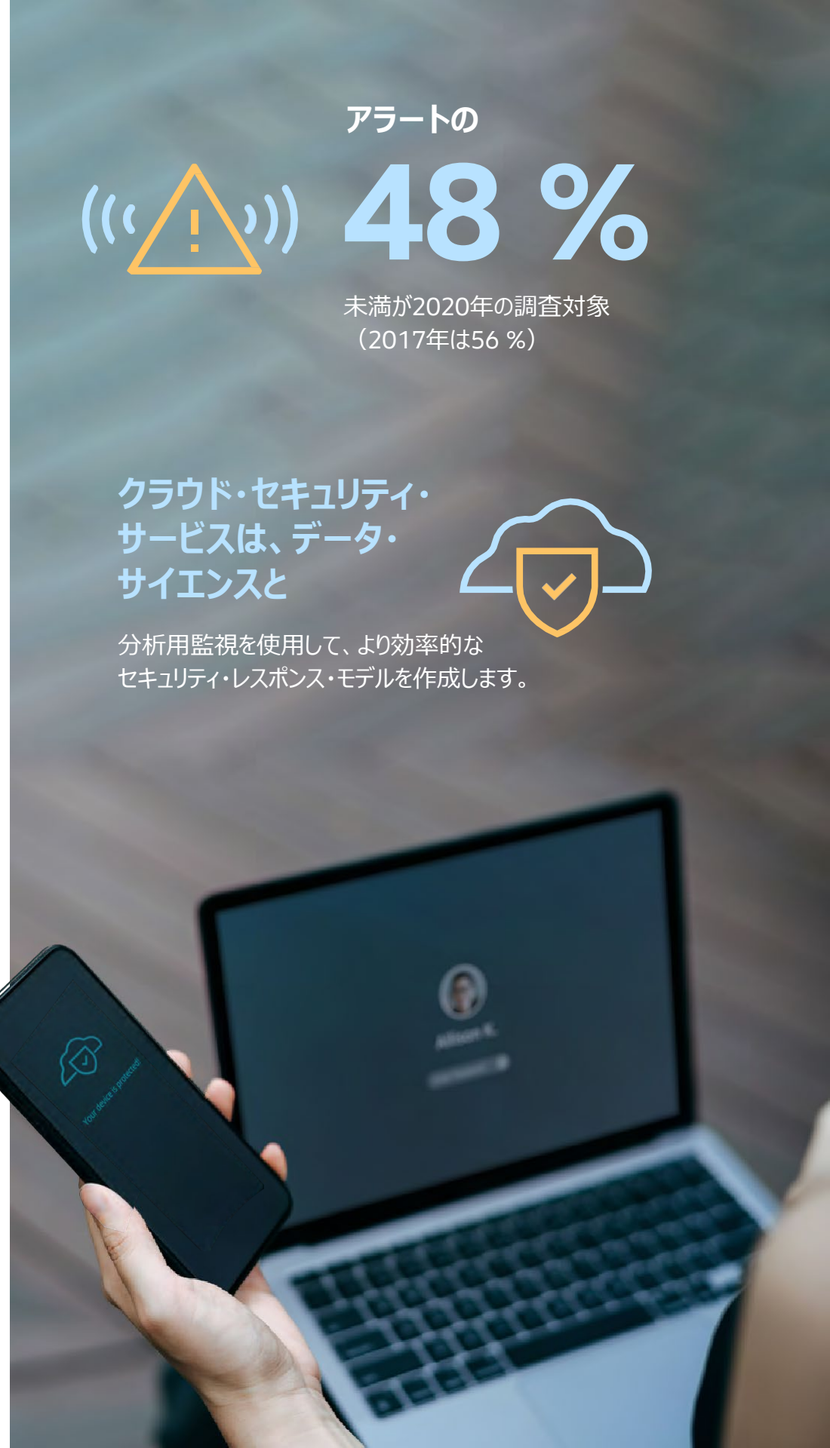
クラウド・サービスによる脅威の検出

組織は、より効率的に脅威を特定できるクラウド・サービスに移行しつつあります。

ITインフラストラクチャが拡大し、ビジネス・クリティカルなアプリケーションがパブリック・クラウドへ移動するにつれて、新たな脆弱性が明らかとなり、悪意のあるアクティビティによる組織のリスクが高まる可能性があります。リスクが高まるということは、生成されるアラートが増加し、すでに人員不足で極度の疲労状態にあるセキュリティ・チームにさらに圧力がかかることを意味します[5]。

Ciscoの"2020 CISO Benchmark Report"によると、多くの組織はアラートの調査において遅れています。レポートによると、2020年に調査されたアラートは48 %で、2017年の56 %と比べると減少しました[6]。セキュリティ・チームへの増加する負担を緩和するため、組織はクラウド・サービスに移行して、検出率を向上させ、侵害の影響を減少させ、およびリカバリにかかる時間を短縮しています。

