Application Control for Windows Servers

役割ベースのユーザーアクセスで Windows サーバーの安全を確保

Ivanti® Application Control for Windows Servers を使用すると、特定の業務に関連するタスクを実行するためにサーバーにログオンする必要があるユーザーの管理者権限を制限し、サーバーへのアクセスを制御し、リスクを軽減できます。これは多目的（例：SQL と IIS）で複数の管理者権限を持つユーザーによってサーバーが使用されている場合や、企業がコンピューティングインフラストラクチャのセキュリティプラクティスの規制に従う必要がある場合、特に有効です。

サーバーログオン時にユーザーの権限を特定のタスクのみを実行できる権限に制限する

Ivanti Application Control for Windows Servers を使用することで、IT 部門は管理者権限を特定のコンソールやアプリケーション、サービスやコマンドに制限でき、管理者に起因するマルウェアのリスク、基幹サービスの中断、ミッションクリティカルなパフォーマンスへの影響を軽減できます。

権限の昇格

適切なトレーニングを受けていないユーザーにサーバーでフル管理者権限を付与することは、誤ってサービスを開始/停止する、ソフトウェアをインストール/アンインストールするなどさまざまなリスクにつながります。これは、セキュリティのリスクの増大や管理費の増加、生産性の低下につながり、法的責任の問題に発展し、コンプライアンス遵守を難しくさせる可能性があります。ユーザーからフル管理者権限を除去し、担当業務に必要なタスクのみにアクセスできる権限昇格をユーザーに付与することで、エンドポイントの安全性を簡単に確保し、サポートへの問い合わせ電話の件数を軽減し、TCO（総所有コスト）を削減できます。

Application Control

Ivanti Application Control for Windows Servers を使用すると、アプリケーションのホワイトリストに基づく、サーバーアプリケーション、サービス、コンポーネントへの権限が付与されたアクセスが可能となります。Application Control を使用することで、IT 部門はファイルの整合性を確保するため SHA-1、SHA-256、または ADLER32 デジタル署名を割り当てることができます。さらに、IT 部門はベンダー、証明書、発行元、バージョンなどファイルのメタデータも確認できるため、アプリケーション、コンポーネント、スクリプトが正規のものであることを保証し、改竄されたアプリケーションやなりすましのアプリケーションの実行を防ぐことができます。

System Controls による保護

特定のサービスへのアクセス権を昇格または制御するために System Controls を適用することで、サーバーアプリケーションやプロセスの削除や変更や、指定されたイベントログの削除を防ぐことができます。

アプリケーションのブラックリスト化

重要なアプリケーションやサーバーオペレーティングシステムのコンポーネントへの管理者のアクセスを管理するため速やかにブラックリストを適用します。ブラックリスト化することで、重要なサーバーリソースが変更されることを防ぎ、データセンター内でサーバー保護を強化できます。

コマンドラインのマッチング

Application Control for Windows Servers を使用することで、実行中のアプリケーションやそれに関連するコマンドライン引数にセキュリティポリシーを適用できます。サーバー環境にある Windows PowerShell などのアプリケーションに対して、管理者アクセスを特定のファイルとスクリプトの実行のみ可能な権限や、特定の条件下でアプリケーションの実行のみ可能な権限に制限できます。

Application Network Access Control

この機能は、ルーター、スイッチ、ファイアウォールなど複雑な制御を導入することなく、ネットワークへのアクセスを防ぎます。保護されているデータセンターやネットワークリソースに特定のサーバーからアクセスする権限を持つ IT 部門の管理者に起因するセキュリティの脆弱性を排除できます。

コンディション管理

Application Control は、ログオンしているユーザーの状況に基づいてサーバーリソースへのアクセスを管理するため、広範にわたるコンディションチェックを実施します。コンディションに応じてリソースやアプリケーションにアクセスできます。状況の評価には、ユーザー、グループまたは OU メンバー、デバイス名、デバイス IP や MAC アドレス、接続中のクライアント情報、オペレーティングシステム、サイトメンバー、日時に加え、PowerShell や VBscript、Jscript を使って作成されたカスタムルールなどに限定されません。さらに、Microsoft RDSH、Citrix XenApp、Citrix XenServer、VMware のサポートが完全装備されているため、リモートのセッションにもセキュリティポリシーを適用できます。