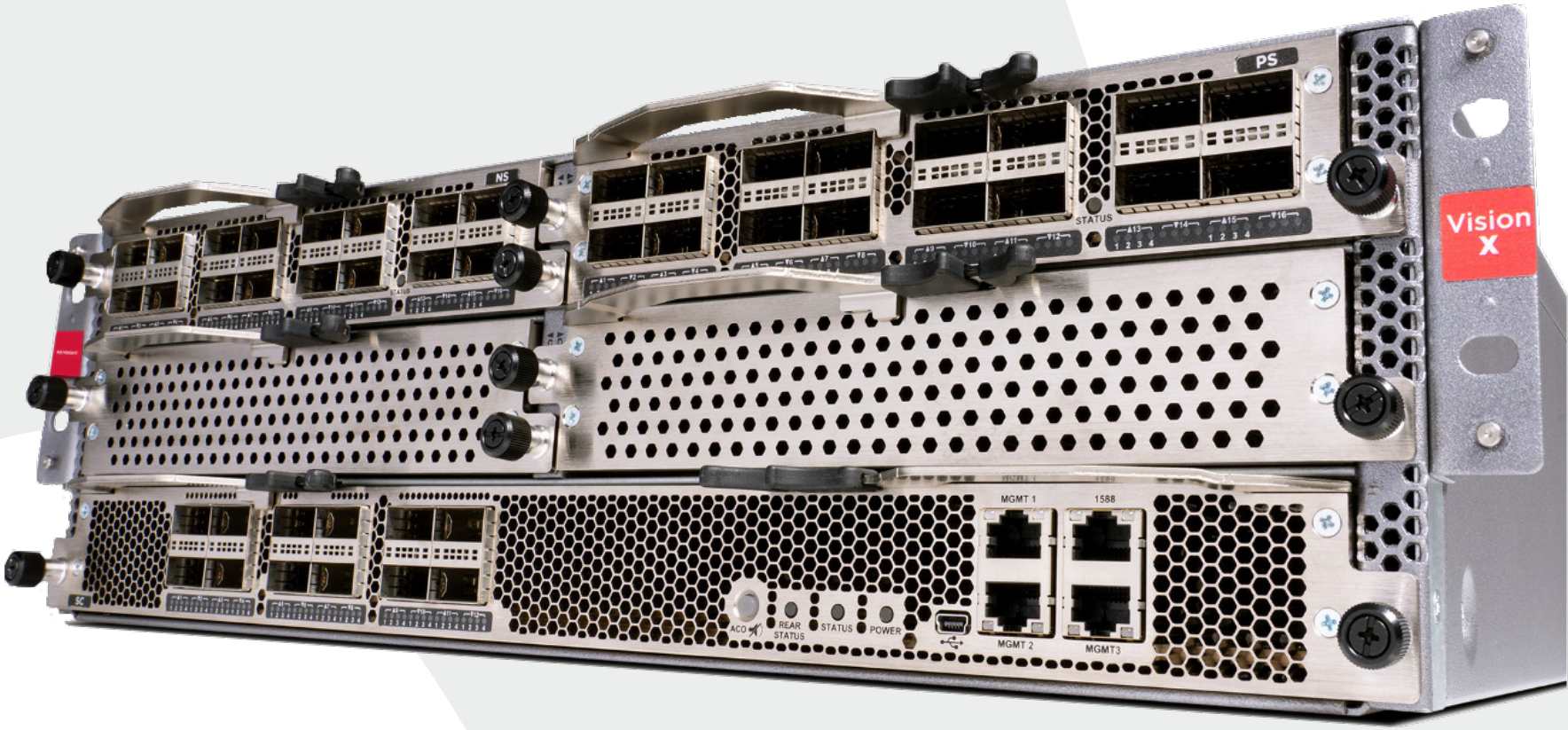
Network Visibility Products

カタログ



KEYSIGHT

目次

Connect and Secure the World with Dynamic Network Intelligence

常時接続されたネットワークを前提にしたアプリケーションやツールの普及にともない、ネットワークの安定性とセキュリティ保護への期待も高まっています。テクノロジーが進歩するにつれ、エッジコンピューティング、クラウド環境、巧妙化するセキュリティ上の脅威、増大する帯域幅要件、厳しいコンプライアンス規制などが要因となり、ネットワークからすぐに役立つ実用的な解析情報を得ることが難しくなっています。

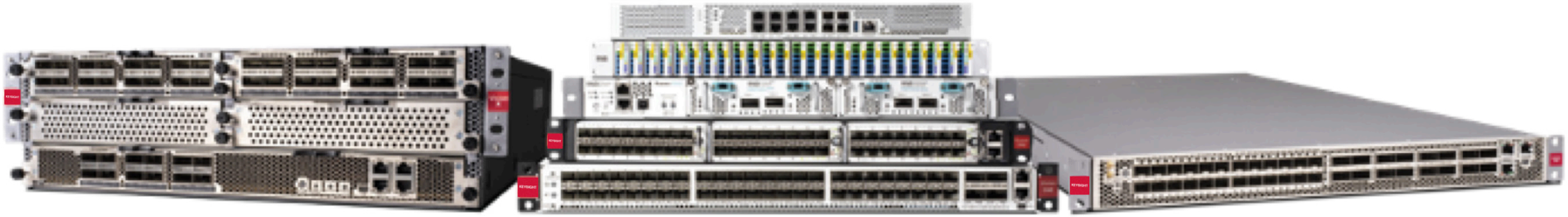
キーサイトのソリューションを利用すると、お客様はあらゆるネットワーキング環境でネットワークトラフィック、アプリケーション、ユーザーに関する豊富なデータを利用できるようになります。この詳細な解析情報は、キーサイトがダイナミック・ネットワーキング・インテリジェンスと呼んでいるものです。これは、継続的にイノベーションを推進し、厳しいサービスレベル契約に対応し、アプリケーションのスムーズかつセキュアな稼働を維持するのに役立ちます。

ダイナミック・ネットワーキング・インテリジェンスを利用できるようにするにはネットワークの可視化が必要であり、キーサイトでは幅広い製品スイートを提供しています。その核となるのは、Keysight Vision network packet broker(NPB)です。NPBでは、効率化されたフィルタリング済みのトラフィックを提供することで、セキュリティツールおよびネットワーク監視ツールを最大限に活用できます。

Keysight iBypassなどの外部バイパススイッチを使うと、ネットワークを常にオンライン状態に維持するためのハイアベイラビリティとインラインフェイルオーバーを実現できます。また、TAPを使ってネットワーク上のトラフィックをありのままに捕捉することができます。これは、ダイナミック・ネットワーク・インテリジェンスの基盤となるものです。

キーサイトのネットワーク可視化製品を組み合わせることで、既存の各種ネットワークツールをさらに効率的かつ効果的に活用し、常に高いパフォーマンスと厳しいセキュリティを維持することができます。

GET A CRASH COURSE IN NETWORKING FUNDAMENTALS.



