PICUS

BAS（Breach & Attack Simulation）

「自動化されたサイバー脅威のシミュレーション及び軽減」を可能にする継続的なセキュリティ検証ソフトウェア

Picusは、新たな脅威のサンプルを使用して、新たな脅威に対する顧客の準備態勢に継続的に挑み、セキュリティ対策の長所及び短所をリアルタイムで特定し、ユーザがセキュリティ投資を最大限に生かすのを支援します！

主なメリット

●セキュリティテクノロジーに挑む

セキュリティチームがサイバー犯罪者よりも前に実際の攻撃を用いてセキュリティコントロールに挑むことを可能にします。

●セキュリティギャップを特定する

セキュリティギャップをリアルタイムで特定し、Picus軽減ガイダンスを用いて数分で措置を講じます。

●セキュリティインフラを最大限に利用する

Picusは、企業がわずか数週間で脅威阻止の成功率を倍増させ、その成功率を持続させるのを支援します。

●運用効率

リアルタイムの特定
セキュリティギャップの迅速な解決

● ハッカーは既知の方法を使用して迂回する

現在、セキュリティ市場は、2018年末までに96億米ドルに達すると予測されています(*1)。この成長にもかかわらず、セキュリティ侵害は依然として増加しています。今後2年間でデータ侵害が繰り返される可能性は27.7%です(*2)。
「新しい高度なテクノロジーや計画的な運用の取り組みがこの傾向を遅らせていないのは何故か?」という明らかな疑問が生じます。

● 十分に活用されていないセキュリティ投資

企業は、リソースが限られていることや、複雑なセキュリティテクノロジーを微調整するのに専門知識が必要になることが原因で、セキュリティ投資を十分に活用していません。
運用コストは、増大するデバイスリストを維持するために絶えず増加しており、最終的には重荷になります。

● 誤った安心感

良く知られているセキュリティソリューションに投資・装備した後、多くの企業はサイバー攻撃の影響を受けないと考えます。
しかし、メトリック（評価基準や指標）がなければ、ソリューションがどれだけセキュリティ態勢に貢献しているかを知ることは不可能です。

● 従来のツール及びサービスを超える

企業は、サイバー攻撃に対する準備態勢を測定するためには、その時点でセキュリティツール等を使用したサービス以上のことを行う必要があります。

セキュリティ態勢をロバストに維持することは、持続的なプロセスでなければなりません。今、その継続的なセキュリティ検証ソリューションがPicusプラットフォームによって可能になります！

SIEM Integration

splunk> IBM QRadar
ArcSight An HP Company
McAfee Together is power. nitrosecurity
LogRhythm
And other SIEM Providers

Technology Alliances

paloalto NETWORKS
FORTINET
cisco Solution Partner
Check Point SOFTWARE TECHNOLOGIES LTD.
McAfee Together is power.
TREND MICRO
f5 NETWORKS
CITRIX
SNORT

Gartner COOL VENDOR 2019

© Picus Security, 2019.
415 Jackson St., Suite B,
San Francisco, CA 94111 USA
info@picussecurity.com
www.picussecurity.com

