KEYSIGHT TECHNOLOGIES

ネットワークパフォーマンスとセキュリティ製品カタログ

目次

ダイナミック・ネットワーク・インテリジェンスで攻撃を回避し最高のパフォーマンスを確保

ネットワークでは多くのことが発生します。ユーザーをセキュアに接続させ、重要なアプリケーションを保護し、機密データを保護する必要があります。ネットワークの稼働時間、ユーザーエクスペリエンス、セキュリティはこれまで以上に重要ですが、サービスの中断を最小限に抑え、攻撃を防ぐことはかつてないほど困難になっています。

- 分散ネットワークアプリケーション、エッジコンピューティング、およびSD-WANは、すべてを一元管理することを困難にしています。
- 在宅勤務により分散した従業員が増えたことで、攻撃対象領域が増えて、一貫したサービス品質（QoS）を維持することを困難にします。
- 誤って構成されたツールは攻撃者によって絶えず悪用され、それがパフォーマンスの問題にもつながります。

信頼できる情報源が必要です。そこでキーサイトが役立ちます。アプリケーションと脅威インテリジェンスの世界的リーダーとして、キーサイトは、クラウド、仮想、オンプレミスのインフラストラクチャにまたがるネットワークの隅々からプロアクティブな知見とリアルタイム分析の組み合わせを提供し、お客様からの信頼を得ています。この動的なネットワークインテリジェンスを利用すると、パフォーマンスの問題を防ぎ、攻撃回避が簡単になります。

セキュリティやユーザーエクスペリエンスを脅かすような問題を事前に回避してください。当社のネットワークパフォーマンスおよびセキュリティ製品を発見して、フォーチュン100社のうち77社がダイナミック・ネットワーク・インテリジェンスに依存している理由を確認してください。

ダイナミック・ネットワーク・インテリジェンスとは何でしょうか？

電子ブックをダウンロード（英語）

攻撃される前に自社環境を検証してください。Keysight Threat Simulatorが、セキュリティ運用の脆弱性の特定と修正にどのように役立つかをご覧ください。

紹介ビデオを視聴

Threat Simulator: Breach and Attack Simulationプラットフォーム

セキュリティは決して静的ではありません。新しい脅威は常に存在し、設定ミスはネットワークを瞬時に危険にさらす可能性があります。直感に反するように聞こえるかもしれませんが、他の誰かが攻撃する前に、自分自身を攻撃する必要があります。本番ネットワークでキルチェーン全体を安全にシミュレートすることで、リスクを確実に測定し、ギャップを明らかにし、段階的に軌道修正できます。

キーサイトのThreat Simulatorは、脅威インテリジェンスとセキュリティテストにおける20年以上のリーダーシップに基づいて構築されており、セキュリティ有効性を継続的に検証し、以前よりも安全であることを簡単に確認できます。SIEM統合と脅威インテリジェンスデータベースからの年中無休の更新により、Threat Simulatorは、セキュリティ運用（SecOps）チームが急速に変化する攻撃対象領域を制御できるようにします。

導入	ライセンス	攻撃シミュレーション	検証対象ツール	SIEM 連携	アップデート頻度	ツール特有の改善提案	本番ネットワークの安全な検証	自動検証
Software-as-a-Service (SaaS)	Annual	Malware, spear phishing, cross-site scripting, data exfiltration, database exploits, advanced persistent threats, cryptojacking, MITRE ATT&CK Tactics & Technics, and more	WAF, IDS, IPS, DLP, URL filtering, gateway antivirus, malware sandbox, EDR, Email Gateway	IBM QRadar, Splunk	Continuous updates to attack library from Keysight Application and Threat Intelligence (ATI) Research Center	✓	✓	✓