Network Packet Brokers: 適切なデータを適切なツールに

NPBは、ネットワーク全体でダイナミック·ネットワーク·インテリジェンスを利用できるようにするための核となる製品です。NPBでは、アプリケーション認識型のトラフィックフィルタリング、暗号解読、重複排除を利用し、セキュリティツールや監視ツールが適切なデータを過不足なく得られるようにすることで、これらのツールを効率的かつ効果的に活用できるようにします。さらに、Keysight NPBでは、他の多くの競合製品と異なり、Field-Programmable Gate Array(FPGA)によるハードウェアアクセラレーションを利用でき、トラフィック損失、ブラインドスポット、パケットロスなしにラインレートで各種機能やフィルタリングを利用できるようになります。この機能は、ミッションクリティカルなセキュリティやネットワーク監視をサポートする可視化ソリューションを配備する場合には常に重要な検討事項です。部分的な可視化では十分ではありません。

Keysight NPBは、以下の特長を備えています：

- ゼロ-ロスアーキテクチャ
- 複数の監視ツールまたはセキュリティツールに対応したロードバランシング
- 集中型の暗号解読可能(TLS1.3対応)
- Dynamic filter compilerによる運用の複雑さの軽減
- 使いやすいGUI

Vision X NPB

Visibility for finance

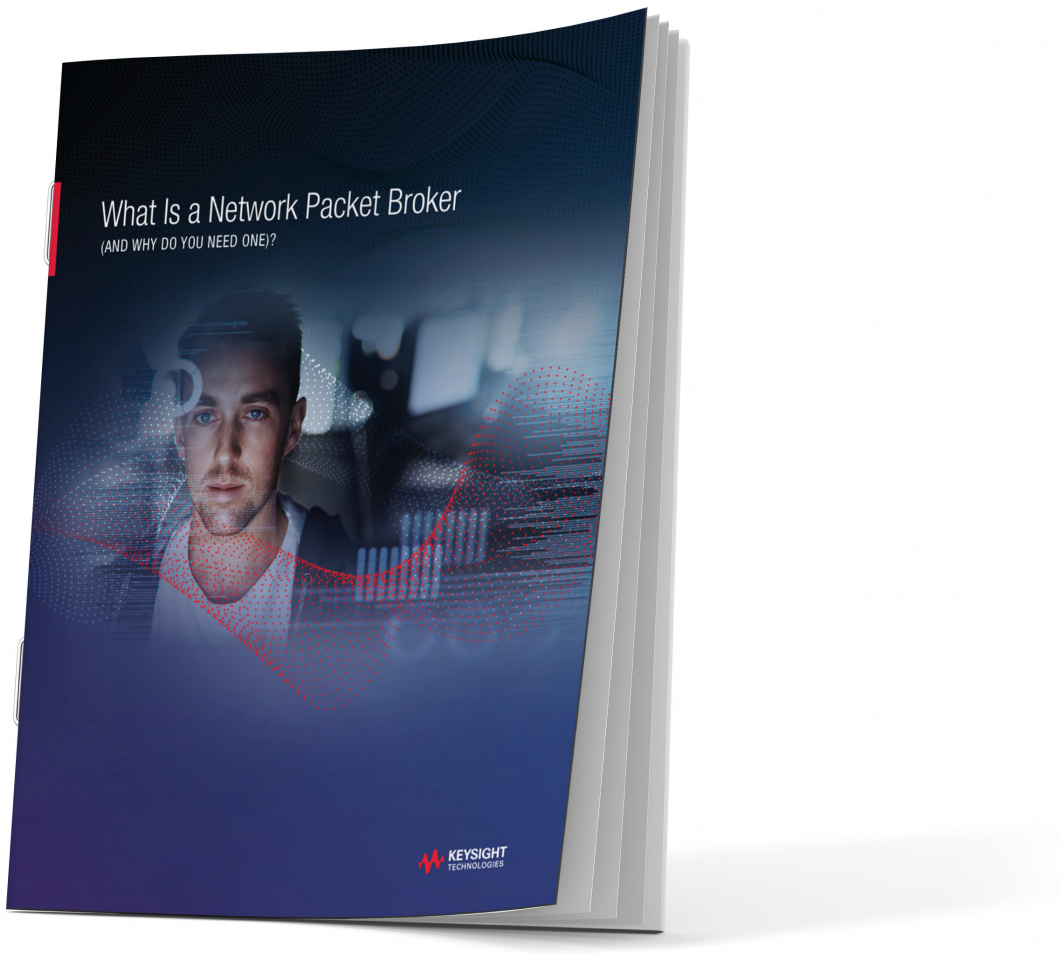
Keysight TradeVisionは、金融サービス機関向けのユニークな製品です。これは、マーケットフィードヘルス監視に毎秒2億4千万件の取引値／気配値メッセージを監視できる機能を組み合わせたものです。これは、米国の株式市場とオプション市場を合わせたものの12倍の規模です。TradeVisionでは、損失のないFPGAベースのハードウェアアクセラレーション、高精度のタイムスタンプ、TAPアグリゲーション機能により、大きな被害をもたらす可能性のある問題に対処するのに要する時間を短縮できます。他にも以下の機能を備えています：

- マルチキャストギャップ検出
- 高度なレイテンシー解析
- マイクロバーストアラート
- 高解像度のトラフィック統計
- 簡素化されたフィード管理

Accredited security for US federal agencies

政府機関、軍事、その他のセキュリティを重視する組織には、最高水準のセキュリティ保全が求められます。このため、キーサイトのすべてのNPBはコモンクライテリア、FIPS 140–2、DoDIN APLの要件に適合しています。また、最新の認定はソフトウェア・モジュール・アプローチを利用しているため、常に最新のソフトウェア拡張機能を利用できるというメリットもあります。

詳しくお知りになりたいですか？
NPBの機能と必要性について、詳細をご覧ください。



Advanced packet processing and intelligent context-aware filtering

キーサイトの信頼性の高いインテリジェントな可視化機能(Stack)は、Vision Series NPBと既存の可視化／セキュリティプラットフォーム全体を最大限に活用するのに役立ちます。これらのソフトウェアスタックでは、L2からL7に基づいたフィルタリング機能が利用できます。各機能スタックは、物理データセンターまたはプライベート／パブリック／ハイブリッドクラウドのいずれでも、最高のパフォーマンスが得られるように設計されています。

NPBの機能スタックにより、高度なパケット処理でNPBの機能を拡張および強化するダイナミック・ネットワーク・インテリジェンスが可能になります。以下に各スタックの詳細を示します。

NetStack

ネットワーク可視化を実現するための基本的なスタンダード機能を提供します。これには、信頼性の高いフィルタリング、ロードバランシング、アグリゲーション、レプリケーションなど、3段階のフィルタリング(ingress、dynamic、egress)とDynamic filter compilerが含まれます。

PacketStack

重複するパケットを除去する重複排除を用いて、フル・ライン・レートで損失のないインテリジェントなパケットフィルタリング、操作、伝送を行います。この他に、ヘッダーストリッピング、パケットトリミング、タイムスタンプ、データマスキング、バーストプロテクションなどの機能があります。

PacketStackでは、以下を行うことができます：

- 監視ツールを保護して耐用年数を延ばし、より効果的に運用できます。
- 必要なヘッダーバイトのみを維持し、ペイロードをユーザが必要とする長さにトリミングすることで、ツールのパフォーマンスを向上させることができます。
- クレジットカードや社会保障番号などの個人を特定できる情報を秘匿してから、データを解析ツールに送信できます。
- ツールを監視し、時間制約のあるアプリケーションではすべてのパケットにタイムスタンプを付加することで、ナノ秒の分解能と精度で遅延を測定できます。
- vTapからのL2GREまたはERSPANトンネルを終端し、通常のイーサネットトラフィックを既存ツールに提供できます。
- Generic header strippingを用いて、L3GRE、Jmirror、PBB-TE、LISP、VSL、OTV、PPPoEなどの新規プロトコルや独自プロトコルをストリッピングできます。

SecureStack

セキュアなトラフィックの処理を最適化し、インラインおよびアウトオブバンドのSSL/TLS decryptionをサポートします。Data Masking Plusは、Health Insurance Portability and Accountability Act(HIPAA)やクレジットカード業界などの規制適合要件に準拠しています。トラフィックを復号化してマルウェアをすばやく検出し、データ損失やセキュリティツールのボトルネックを解消することで、高い可視性を実現します。

AppStack

すばやく正確なアプリケーションの識別、ジオロケーションとタグ付け、特許取得済みのシグネチャー検出、オプションのRegExフィルタリングによる、コンテキストアウェアなシグネチャーベースのアプリケーション層フィルタリングを提供します。ポイントアンドクリックのシンプルな管理インタフェースで、必要なアプリケーショントラフィックのタイプを選択し、ツールへのトラフィックをフィルタリングできます。AppStackは、地理的情報、アプリケーション情報、デバイス情報を付加することで、監視プラットフォームを強化します。

MobileStack

General Packet Radio Service Tunneling Protocol(GPRS Tunneling Protocol(GTP))に対応したモバイルキャリアのEvolved Packet Coreの可視化インテリジェンスを提供します。MobileStackでは、Session Initiation Protocol(SIP)の相関とロードバランシング、加入者ごとのフィルタリング、加入者許可リストおよび加入者サンプリングを利用できます。MobileStack on Vision Xでは最大5億1,200万件の加入者セッションと、5Gパフォーマンスをサポートする1シャーシあたり最大1,600 GBのユーザープレーントラフィックを用いた相関が可能です。

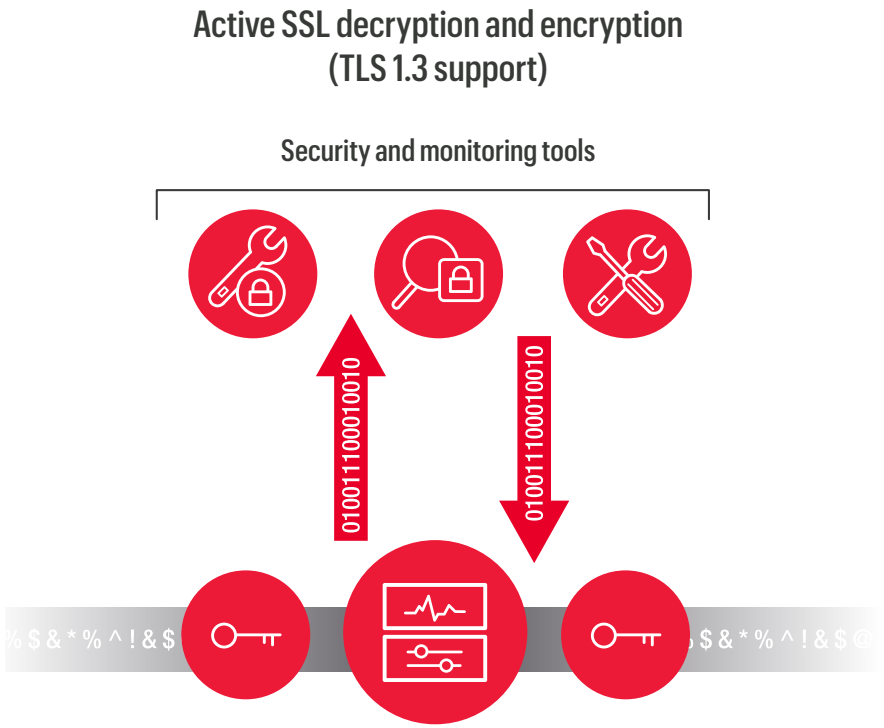
TradeStack

金融市場にシンプルなマーケット・フィード・データ管理ツールを提供し、マーケット・フィード・データの構成、解析、管理の手間を解消します。高解像度のトラフィック統計(0.1 msまでの解像度に対応)、マイクロバースト検出、フィードヘルス、レイテンシー測定、ギャップ検出などの機能が含まれます。

キーサイトのNPBスタックはモジュラー式なので、必要なときに、必要な機能だけを追加することができます。既存のNPBにフルスタックのソフトウェアソリューションを追加することで、現在および将来のニーズに合わせて、ネットワーク可視化アーキテクチャーを進化させ拡張していくことができます。