クラウド・セキュリティ・サービスでは、データ・サイエンスと分析用監視を使用して、より効率的なセキュリティ・レスポンス・モデルを作成します。脅威の検出を組み合わせて表示することで、アラートの緊急性がより正確に反映され、異常を個々に調査する必要がなくなります。



[5] Kimberly Adams and Jesus Alvarado, "Cybersecurity professionals face burnout," Marketplace Tech, March 24, 2022, "2020 CISO
[6] Benchmark Report," Cisco, 2020

オラクルが他と異なる点

脅威の検出強化を支援するクラウド・インテリジェンス

Oracle Cloudの組込みセキュリティ機能およびサービスは、重要なワークロードの保護とセキュリティ態勢の強化に役立ちます。

Oracle Cloud Guardを使用して、Oracle Cloud Infrastructure（OCI）の顧客テナント全体のクラウド・セキュリティ状況を統合ビューで把握できます。

Oracle Threat Intelligence Serviceからの処方的かつ総合的な信頼性評価を用いて、脅威インテリジェンス・データを集計します。

MITRE ATT&CKフレームワークに沿った、ターゲットを絞った行動モデルを使用してアラートの優先順位を決定し、ノイズから有効なシグナルを選別して、Oracle Cloud Guard Threat Detectorによって悪意のある行動を検出します。

オラクルのWebアプリケーション・ファイアウォール・サービスにより、悪意のある攻撃や不要なインターネット・トラフィックからアプリケーションを保護します。

Oracle Cloud Infrastructure Vulnerability Scanning Serviceにより、ホストおよびコンテナ・イメージに潜在的な脆弱性がないかをチェックし、セキュリティの信頼性を高めてリスクを緩和します。

「Oracle Cloud Infrastructure Cloud Guardを使用することで、数多くの利点が得られます。最大の利点の1つは、検出から実際の対応、そしてセキュリティ・ポリシーの実施までを行えることです。」

Motorola Solutions、Senior Director of IT Infrastructure and Information Security、Scott Shepard氏

傾向

自動化の使用によるデータ損失のリスクの軽減

データ損失を防止するため、組織はクラウド・サービスに移行しています。そこでは、構成の自己更新、自己保護、および簡素化を行うテクノロジーによって人的エラーやインフラストラクチャの複雑さを軽減できます。

データ・インフラストラクチャ・セキュリティは、ITおよびセキュリティ部門のリーダーにとって引き続き重要な懸念事項です。データ損失のおもな原因は人的エラーと不適切な構成で、どちらもリモート・ワークの増加によって悪化してきました[7]。サービス、ユーザー、システム、およびイベントが増加する一方で、ITおよびセキュリティ部門の有能なスタッフは不足しており、組織には過剰なデータがあふれています[8]。そのためにITインフラストラクチャが複雑化したことで、新たなセキュリティ・リスクが生じる可能性があります。

PwCの調査によると、経営幹部の75 %が、自社組織が複雑すぎるためにサイバーセキュリティに関する懸念が生じていると回答しています[9]。しかし、複雑なインフラストラクチャによって生じる脅威はデータ侵害だけではありません。煩雑なインフラストラクチャに対処している組織も、運用面でのレジリエンス、サイバー攻撃からの迅速なリカバリ、および急速に変化する市場での迅速なイノベーションに対応できない場合があります。

より多くのイベントを分析し、不適切な構成に備えて事前に計画を立てて監視する必要性が増していることで、クラウドが解決に役立つ課題が生じています。組織は、スキルを備えた従業員の不足、サイバーセキュリティのスキルのギャップ、複雑化するITインフラストラクチャに対処しながら、構成の自己更新、自己保護、および簡素化を行うクラウド・サービスに移行しています。

75 %

の経営幹部が、

自社組織が複雑すぎるためにサイバーセキュリティに関する懸念が生じていると回答しています。

組織が移行しているクラウド・サービスでは

人的エラーやインフラストラクチャの複雑さを軽減できます。

[7] Tony Pepper, “Remote Working Is Here to Stay,” CPO Magazine, April 28, 2021
[8] Steve Morgan, “Top 6 Cybersecurity Predictions and Statistics for 2021 to 2025,” Cybercrime Magazine, December 30, 2021
[9] “Is your organization too complex to secure?,” PwC, 2022

オラクルが他と異なる点

自動化されたクラウド・セキュリティによる複雑さの軽減

オラクルは、包括的なサービスのセットを通じて、お客様がデータ侵害のリスクを緩和する支援を行うことに重点を置いています。

Oracle Autonomous DatabaseおよびOCIによる暗号化とユーザー行動の継続的な監視を使用してビジネスの保護を維持し、Oracle CASB Cloud Service およびOracle Cloud Infrastructure Identity and Access Managementによって さらにリスクを軽減します。

Oracle Cloud Guardで パブリック・アクセス可能な オブジェクト・ストレージなどの 一般的なセキュリティ面の課題の 修正を、セキュリティ・レシピを 使用することで自動化し、 セキュリティ・チームの運用 効率の向上を支援します。

Oracle Security ZonesによってOCIのセキュリティ・ポリシーを自動的に設定して適用し、ストレージ・バケットがインターネットを通じてアクセスできない不変ポリシーのようなクラウド・コンパートメントの人的エラーの回避を支援します。

「私がCloud Guardで気に入っているのは、継続的に稼働してより幅広いグループの従業員が使用できるため、当社のセキュリティ態勢に継続的な改善プロセスが提供される点です。OCIにも搭載されており、これは十分に価値があります。」

Darling Ingredients、Cyber Security Group、Threat Intelligence Lead、Tom Morgan氏

傾向

マルチクラウド・アプローチをサポートする階層化されたセキュリティ戦略

マルチクラウド・アプローチを採用する組織が増加しており、それらの組織は、クラウド・ネイティブ・サービスと、統合されたサード・パーティ・ツールを使用する、階層化されたセキュリティ戦略に移行しています。

クラウド・サービスに費やされる費用は2024年に1兆ドルを超え[10]、76 %の企業がマルチクラウドおよびハイブリッド・クラウド・アプローチを採用しています。マルチクラウド戦略は、ビジネス・プロセスおよびアプリケーションの最適化に役立つことが分かっています。しかし、階層化されたセキュリティ戦略がないと、このアプローチによって、統合されていないセキュリティ・ツールがクラウドに分散し、セキュリティ・ツールのスプロール化が生じる可能性があります。

セキュリティ・ツールが異なり、ベンダーが複数ある場合、セキュリティの運用が複雑化し、セキュリティの人員が増加することがあり、これによってコストのかかる非効率性、無効性、不要なセキュリティ・リスクが生じる可能性があります。オラクルとKPMGのレポートによると、組織は平均して100を超えるサイバーセキュリティ・ツールを使用しており、80 %が多数のセキュリティ・テクノロジーを1つのベンダーで統合することを検討しています。

組織は、サイバーセキュリティを統合し、俊敏性、スケーラビリティ、および効率を向上させるためにテクノロジー・スタックを再評価するにあたり、組込みセキュリティを備え、サード・パーティ・ベンダーとシームレスに統合できる製品とサービスを提供するクラウド・サービス・プロバイダ（CSP）を求めています。今日のセキュリティ・ツールも、マルチクラウドのデプロイメントを実施した組織が、接続されていないポイント製品が原因で生じる問題を簡単に修正できるように、異なるCSP間で機能する必要があります。

階層化されたセキュリティ戦略では、CSPが提供する組込みクラウド・セキュリティ・サービスを、プロバイダと一般的なイベント・モデルを統合して大規模にアラートを処理するビルトインAPIおよびCSPパートナーシップと組み合わせて使用することで、アプローチを簡素化できます。組織は、統合型パートナーシップとベンダー統合の機会の領域を追求し続けており、おもなCSPは階層化されたアプローチをサポートするために、組込みセキュリティ、およびサード・パーティ・ベンダーとの技術面の統合を強化し続けるとみられます。

[10]"IDC Forecasts Worldwide "Whole Cloud" Spending to Reach $1.3 Trillion by 2025", IDC, September 14, 2021

オラクルが他と異なる点

クラウド・セキュリティの複数のレイヤー

オラクルは、クラウド・ネイティブのセキュリティ、組込みセキュリティ・アーキテクチャおよびサービス、パートナーおよび他のCSPへの接続を提供します。

オラクルのネイティブ・セキュリティ制御を容易に実装し、Autonomous DatabaseおよびOCIによる暗号化とユーザー行動の継続的な監視を使用して、不適切な構成によるエラーを防ぎ、拡大した攻撃対象領域を保護します。

単一のIdentity and Access Managementサービスによってクラウドからオンプレミス環境までセキュリティを拡張し、クラウド・ネイティブのIdentity-as-a-Serviceプラットフォームを用いてユーザー・アクセスおよびエンタイトルメントを管理します。

マルチクラウド設計を採用することによってCloud Security Notification Framework（CSNF）のようなアラートの共通情報モデルを確立し、Open Community Networking User Group（ONUG）の活動を通じてOracle Cloud Guardと統合します。

OCIによって、データベース・サービス、広範な監視機能、および組織の要件に合致する戦略的なパートナーシップを含むマルチクラウド・ソリューションの包括的なセットにアクセスします。

傾向

サイバーセキュリティの知識を備えた企業役員

ビジネス・プロセスを中断させる可能性があるサイバー攻撃が発生する頻度は増しており、企業の取締役会ではサイバーセキュリティに関するリスクの意識と理解が進んでいます。

サイバー攻撃はより高度になり、コストも増加しています。2025年までに、サイバー犯罪による被害額は年間10.5兆ドルに達すると予想されています[11]。また、2031年までに、ランサムウェア攻撃は2秒おきに発生すると予想されています[12]。サイバー攻撃の頻度が増え続けており、組織は、ビジネスにより良い助言を与え、企業、消費者、およびパートナーの情報を保護するために、サイバーセキュリティに関する深い知識を備えた新しい役員を加えることで対応しています[13]。

サイバー攻撃には迅速なアクションが必要です。場合によっては数秒の内にレスポンスが求められます。Ponemon Instituteによる調査では、セキュリティ侵害が組織に与えた被害額は2021年に平均でインシデントあたり424万ドルと推定されており、2019年から10 %増加しました14。レポートで調査された侵害のほぼ半数で、顧客の個人情報（PII）が漏洩していました。
機密情報を狙う侵害の可能性により、サイバーセキュリティが戦略およびリスク管理のおもな焦点となっています。取締役会にサイバーセキュリティの専門家がいないと、侵害による影響に対する行動を即時に起こせずに、ビジネス・グループ、顧客、パートナー、およびブランド評価に悪影響が及ぶ可能性があります。

サイバー脅威に対して効果的に準備をして対応するには、取締役会は組織のデータ資産、サイバーリスク、インシデント対応計画、規制および法的義務についての理解を備えていなければならず、これらの問題について定期的に議論する準備をしておく必要があります。サイバーセキュリティに関する知識を持つ役員は、ビジネスに助言を与え、組織、顧客、株主に影響を与え得る混乱や損失のリスクを軽減する、適切な意思決定を行うことができます。

[11] Steve Morgan, “Cybercrime to Cost the World $10.5 Trillion Annually by 2025,” Cybercrime Magazine, November 13, 2021
[12] David Braue, “Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031,” Cybercrime Magazine, June 2, 2022.
[13] Kasey Panetta, “The Top 8 Security and Risk Trends We’re Watching,” Gartner, November 15, 2021,
[14] Abi Tyas Tunggal, “What Is the Cost of a Data Breach in 2022,” UpGuard, May 12, 2022

オラクルが他と異なる点

取締役会でのセキュリティ面の最大懸念事項への対応を支援するソリューション

オラクルは、セキュリティ部門のリーダーが取締役会にインサイトを提供できる、シンプルかつ処方的で統合されたセキュリティ機能の包括的なセットを提供することで、組織がリスクを軽減する支援を行うことに重点を置いています。

セキュリティ：オラクルには、何十年にもわたってデータとアプリケーションを保護してきた実績があります。Oracle Cloudは、組織のインフラストラクチャ、アプリケーション、およびデータをサイバー攻撃から保護し、コンプライアンス指令を遵守する支援ができる組込みセキュリティを備えています。

データ・プライバシー：オラクルは、Oracle Cloud Infrastructureのプライバシー機能により、お客様がデータ・プライバシーの原則に準拠する支援を行います。

コンプライアンス：オラクルは、Oracle Cloudを監査し、お客様がグローバル、地域、および業界特有の認証の遵守に対応できるようにするための多数のプログラムを遂行しています。

次のクラウド・セキュリティ

変化するITインフラストラクチャおよびビジネスの要件に応じてセキュリティ戦略は進化し続けており、シンプルなセキュリティ・ソリューションの必要性は明らかです。
また、ITイノベーションに匹敵する精巧さとスピードでサイバー攻撃が増加しているため、セキュリティは組織のあらゆるレベルから注目を集め続けることになります。

一歩先を行くために、ITおよびセキュリティ部門のリーダーは、クラウド・サービスによってサイバー脅威を上回り、複雑さを軽減し、重要なビジネス資産を保護しようとしています。
クラウドと、経営陣や役員からの増加するサポートに支えられて、ITおよびセキュリティ部門のリーダーは、組織全体のセキュリティを革新して強化する新しい機会を得ています。

Oracle Cloud Free Tierを試す

Oracle Cloudを使用して
セキュリティを簡素化する方法を見る

詳細を見る

Oracle Cloud Infrastructure
のセキュリティの詳細情報

詳細情報

クラウド戦略インサイトの詳細

詳細情報

ORACLE