aruba
a Hewlett Packard Enterprise company

ITセキュリティギャップの解消:

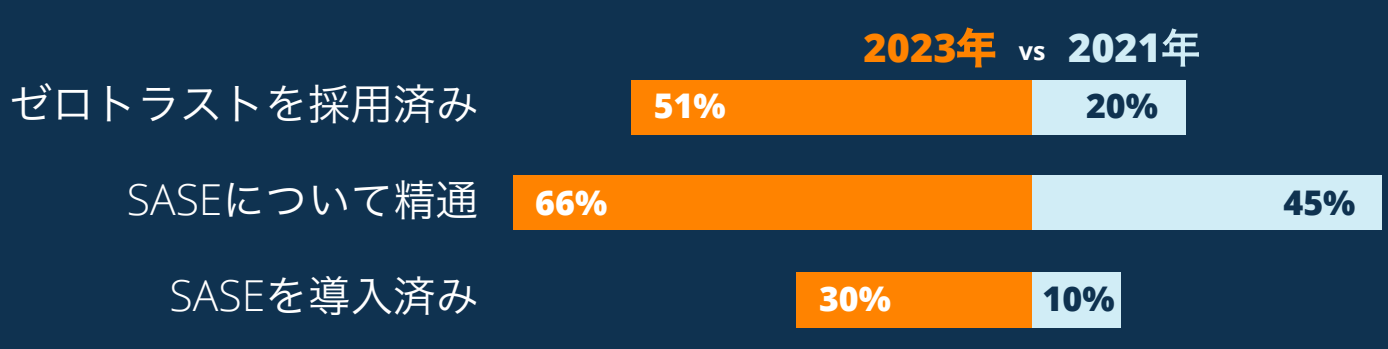
2023年におけるゼロトラストとSASEセキュリティアーキテクチャーの導入状況

ハイブリッドワークの増加、IoTの利用拡大、容赦ないサイバー攻撃などにより、組織が直面するセキュリティの課題はかつてないほど増大しています。新たな課題の登場は、新しいセキュリティモデルの採用を促しています。ゼロトラストとSASE (セキュアアクセスサービスエッジ) アーキテクチャーには、以下の実現を期待できます。

- エッジからクラウドまでのセキュリティの組み込み
- リソースに対して最小権限のアクセスを動的に適用してサイバーリスクを低減
- あらゆる場所からエンタープライズアプリケーションに安全に接続

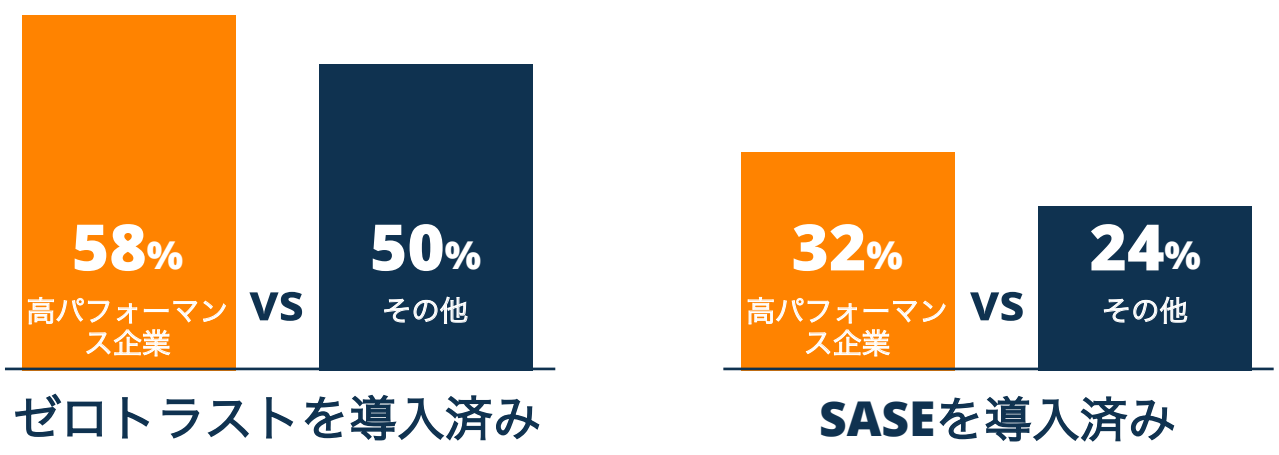
セキュリティアーキテクチャーはどのように変化しているのでしょうか?