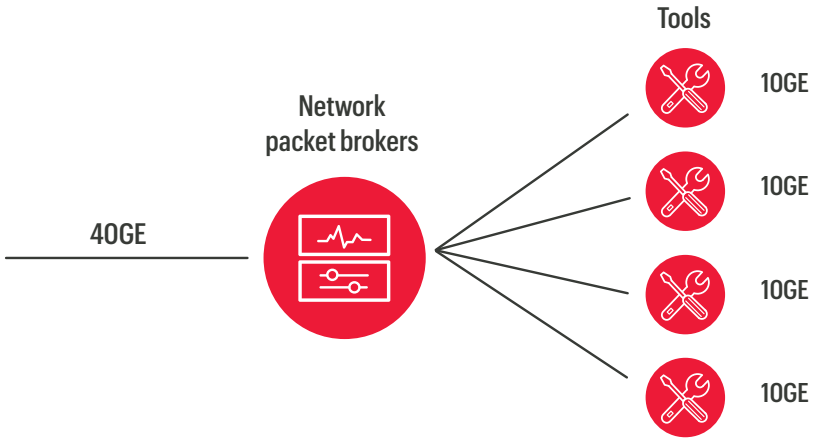
セキュアなトラフィック処理とSSL/TLS decryptionによるハッキングの阻止

ブラインドスポットをなくすためには、復号化されたトラフィックと暗号化されたトラフィックの両方を含めて、すべてのネットワークトラフィックを確認する必要があります。しかし、データ保護のために暗号化を使用することには、メリットがある反面デメリットもあります。サイバー犯罪者は、トロイの木馬のように、ランサムウェアやマルウェアを暗号化データの中に隠してネットワークを攻撃する可能性があります。処理負荷の高いSSL/TLS decryptionのタスクをSecureStackを搭載したVision Series NPBにオフロードすれば、ハッカーの得意な分野での攻撃を阻止することができ、ツールに過大な負荷をかけたりパフォーマンスを損なったりすることなく、ツールの効率性を高めることができます。

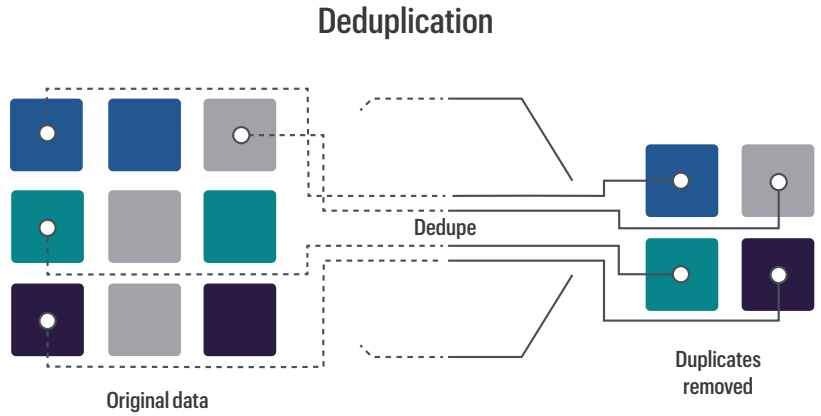


ロードバランシングによるコスト削減とツールの長期利用

NetStackを搭載したVision NPBは、アグリゲーションとロードバランシングを実行することで、データを複数の低速ストリームに分割して適切なツールに送信します。例えば、40 Gbpsのトラフィックを10 Gbpsの複数のツールに分散させると、より高速なデータレートに対応した高額なツールの予算を確保できるまで10 Gbpsのツールの利用期間を延ばすことができます。



ツールに送信するフィルタリング済みデータを減らすことで**モニタリングおよびセキュリティツールの効率性を35 % ～ 50 %向上させる重複排除**



NextGen network packet broker: Vision 400 and E400S

最大400Gの速度まで可視化を拡張

Keysight Vision 400およびVision E400Sは、次世代型のネットワーク可視化ソリューションです。幅広い機能セットが提供されているため、最大400 Gbpsのネットワーク速度の実稼働ネットワークで変化を続ける可視化ニーズに対応できます。

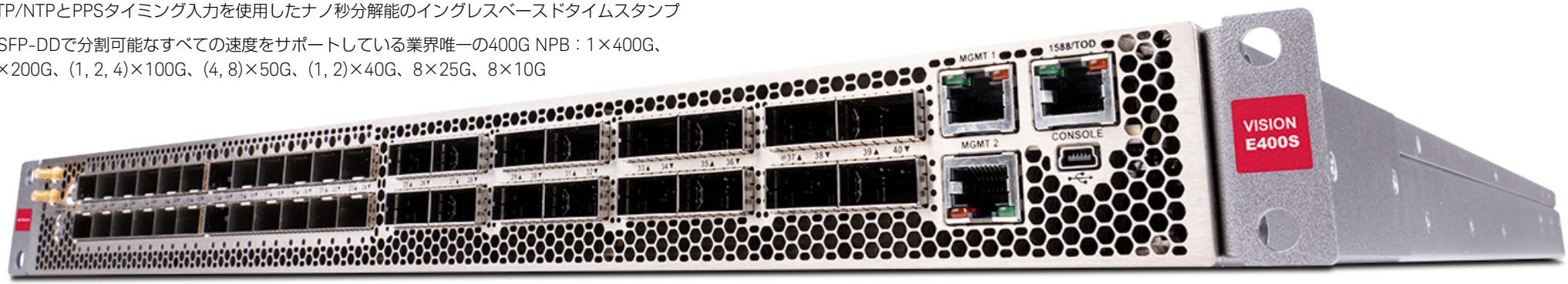
コンパクトな1RUサイズの筐体で、フロントパネルに24個のQSFP56ポートと16個のQSFP-DDポートを備えています。各QSFP-DDは、ファンアウトケーブルを使って複数の低速ポート(200G、100G、40G、50/25/10G)に分割できます。これは分割可能なすべての速度をサポートしている唯一のNPBで、デザインの柔軟性を最大限に高めながら、同時にレガシーデバイスとの相互運用性を維持しやすい構成になっています。

シリコンレベルでプログラム変更が可能であるため、ウェルノウンプロトコルまたは独自プロトコルを問わず、新しいプロトコルのパーサーやヘッダー・ストリッピング・オプションをすばやく実装することができます。新しいロードバランス(LB)オプションでは、ポートグループ単位のロードバランシングをサポートしています。従来型のセッションベースのロードバランシングに加えて、新しいオプションでは、非対称ロードバランシング、重み付きロードバランシング、ランダムロードバランシング、トンネル化IPヘッダーを使用したロードバランシングが利用できます。

Vision 400には高性能FPGAが搭載されており、ラインレート重複排除、パケットトリミング、バーストプロテクションなど、E400SにはないPacketStack機能が利用できます。

Highlights

- 10/25/40/50/100/200/400Gのポート速度をサポートするコンパクトな1RUのNPB
- P4およびTofinoベースのプログラマブルシリコン
- 全二重、non-blocking、ラインレートL2転送による9.2 Tbpsの実現
- PTP/NTPとPPSタイミング入力を使用したナノ秒分解能のイングレスベースドタイムスタンプ
- QSFP-DDで分割可能なすべての速度をサポートしている業界唯一の400G NPB：1×400G、2×200G、(1, 2, 4)×100G、(4, 8)×50G、(1, 2)×40G、8×25G、8×10G



Vision E400S

Product	Vision 400	Vision X	Vision ONE	Vision E400S	Vision 7816	Vision Edge 100
Description	Scalable 1RU chassis that supports intelligent visibility stacks for 10 / 25 / 40 / 50 / 100 / 200 / 400G networks	High-performance, high-density, modular, scalable 3RU chassis for 10 / 25 / 40 / 50 / 100G networks	Full-featured, turnkey 10 / 40G visibility in a 1RU form factor	Scalable 1RU chassis for 10 / 25 / 40 / 50 / 100 / 200 / 400G networks	Scalable, high-density, 2RU chassis supporting 10 / 25 / 50 / 100G networks	Cost-effective, high-density rack-level visibility for 10 / 25 / 40 / 50 / 100G
Zero-packet-loss architecture	✓	✓	✓	✓	✓	✓
Dynamic filter compiler	✓	✓	✓	✓	✓	✓
System height (RU)	1	3	1	1	2	1
Advanced packet processing	✓	✓	✓	✓	—	—
Port ingress time-stamping	✓	—	—	—	—	—
AC redundant power supply (hot swap)	✓	✓	✓	✓	✓	✓
DC redundant power supply (hot swap)	✓	✓	✓	✓	✓	✓
Max backplane capacity (Gbps)	9200	6400	640	9200	6400	3200
Max number of 1G ports	0	0	64	0	0	0
Max number of 10G ports	152	108	64	152	128	128
Max number of 25G ports	152	108	0	152	128	128
Max number of 40G ports	32	76	16	32	64	32
Max number of 50G ports	152	108	0	152	128	64
Max number of 100G ports	64	60	0	64	64	32
Max number of 400G ports	16	0	0	16	0	0
	Get a quote ›	Get a quote ›	Get a quote ›	Get a quote ›	Get a quote ›	Get a quote ›

Product	Vision Edge 40	Vision Edge 10S	Vision Edge 1S	Vision Edge OS	Vision T1000	TradeVision
Description	Cost-effective rack-level visibility for 1 / 10 / 40G	Ideal for remote site deployments supporting 1 / 10G networks	Compact, cost-effective visibility for branch sites	Disaggregated visibility OS for open switch hardware	Tough NPB designed for harsh environments -40 C to +85 C op. temp.	Market-feed monitoring and tap aggregation for financial markets
Zero-packet-loss architecture	✓	✓	—	✓	—	✓
Dynamic filter compiler	✓	✓	—	✓	—	✓
System height (RU)	1	1	1	↓	1	1
Advanced packet processing	—	—	—	—	—	—
Port ingress time-stamping	✓	—	—	↓	—	—
AC redundant power supply (hot swap)	✓	✓	✓	↓	✓	✓
DC redundant power supply (hot swap)	✓	✓	—	↓	✓	✓
Max backplane capacity (Gbps)	720	480	12	↓	12	640
Max number of 1G ports	48	48	10	↓	26	64
Max number of 10G ports	72	48	4	↓	—	64
Max number of 25G ports	0	0	0	↓	—	0
Max number of 40G ports	18	0	0	↓	—	16
Max number of 50G ports	0	0	0	↓	—	0
Max number of 100G ports	0	0	0	↓	—	0
Max number of 400G ports	0	0	0	↓		
	Get a quote ›	**Get a quote ›**	**Get a quote ›**	**Get a quote ›**	**Get a quote ›**	**Get a quote ›**

↓ Switch dependent

Bypass Switches: アップタイムとネットワーク可用性の確保

外部バイパススイッチは、ネットワーク監視とセキュリティ配備のハイアベイラビリティとメンテナンスの容易さを実現する鍵となります。侵入防止やファイアウォールなどのツールの必要性は誰もが認識していますが、これらのツールのインラインでの設置は、再起動、メンテナンス、または交換を行う際にリスクとなり、ダウンタイムを引き起こす可能性があります。Keysight iBypassなどの外部バイパススイッチは、自動フェイルオーバー機能を備えているため、ツールの更新や停止によってネットワークがダウンするのを防ぐことができます。

Keysight iBypassは、以下の特長を備えています：

- 冗長なシリアルアーキテクチャーをサポート
- ハイアベイラビリティ：active-activeまたはactive-standby
- 構成済みハートビート
- 一元的な管理
- 使いやすいGUI

iBypass 100G

Product	iBypass 100G	iBypass DUO	iBypass VHD	iBypass 4 Copper
Description	Single-segment 100G intelligent bypass	High-density bypass with redundant management	Very-high-density, 12-segment intelligent bypass	Single-segment intelligent bypass for copper networks
Speed	100/40G	1G / 10G	1G / 10G	10 / 100 / 1G
Media type	Fiber	Fiber	SFP+ / SFP	Copper
Networks per device	1 or 2 segments	1 or 2 segments	12 segments	1 segments
High availability	Active-active / active-standby	Active-active / active-standby	Active-active / active-standby	—
Configurable	✓	✓	✓	✓
Link fault detection	LFD	LFD / LFDC	LFD / LFDC	LFD / LFDC
	Get a quote ›	Get a quote ›	Get a quote ›	Get a quote ›

Which iBypass belongs in your network?