詳細情報

THREAT SIMULATOR

直感的な製品ダッシュボードを使用して、ネットワークセキュリティの有効性を一目で確認できます

いつでもどれだけ安全かをスコアで確認できます

詳細を掘り下げて、セキュリティ検証で合格している検査と、問題が発生している検査を確認します

ThreatARMOR:
脅威インテリジェンスゲートウェイ

攻撃者は粘り強いですが、完璧ではありません。多くの脅威は予防可能ですが、侵害は相変わらず蔓延しています。SecOpsチームは攻撃を防ぐためにたゆまぬ努力をしていますが、SIEMアラート量は膨大であり、重要な手がかりを見逃すことがよくあります。

攻撃対象領域を減らす必要があります。それは攻撃者がネットワークに侵入するのを防ぐことで実現できます。だからこそ、SecOpsチームはThreatARMORを利用して、悪意のあるIPトラフィックが最初からネットワークにアクセスするのを防いでいます。悪意のある攻撃者がファイアウォールフィルターを絶えず回避しているため、ThreatARMORなどの脅威インテリジェンスゲートウェイは、既知の攻撃者の継続的に更新されるデータベースを利用して、動作ではなく場所ごとに脅威をブロックする、より回復力のある防御を提供します。

紹介ビデオを視聴

導入	管理と操作	対応スピード	インバウンド IPブロッキング	アウトバウンド IPブロッキング	フェールセーフ冗長	ラインレートパフォーマンス	悪意のある活動の防御	テクニカルサポート
On-premises (1RU)	Web-based controller with integrated metrics dashboard	1 G, 10 G	Known-bad sites and untrusted locations	Botnet communication from infected internal systems	Built-in bypass mode and dual-redundant power supplies	✓	✓	✓

詳細情報

THREATARMOR

保護スコアは、ネットワークの安全性を正確に示します。分析は不要です

脅威がどこから来ているかを確認し、ラインレートでブロックします

業界をリードする脅威インテリジェンスの知見で、セキュリティ防御力を向上

セキュリティに関しては、遅れをとる余裕はありません。ThreatARMORとThreat Simulatorは、業界をリードする何十年にもわたる専門知識に基づいて構築されたキーサイトのアプリケーションおよび脅威インテリジェンス（ATI）リサーチセンターによって支えられています。グローバルセキュリティ研究者のエリートグループは、SecOpsチームを最新の既知の脅威とエクスプロイトで最新の状態に保ちます。私たちのデータベースには5000万を超えるレコードが含まれており、毎月何百万もの新しい脅威が分析およびカタログ化されています。

最新の攻撃をエミュレートする場合でも、新たな脅威がネットワークに足場を築くのを防ぐ場合でも、チームがKeysight ATIの一歩先を行くと信じることができます。

脅威インテリジェンスでネットワークを保護する方法を発見してください。

ホワイトペーパーをダウンロード（英語）

Hawkeye:
アクティブ・モニタリング・プラットフォーム

ネットワークチームは、さまざまなアプリケーション（ユニファイドコミュニケーション（UC）、VoIP、ビデオなど）をサポートしており、すべて遅延とパフォーマンスに対する感度が異なります。ただし、パフォーマンスの監視に関しては、ライブネットワークデータを受動的に待機するだけでは不十分です。ユーザーよりも先に接続の問題やパフォーマンスの問題を見つけたい場合は、積極的に取り組む必要があります。

組織がHawkeyeをネットワーク監視で活用する理由がそこにあります。アクティブなネットワーク監視を使用すると、ネットワークのあらゆる場所でユーザーが活用するアプリケーションのサービス品質を継続的にテスト、検証、監視することで、コストのかかるダウンタイムを最小限に抑えることができます。

紹介ビデオを視聴

導入	管理と操作	テストタイプ、機能	KPIs	アラーム	APIコントロール	合成テストライブラリ	マシンラーニング	リアルタイムのデータ、結果	スケジュール自動化
On-premises (software-based platform)	Web-based controller with integrated metrics dashboard	Node-to-node, mesh, real service, application / web / Wi-Fi monitoring	Basic and advanced metrics	SNMP and email	SOAP API	✓	✓	✓	✓

詳細情報

Hawkeye活用で、問題が発生する前に、能動的・定期的に検知、診断、修正します。

アクティブモニタリングについて詳しい情報を見るには、下記資料をダウンロードください。

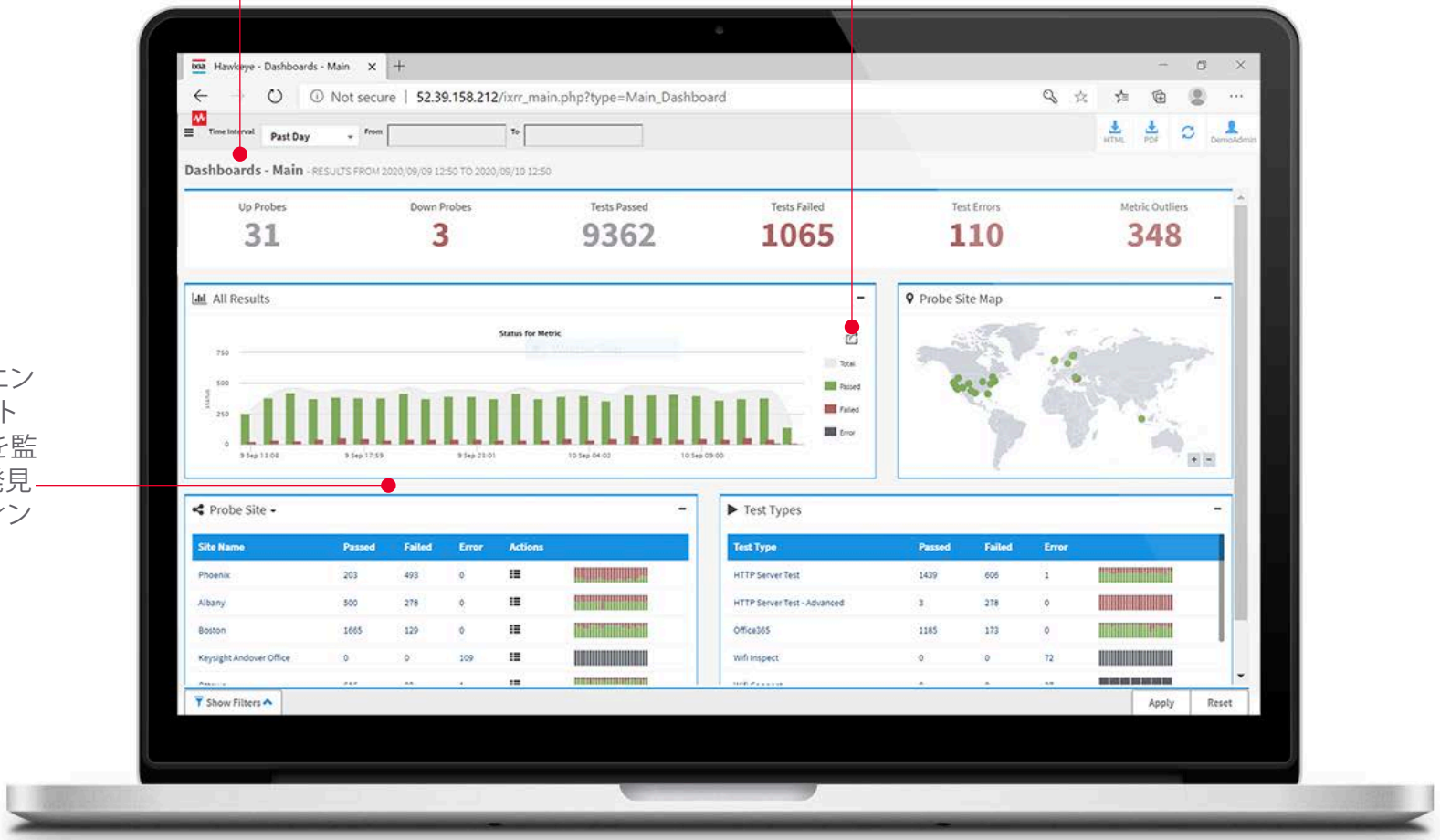
ガイドをダウンロード（英語）

HAWKEYE

使いやすいダッシュボードを使用すると、コアからエッジまでパフォーマンス監視を一元管理できます

合格/不合格の指標は、実用的な知見を提供します

ユーザーエクスペリエンスを制御します。サイト間のパフォーマンスを監視し、問題を早期に発見し、トラブルシューティングを迅速に行います



HAWKEYE エンドポイント：コンパクトサイズで広範囲をカバー

測定していないものを管理することはできません。ビジネスがピークパフォーマンスに依存している場合、ブラインドスポットの放置はコスト発生につながります。トラブルシューティングの遅延、停止の長期化、問題が発生した場合の生産性の低下などです。常にどこで何が起こっているのかを知る必要があります。

Hawkeyeを使用すると、パフォーマンス監視エンドポイントと組み合わせて、データセンターからネットワークのエッジまでのユーザーエクスペリエンスを監視できます。純粋なSoftware-as-a-Service（SaaS）ソリューションとは異なり、ネットワークパケットブローカー、インラインモニタリングプローブなど、ハードウェアベースおよびソフトウェアベースのあらゆるエンドポイントをネットワーク全体に簡単に展開できます。

Hawkeyeのエンドポイントについて知る

Hawkeye エンドポイント	活用例	インターフェース	合成モニタリング	インライン モニタリング	Fall to Wire	パケットキャプチャ、統計、アグリゲーション、フィルタリング	NetFlow, 重複排除	ローカル管理	リモートプロビジョニング
Virtual / Software (Docker, Cloud, Android, iOS, Microsoft Windows, Linux, Mac)	In conjunction with other endpoints	Ethernet, virtual, Wi-Fi, mobile, wireless	✓						✓
Vision E1S NPB	Large offices	4x 10 G (SFP+), 6x 1 G BASE-T, 2x 1 G BASE -T, 1x USB, 1x RJ45	✓			✓	✓	✓	✓
IxProbe	Branch locations or small offices	2x 1 G	✓	✓	✓			✓	✓
XRPI	Small offices	1x Wi-Fi, 1x FE, 2.4 GHz, 5 GHz, AC	✓						✓

SSL VPN
ゲートウェイ検査サービス

堅牢なVPNインフラストラクチャは、ネットワークアーキテクチャの重要な部分です。問題が発生した場合、ビジネスの継続性に影響を与え、従業員がリモートで作業できなくなる可能性もあります。問題に備えるには、使用量の急増に備えて十分なVPN容量をプロビジョニングする必要があるだけでなく、ネットワークがトラフィック負荷のピーク時に重要なアプリケーションをスムーズにサポートできることを検証する必要があります。

VPNゲートウェイのサイズを適切に設定して展開する際に、キーサイトがお手伝いできます。ユーザーが接続の問題を報告するのを待つのではなく、制御された現実的なパフォーマンステストを使用してVPN容量を能動的に検証できます。キーサイトのゲートウェイ評価サービスを使用すると、ボトルネックを特定し、セキュリティポリシーを最適化して、ネットワークが予期しない事態に常に備えることができます。

Testing as a service	Bandwidth-per-tunnel test	Usage capacity test	Connection time test	Throughput analysis	Live network impact	Average duration per assessment	Required information
✓	✓	✓	✓	✓	None	4 hours	SSL VPN address

詳細情報

SSL VPN GATEWAY
検査サービス

中央のダッシュボードからVPNゲートウェイの評価結果を確認します

VPNゲートウェイは何人のユーザーをサポートできますか?トンネルごとにどのくらいの帯域幅を維持できますか?これらの重要な疑問への回答を入手してください。

製品および販売に関するお問い合わせ先

SCSK株式会社

プラットフォーム事業グループ
IT プロダクト&サービス事業本部 ネットワーク部
〒135-8110 東京都江東区豊洲 3-2-20 豊洲フロント
TEL 03-5859-3034 / FAX 03-5859-3102
E-mail : ixia-info@ml.scsk.jp
製品情報：https://www.scsk.jp/sp/ixia/

KEYSIGHT TECHNOLOGIES