この2年間で、ゼロトラストとSASEセキュリティの採用が加速しています。
貴社も先手を打てているでしょうか?



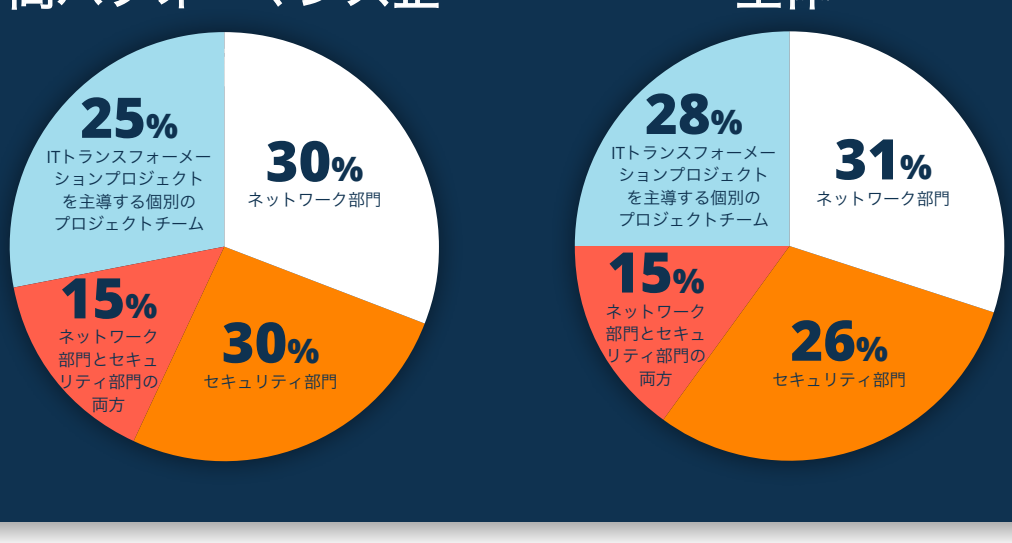
高パフォーマンス企業はどこが違うのでしょうか?

高パフォーマンス企業では、ゼロトラストと
SASEアーキテクチャーを導入する傾向が強まっています。



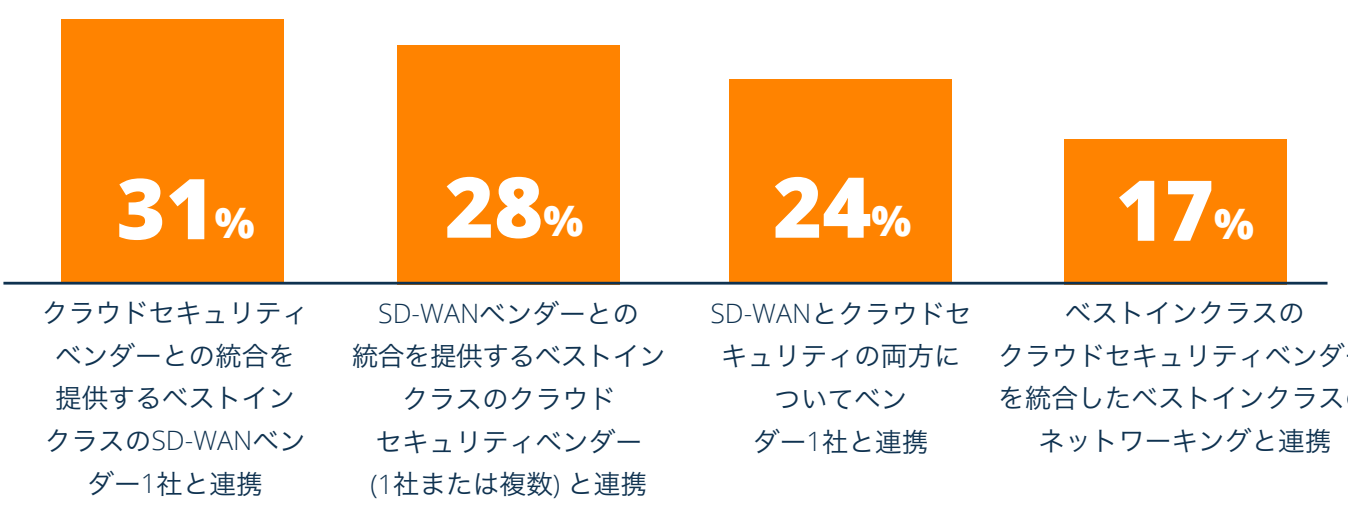
セキュリティアーキテクチャーに関する意思決定を行っているのは誰ですか?