Network Taps:
ダイナミック・ネットワーク・インテリジェンスの基盤

ダイナミック・ネットワーク・インテリジェンスの基盤となるのは、ネットワークTAPと、これらが提供する純粋でフィルタリングされていないトラフィックの情報です。SPANポートやポートミラーリングと異なり、TAPはすべてのトラフィックの可視化情報を提供します。通常はドロップされるような不正なトラフィックやエラーも含め、すべてのトラフィックを表示します。この真の可視性により、トラブルシューティング、セキュリティ、フォレンジックが容易になります。

キーサイトは、Flex Tap(光ファイバー TAP)、Flex Tap Secure+(セキュリティ強化TAP)、Copper Tap、Aggregation Tap、Industrial Tough Tapsなど、あらゆるネットワークに対応する幅広いTAPを提供しています。

キーサイトのTAPは、以下の特長を備えています：

- シンプルなプラグアンドプレイ方式
- IPアドレスが不要
- ハッキング不可能なセキュリティーを確保
- カッパーとファイバーに対応
- 最大400 Gbpsまで対応

Learn more about taps and why they are critical to network visibility.

Flex Tap

Product	Flex Tap	Flex Tap Secure +	Patch Tap	Copper Tap	Tap aggregators	iLink Aggregator II
Description	Modular, passive fiber taps	Modular, passive fiber taps with optical diode	Low-latency, passive fiber taps	Active copper taps	Active copper taps with aggregation mode	Multiple (x8) copper taps with aggregation[1]
Speed	1G to 400G	1G to 400G	1G to 100G	10 / 100 / 1000 Mbps copper	10 / 100 / 1000 Mbps copper	10 / 100 / 1000 Mbps copper + 4 x SFP+ for aggregation ports
Port type	LC and MTP	LC	LC	RJ45	RJ45	RJ45 / SFP+
Unique features	• 40 / 100G BiDi PSM4, SR4, SR10, and QSFP+ 40G-LX4 • Multiple split ratios and fibers • OM3, OM4, and OS2	• Advanced security prevents accidental or intentional light or data injection • Ideal for lawful intercept, government, military, and other high-security deployments	• Low latency down to < 8nSec • Bend-insensitive • Multimode OM4 • Single-mode OS2	• Independent auto-negotiate (tap low-speed networks and send data to higher-speed tools) • Physical air-gapped monitor ports — data • Diode between tool and monitor ports • Fail-to-wire capability	• Monitors full-duplex traffic with a single NIC • Aggregates both directions into a single monitoring link • Works as a standard or aggregation tap • Offers fail-to-wire capability	• Cost-effective tap aggregator designed to combine traffic from multiple taps • Supports low-medium speeds that high-performance NPB often do not support • Inbuilt taps have fail-to-wire capability
	Get a quote ›	Get a quote ›	Get a quote ›	Get a quote ›	Get a quote ›	Get a quote ›

1. Also available as a 16-port SPAN aggregator. 16 x 10 / 100 / 1G input ports and 4 x 10G SFP+ monitor / any-to-any.

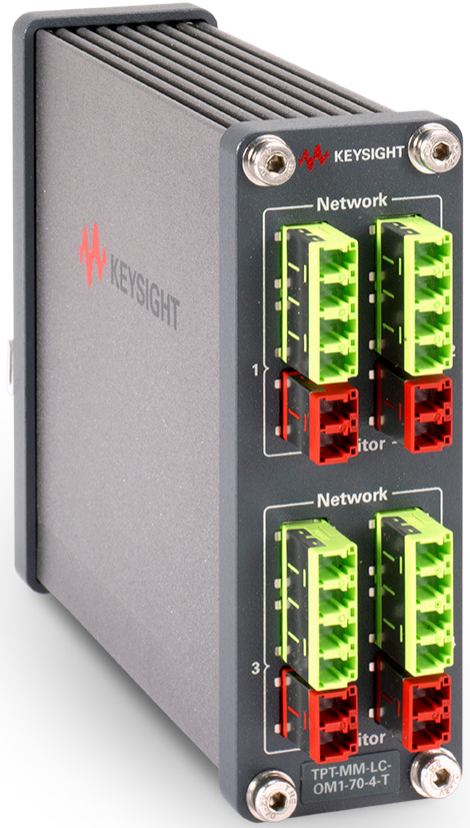
産業環境向けのTough Tap

Keysight Tough Tapは、過酷な環境向けに新たに設計された業界初の高耐久性ネットワークTAPです。広い温度範囲に対応し、衝撃や振動への耐久性を備え、10/100M、1G、10Gの最適化されたカッパーおよびファイバーポートを備えています。Tough Tapは、安全性に関するIEEE 1613規格やIED(Intelligent Electronic Device)向け通信プロトコルに関するIEC 61850規格などの、Institute of Electrical and Electronics Engineers (IEEE) standardsの認定を受けています。

Copper Tough Tapは、セキュリティツールおよびパフォーマンスツール向けにアウトオブバンド監視を提供し、すべてのパケットを複製して完全な可視化を実現します。アップタイムの保護を強化するため、冗長な電源コネクタ(ターミナルブロック)を備えており、主電源に不具合が発生した場合は、自動的にバックアップ電源に切り替わります。両方の入力電力に不具合が発生した場合でも、ネットワークポート間でのトラフィックの受け渡しは継続されます(フェイルオープン)。

Flex Tough Tapは、ネットワークトラフィックを収集してアーカイブします。このTAPは、遠隔地の変電所に見られる新旧のファイバーモードが存在するファイバーネットワーク向けに最適化されており、TAA-compliantです。これらのTAPは、ネットワーク内のあらゆるインライン接続に配備できます。

Flex Tough Tap



Copper Tough Tap

Product	Copper Tough Taps	Flex Tough Taps
Description	Industrial active copper taps	Industrial multimode, modular, passive fiber taps
Speeds	10 / 100 / 1000 Mbps copper	1G to 400G
Port types	RJ45	LC
Certification, standards, and compliance	TAA; IEC 61000-4-2,3,4,5,6,8,11; IEC 60068-2-6; IEEE-1613; UL 508 Listed; UL 60950-1; EN60950-1; CE; IEC 61850	TAA; CE; RoHS 10
Unique features	• Supports Power over Ethernet (PoE) • Auto speed negotiation • Secured by design — with no management interface or IP address, it is unhackable • Physical air-gapped monitor ports — data diode between tool ports and monitored ports prevents malicious injections from monitoring network • Silent operation • DIN rail mountable • Fan-less • Operating temperature range -40 C to +85 C	• No power required • Secured by design — with no management interface or IP address, it is unhackable • Passes all traffic (including errors) from all layers • Compact — 4 taps in one module • Completely passive, optical device • OM1, OM5 multimode models in 70 / 30 split ratio • Deploy at any inline network connection • DIN rail mountable • Same form factor as Copper Tough Tap • Operating temperature range -40 C to +85 C
	Learn more >	Learn more >

Cloud Visibility

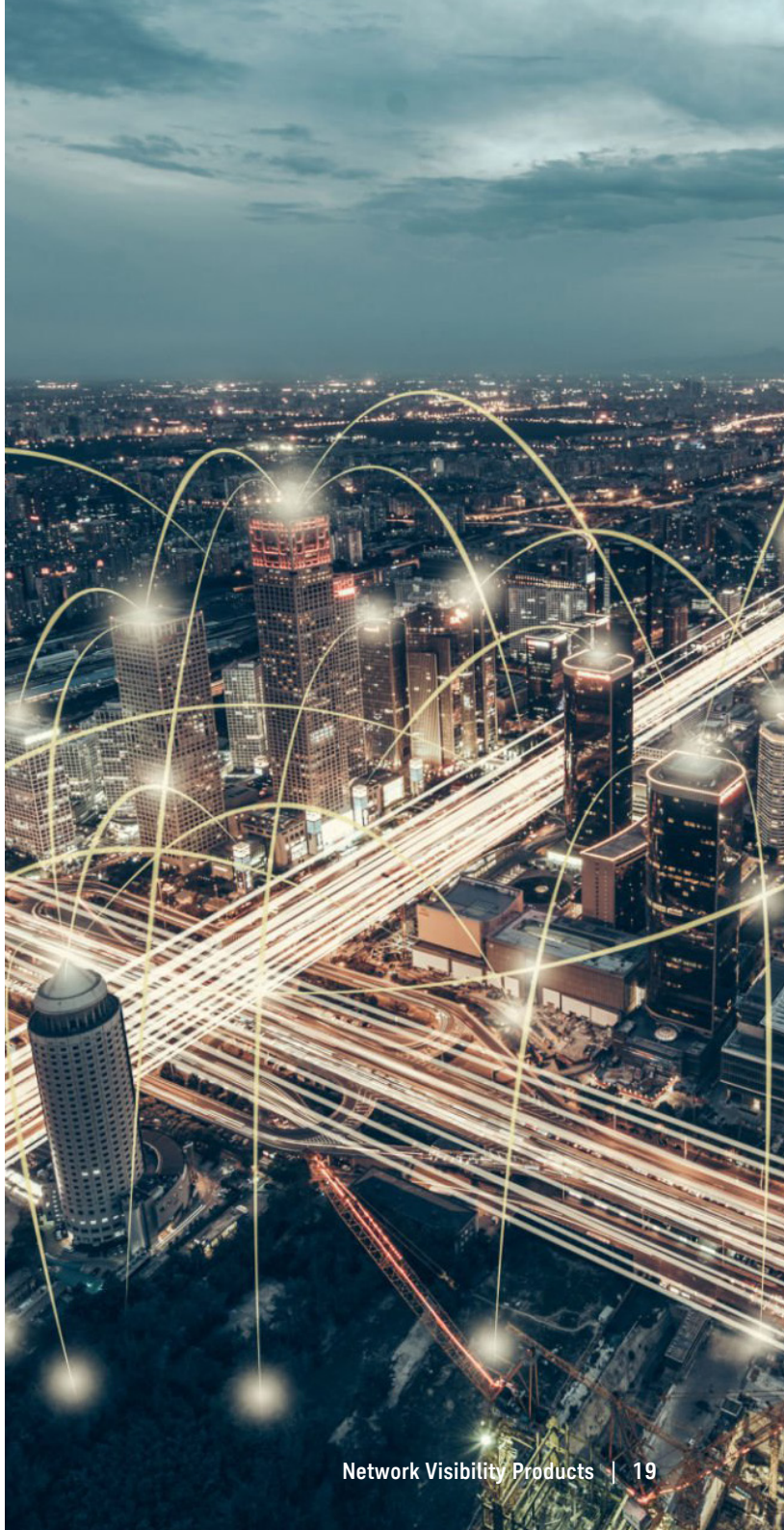
CloudLensにより、クラウドのセキュリティ、可視性、パフォーマンス監視をさらに強化

Keysight CloudLensは、パブリック／プライベート／ハイブリッドクラウドを可視化するプラットフォームであり、パケットキャプチャー、フィルタリング、および分析を可能にし、あらゆるクラウド環境でダイナミック・ネットワーク・インテリジェンスを提供します。独自のクラウドネイティブアーキテクチャーを導入したCloudLensは、クラウドオンリー／クラウドファースト戦略に適しており、マルチクラウド環境やハイブリッドクラウド環境を利用する企業にも最適です。

ネットワークのセキュリティとパフォーマンスを特に重視する企業は、CloudLensを利用して自社の最も脆弱なブラインドスポットに光を当てることができます。

CloudLensは、以下の特長を備えています：

- 仮想マシン、コンテナ、またはPod間ネットワークトラフィックの全パケットとNetFlowを捕捉してツールに転送できます
- 仮想化されたNetwork Packet Brokerとして稼働し、仮想ネットワークトラフィックのアグリゲーション、フィルタリング、重複排除をすべてクラウド内で行うことができます
- クラウドインスタンスに合わせてオンデマンドで柔軟に自動スケーリングできます
- マルチプラットフォーム対応で、クラウドサービスプロバイダーやプラットフォームに依存しません



Visibility Central Management: Single Pane of Glassで多くのNPBを管理

ネットワークからダイナミック・ネットワーク・インテリジェンス情報を抽出するタスクと同様に、ネットワークも複雑化の一途をたどっています。NPB、bypass switchとTAPで構成される可視化ファブリックは、ネットワークの重要な基盤となります。この場合、これらすべてのシステムの管理と調整を行う必要があります。そこで役立つのがKeysight Visibility Central Managementです。

一元管理では、監視、スケジュールされた構成変更、およびソフトウェアの一括アップグレードを使用して、何百ものデバイスを管理できます。構成のインポートまたはエクスポート、スクリプトの実行、帯域幅使用率の表示などを行うことができます。さらに、ダッシュボードをカスタマイズし、ノースバウンドインタフェースを介して他のネットワーク管理システムと統合できます。

キーサイトの一元管理は、以下の特長を備えています：

- Single-pane-of-glassでの管理
- デバイスの自動検出
- シングルサインオンとゼロタッチプロビジョニング
- 物理、仮想の両方のフォームファクターに対応
- プライマリ／バックアップ用フローティングIPによるハイアベイラビリティ
- RADIUS、TACACS+、LDAP認証をサポート