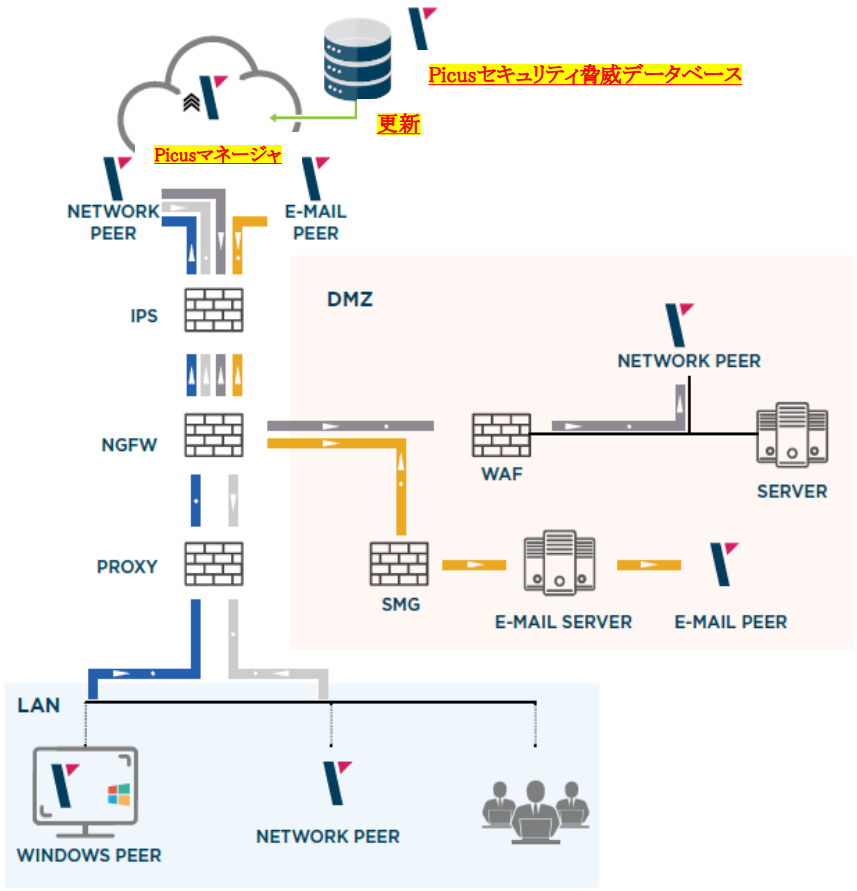
コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

Picusの動作原理

Picusは、セキュリティコントロールにおけるギャップを特定し、軽減オプションを提示するように設計されています。これらを果たす為に、Picusは4段階のアプローチを取ります。

実環境で動作！

- **展開**
  数時間でオフザシェルフのPicusソフトウェアソリューションをインストール・設定します。
  展開後、ユーザはわずか数分以内に結果を得られます。
- **評価**
  セキュリティギャップをリアルタイムで特定し、Picus軽減ガイダンスを用いて数分で措置を講じます。
- **測定**
  インタラクティブなダッシュボードは、客観的なメトリックを用いて全体像をキャプチャし、明らかになったギャップをリストアップします。
- **軽減**
  評価中に明らかになったギャップについて、Picusはベンダ固有の修復シグネチャを提供し、実用的な優先順位付けリストを作成します。



Picus セキュリティラボ

Picusラボは、新たな脅威を特定して即時の対応を提供するだけでなく、攻撃側セキュリティチームと防御側セキュリティチームの間のギャップを埋めます。

レッドチームが新たな脅威を解析、分類、検証しているとき、ブルーチームはセキュリティテクノロジーが新たな脅威に対してどのように動作するかを特定します。

Picus脅威データベースは、以下の攻撃カテゴリーを特に重視した現実の脅威のサンプルで構成されています。

・脆弱性のエクスプロイト
・マルウェア
・ウェブアプリケーション攻撃
・データ漏洩

Picusを採用する主な理由

- **セキュリティコントロールを重視**
  従来のサービス及びツールは脆弱性の特定に重点を置いていますが、Picusはセキュリティデバイスの効率性に重点を置いています。
- **全ての防止ソリューションに有効**
  標準的なセキュリティデバイス設定テストソリューションでは、IPS、WAF、サンドボックスツール及びプロキシなどのアプリケーションレイヤセキュリティデバイス向けに提供されるものが限られています。
- **プロダクション環境にリスクのない評価**
  大型のセキュリティデバイステストアプライアンスは、ラボ環境におけるセキュリティデバイスの負荷/有効性テストに重点を置いています。

これに対し、容易な展開及び使用が可能なPicusソリューションは、**実環境で動作**するように設計されています。

*1) (Gartner Inc., Press Release, 2017)。
*2) (Ponemon Institute, Cost of Data Breach Study, 2017)

Picus Security Inc

2013年に設立以来、BAS(Breach & Attack Simulation) テクノロジーのパイオニアであるPicusはITセキュリティ分野に斬新、且つ全体的なアプローチである“継続的なセキュリティ検証”を開発しました。ベンダーやテクノロジーに関係なく、比類のないPicusプラットフォームは、本番環境で新たな脅威のサンプルを使用して、セキュリティ防御の効果を継続的に測定するように設計されており、既に多くの多国籍企業や政府機関に実績を有し、信頼されています。
本社はアメリカ（サンフランシスコ）にあり、拠点はトルコ、英国、ドイツ、中近東、メキシコにあります。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp