

Acronis Cyber Protect

















Acronis

サイバーセキュリティ、データ保護およびエンドポイント管理を統合

AI 搭載コンソールで、バックアップ、ディザスタリカバリ、サイバーセキュリティの重要機能を集中管理し自動化します。

サイバーセキュリティ	(追加) バックアップとリカバリ	(追加) エンドポイント管理	(追加) 自動化
<ul style="list-style-type: none">EDR の Linux 対応 <small>新登場</small>振る舞いベースのマルウェア対策 /AV業界トップクラスのランサムウェア対策URL フィルタリングバックアップのスキャンと修復でマルウェアと脆弱性に対処ウイルスとマルウェアに対するバックアップスキャンと修復	<ul style="list-style-type: none">バックアップ: システムイメージ、ファイルをベアメタルや構成の異なるハードウェアに復旧ディザスタリカバリGoogle Workspace および Microsoft 365 のバックアップ用容量無制限のクラウドストレージ不変ストレージエージェントレスおよびエージェントベースのパブリックVMのバックアップAzure VM 向けエージェントレスバックアップOne-Click Recovery™バックアップの公証とチェックサム整合性の検証アーカイブ内の重複除外複数の保存先へのバックアップレプリケーションEメールアーカイブ <small>新登場</small>Nutanix 向けエージェントレスバックアップ <small>新登場</small>	<ul style="list-style-type: none">セキュアなリモートデスクトップアクセスとサポートハードウェアとソフトウェアのインベントリ脆弱性スキャンフェールセーフパッチの適用によるパッチ管理: パッチのインストール前にエンドポイントをバックアップMicrosoft Defender および Security Essentials の管理リモートデバイスワイプ	<ul style="list-style-type: none">エンドポイントの自動検出リモートエージェントのインストールを自動化AI を活用したサイバースクリプティングによるルーティンタスクの自動化機械学習を活用した監視と、ハードウェア、ソフトウェアおよびネットワークリソースの監視アラート

Acronis Cyber Protect は、以下のプラットフォームとアプリケーションに対応しています。

									
Azure	Windows Server	Windows PC	Exchange	SQL Server	SharePoint	Active Directory	Hyper-V	Microsoft 365	Google Workspace
									
Amazon EC2	Linux Server	Mac	iPhone	iPad	Android	SAP HANA	MariaDB	MySQL	
									
VMware vSphere	Oracle x86 VM Server	Oracle Database	Red Hat Virtualization	Linux KVM	Citrix Hypervisor	Virtuozzo	Nutanix	Synology	

NIST サイバーセキュリティフレームワーク (CSF) 2.0 を網羅した、 包括的エンドツーエンドのサイバーレジリエンス

統治				
特定	保護	検知	対応	復元
<ul style="list-style-type: none"> ハードウェアとソフトウェアのインベントリを最新の状態に維持します。 新しいデバイスを自動的に検出します。 システムのスキャンによって、脆弱性を検出します。 企業全体の保護ステータスを、データ保護マップを通じて一目で把握できるようにします。 バックアップのオフラインマルウェアスキャンによる、エンドポイントのパフォーマンスを向上。 	<ul style="list-style-type: none"> 企業全体で、あらゆるハードウェアプラットフォーム、OS、アプリケーション、データベースおよびクラウドリソースを保護します。 自動化されたリモートエージェントインストールにより、新しいリソースを迅速に保護します。 グループ管理ポリシーを構築およびカスタマイズします。 必要な場合には迅速なローカルバックアップが可能、パッチ適用前の自動バックアップで、リスクのないパッチ適用が可能になります。 不変ストレージによって、人為的なミスや悪意ある攻撃によるバックアップの損失を防止します。 	<ul style="list-style-type: none"> 振る舞いベースのマルウェア対策により、ランサムウェアなどの未知の脅威や高度な脅威を検出します。 ハードウェア、アプリケーションおよびネットワークリソースの健全性を監視します。 アプリケーションの許可リストを通じて、高性能な脅威検出を最適化します。 	<ul style="list-style-type: none"> ランサムウェアの脅威を自動的に終了させ、暗号データをローカルファイルのキャッシュからロールバックします。 エンドポイント全体での IOC 相関により、潜んでいる、持続的な脅威を検出します。 インシデント対応を迅速に優先順位付けします。 脅威の隔離/修復を行います。 バックアップ内のフォレンジックデータを収集し、インシデント後の脆弱性分析を行います。 Acronis Threat Research Unit (TRU) からのアラートを受信すると、パッチ適用、スキャンおよびバックアップが自動的に開始されます。 Microsoft 365 向け E メールアーカイブで、電子情報開示とコンプライアンスを簡素化。 	<ul style="list-style-type: none"> 迅速で柔軟なリカバリによって、データ損失からの復元を実現します。 IT 部門のサポートが無くても、One-Click Recovery™により、ローカルのユーザーが数分で復元を開始できるようになります。 広範な障害のあとも、ディザスタリカバリにより、ビジネスを迅速に再開できるようになります。 マルウェアと脆弱性に対するバックアップのスキャンと修復により、安全なリカバリが確保されます。

Acronis Cyber Protect 独自の強み

バックアップ

- 柔軟なバックアップストレージのオプションには、ローカルの HDD、SSD、テープ、SAN、NAS、プライベートクラウド、Acronis Cloud および主要なパブリッククラウドプロバイダーが含まれています。
- イメージベースバックアップと異なるハードウェアへの復元により、旧式のオペレーティングシステムを実行しているレガシーのワークステーションやサーバーを保護できます。
- 異なるシステムタイプ間でのバックアップと復元では、Acronis Instant Restore が有効化され、障害を発生した物理的サーバーを数秒でフェールオーバーさせ、レプリカの VM を準備できるようになります。
- Acronis One-Click Recovery により、IT 部門のサポートがなくても、あらゆるユーザーが障害を発生したエンドポイントを再構築できるようになります。
- Microsoft 365 および Google Workspace のバックアップが検索可能になっているため、メールボックス全体やアカウント全体を復元する必要なく、個々のファイル、Eメール、チャット、および他のリソースを復元できます。
- Acronis Cyber Protect には、Acronis Cloud で Microsoft 365 および Google Workspace のバックアップを保存できる、容量無制限のストレージが付属します。

サイバーセキュリティとエンドポイント管理

- エンドポイントでは、サイバーセキュリティ、データ保護および管理を単一のエージェントで行えるため、性能が向上し、複数ベンダー間の競合が解消されます。
- 1つのコンソールですべての管理機能に対応できるため、カスタマイズされた保護計画や新しい技術者の迅速なオンボーディングといった、IT 効率の向上が可能になります。
- セキュアなリモートデスクトップとアシスタンスにより、IT スタッフは、Windows、macOS および Linux エンドポイントの監視、構成およびトラブルシューティングをリモートで行える、パワフルなツールを得られるようになります。
- 包括的なインベントリツールにより、ハードウェアおよびソフトウェアのすべてのアセットの検出、追跡およびレポート自動的に行えるようになります。
- サイバースクリプティングにより、IT メンテナンスでのルーティンタスクをオフロードできるようになります。事前に作成されたスクリプトを手動で、あるいは AI のサポートで最適化することができます。
- 機械学習を活用した監視とアラートにより、IT 部門は、アクロニス 製品およびサードパーティ製のセキュリティ、ストレージおよびネットワークリソースの性能や可用性に関する問題を予測できるようになります。
- 柔軟な VM 保護オプションには、エージェントベースの管理とエージェントレスの管理が含まれます。