Hawkeye

アクティブ／総合ネットワーク・パフォーマンス監視でユーザ体感を管理

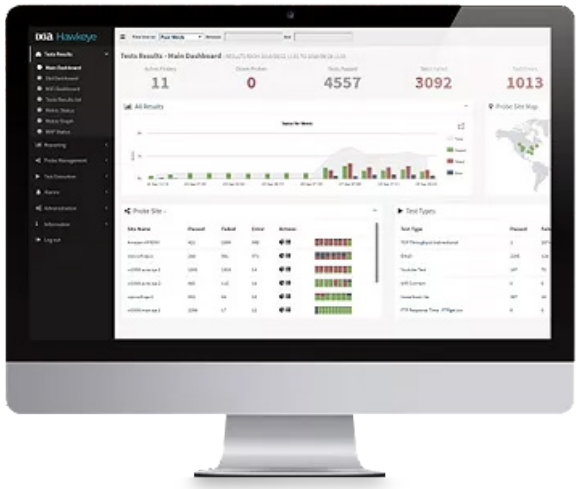
Keysight Hawkeyeはアクティブ監視プラットフォームで、お使いのネットワーク全体のパフォーマンスと接続性を継続的に管理できます。Hawkeyeでは、リモートサイト、データセンター、クラウドサービスなどをすべて1つのツールで簡単に監視できます。

音声アプリケーションでリモートユーザー体験を測定している場合も、拠点オフィスユーザーをWi-Fiで測定している場合も、あるいはSoftware-as-a-Serviceアプリケーションへの一般接続で測定している場合も、ピークパフォーマンスの監視、管理、維持を容易に行うことができます。Hawkeyeでは、この他にもさまざまな機能が利用できます。

Hawkeyeは、以下の特長を備えています：

- 定義済みのサービス品質テストの充実したライブラリ
- ターンキー統合による音声、ビデオ、ユニファイド·コミュニケーション・ツールの監視
- すべてのパフォーマンスデータを1つのインタフェースで確認し、カスタムアラームの設定が可能
- Wi-Fi 6および有線による監視
- 幅広いハードウエアプローブを選択可能(Vision E1S、XR3000、IxProbe、iBypass CU3など)
- ハードウエアプローブ XR3000、Vision E1Sは最大10G Ethernetに対応
- さまざまなプラットフォーム向けエンドポイント・ソフトウエア

Hawkeye Monitor Console



Hawkeye Endpoints

TimeKeeper

エンドツーエンドのインテリジェントなソフトウェア主導のクロック同期

正確な時刻への依存度が高まり続ける中で、システムやプロセスはタイミングインフラに対する故意または過失による攻撃に対してますます脆弱になっています。米国政府のCISA(Cybersecurity and Infrastructure Security Agency)などの機関は、タイムサービスの利用者がそれぞれのタイミングインフラを強化し、タイミング異常を検知して対応するための対策を講じることを強く推奨しています。多くの内部システムやセキュリティプロセスは、正確で疑いの余地のない時刻に依存しています。Global navigation satellite system(GNSS)、Network Time Protocol(NTP)、またはPrecision Time Protocol(PTP)などのタイミング信号が中断すると、クリティカルなシステムの混乱を招く可能性があります。

Keysight TimeKeeperソフトウェアはサーバにインストールされ、標準的なタイミングデーモンの代わりとして機能します。これを利用すると、企業、サービスプロバイダ、および政府は、公衆インターネットで利用可能な複数のタイムソースや、GPSやGalileoなどのGNSS時間信号を使用してシステムクロックを同期できます。また、同期の他にタイミング異常の検知とアラート通知も行われます。世界各地の100社を超える金融機関と複数の政府がすでにTimeKeeperをインストール済みです。

TimeKeeperは、以下の特長を備えています：

- NTPおよびPTPタイムソースの同時サポート
- TrustedTimeのマルチソースフェイルオーバー機能
- フルアラート機能とわかりやすいウェブベースのタイムエラーグラフ
- GUIまたはCLIによる管理
- 金融市場向けの長期間の監査トラッキング（オプション）
- LinuxまたはWindows Serverのサポート
- TimeKeeper Serverで数百のクライアントの時刻同期と管理が可能

Visibility Support Programs

柔軟なサポートオプション

キーサイトの可視化製品のサポートオプションの特長を、以下に示します：

- 迅速な対応と問題の解決
- 立ち上げから、構成、デバッグ、新機能／サービスの展開まで、テクノロジーのライフサイクルをサポート
- ハードウェア修理またはフィールド交換対応による迅速なサービス
- 変化するビジネスニーズをサポートする最新リリースおよび機能
- 新機能、機能拡張、パッチを含む最新のソフトウェアリリースへの即時アクセス
- 技術記事、ブラックブック、製品ドキュメント、ライセンス管理の幅広いライブラリをオンラインで簡単に利用可能
- 日常的なソフトウェアスキャンによるプロアクティブな可視化と一般的なゼロデイ脆弱性に対する修正
- 3つのサポートレベルのオプション

Support agreement features	Basic[1]	Essential	Enterprise 24/7
Response time	1 – 2 business days	2 business hours	2 clock hours
Live support (business hours)	✓	✓	✓
After-hours live support	—	—	24x7x365
After-hours software / hardware upgrades and debug	—	—	24x7x365
Repair service	Return and repair[2]	Advanced hardware replacement	Advanced hardware replacement
Advanced hardware replacement[3]	First 90 days after new product shipment	✓	✓
Expedited hardware shipment from regional inventory[4]	—	✓	✓
Phone, email, customer portal access (business hours)	✓	✓	✓
After-hours phone, email, customer portal	—	—	24x7x365
Software upgrades and bug fix patches[5]	✓	✓	✓
Resource library 24/7	✓	✓	✓
Customer satisfaction health checks	✓	✓	✓
Dedicated support advocate for escalation and QBR[6]	—	—	✓

1. Purchase includes 12-month basic support after product shipment.
2. Requires seven to 10 business days to repair equipment.
3. Replacement hardware shipped in one to two business days.
4. Only available in select countries. Please contact your local Keysight representative.
5. New feature software upgrades, service pack enhancements, bug fix patches, and emergency hot fixes.
6. At your request, and up to once per calendar quarter, a director-level support advocate for escalation will meet with you for a quarterly business review. You will discuss existing and closed technical support cases and updates on any open actions, and you may share your insight into areas where we can improve.

キーサイトの製品により、設計、エミュレーション、テストの課題を迅速に解決し、最高の製品体験を生み出すことで、
技術革新の限界を押し広げることができます。www.keysight.co.jpでイノベーションを始めましょう。

KEYSIGHT