多くの組織でネットワーク部門がセキュリティ上の意思決定を主導していますが、
ITトランスフォーメーションプロジェクトを主導する
個別のプロジェクトチームが意思決定を行う組織も登場しています。



新しいセキュリティアーキテクチャーの導入をご検討中ですか?

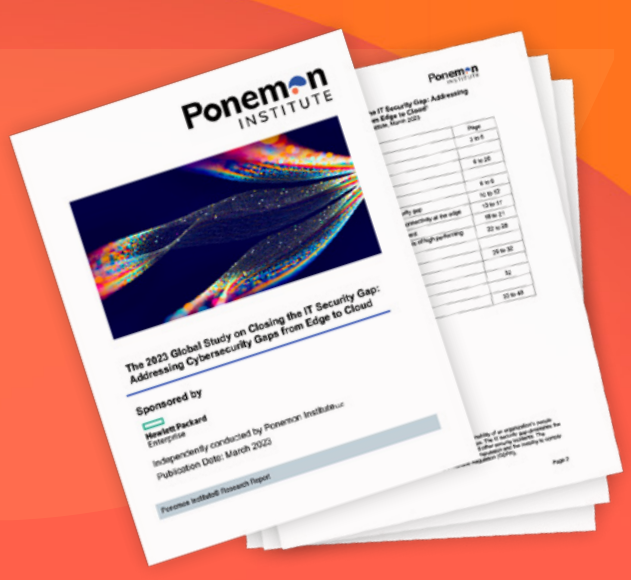
SASEアーキテクチャーの導入にあたってどのベンダーを選択するかという問いに対しては、
ベストインクラスのSD-WAN、ベストインクラスのクラウドセキュリティ、
またはシングルベンダーによるSD-WANとクラウドセキュリティ、
と回答した組織がほぼ同程度の割合で見られました。



先進的でセキュアなSD-WANと最善のSSE (セキュリティサービスエッジ) 機能を組み合わせることは、既存のネットワークやセキュリティインフラストラクチャにクラウドベースのセキュリティサービスを組み込むための効果的な方法ですが、シングルベンダーのアプローチをとれば、大幅にシンプル化できる可能性があります。

レポート全文で以下の内容をご確認いただけます。

- ゼロトラストおよび**SASE**ソリューションの採用率と導入スタイル
- **IT**セキュリティ上のギャップを解消するうえでゼロトラストと**SASE**が果たす役割
- **IT**セキュリティ上のギャップを解消するうえでの可視化の重要性
- 高効率のネットワークセキュリティと実装環境を持つ組織と比較した場合のゼロトラストおよび**SASE**フレームワーク導入に向けた手順



レポートを読む →

aruba
a Hewlett Packard Enterprise company