

A background graphic of a network diagram consisting of numerous light blue circular nodes connected by thin, light blue lines, forming a complex web-like structure that is denser on the left side and fades towards the right.

Gain Insight into Your Network

savvius™

Während andere Monitoring Systeme noch Fehler melden, haben Sie diese mit OmniPeek längst gelöst!

Mit der OmniPeek Produktfamilie von Savvius haben Sie permanent und standortübergreifend die „Gesundheit“ Ihres Netzwerks im Blick. Kommunikationsfehler können rasch identifiziert, Probleme bereits im Vorfeld vermieden und die Anzahl der Techniker-Einsätze vor Ort erheblich minimiert werden. Sie erkennen auf einfache Weise Trends, können im Bedarfsfall aktiv entgegenwirken und dadurch die IT-Dienstgüte deutlich verbessern.

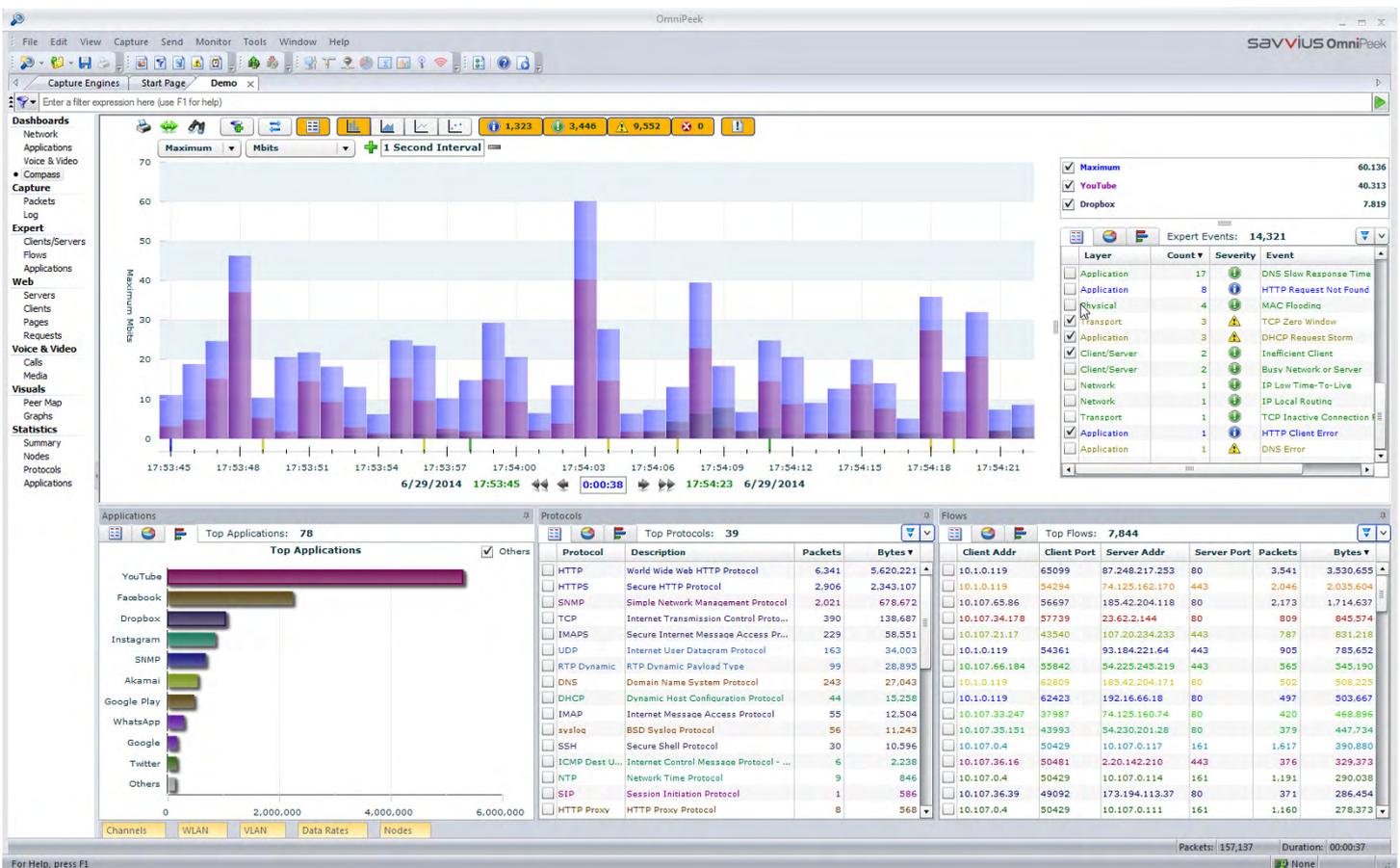
OmniPeek liegt eine Konsolen/Agenten Architektur zugrunde. Die einzelnen Ausprägungen bieten Funktionalitäten für die Anforderungen von Rechenzentren sowie Unternehmens- und Provider-Netzwerken jeglicher Größe.

OmniPeek analysiert Protokolle im Ethernet & Wireless LAN über alle OSI Layer hinweg. Als erste Netzwerk Analyse Software mit einem graphischen User Interface wurde die Technologie in über 25-jähriger Entwicklungsarbeit für eine schnelle und intuitive Identifizierung von Performance-Engpässen, Drill Down auf Paket Level und Fehlerfindung optimiert.

Fehlerzustände werden visualisiert und sämtliche Unklarheiten beseitigt. OmniPeek hält, was es verspricht und sorgt für einen klaren Blick auf die Vorgänge im Netzwerk.

Highlights:

- Best of Breed für Messungen im Ethernet bis 40 Gbit/s, Wireless 802.11a/b/g/n/ac und in virtuellen Umgebungen
- Einfache globale Analyse von Laufzeiten, Paket Verlust und Retransmissionen
- Auswertung sowohl online als auch offline über größere Zeiträume
- Flow“-basierende Experten-Analyse über alle OSI Layer
- Umfangreiche Metriken für Netzwerk- und Applikationslatenz sowie Voice & Video Qualität
- Intuitiv zu verstehende Statistiken über Kommunikationspartner, Protokolle und welche Verkehrsmerkmale die Performance von Applikationen im Netzwerk beeinträchtigen
- Von der Übersicht ins Detail mit exzellenten Drill-Down Funktionen
- Integration in Unternehmensrichtlinien (Datenschutz & Sicherheit)
- Skalierbar für individuelle Anforderungen von Netzwerken jeglicher Größe



Compass - das interaktive Network Dashboard von OmniPeek mit Application Classification

OmniPeek Enterprise

Flows analyzed: 74
Events detected: 266

Name	Packet	Delta Time	Packet Visualizer	Acked By	Ack For	Summary	Expert
1197	0.000000					IP L= 44 TCP ...S. S=1818123863 L= 0 ...	
1199	0.010014					IP L= 40 TCP .A..S. 1818123864=L L= 0 S= 916416000...	
1328	0.991425					IP L= 40 TCP .A... S=1818123864 L= 0 S= 916416001...	
1449	0.851224			1528		IP L= 122 TCP .AP... 1818123864=A L= 82 S= 916416001...	
1528	0.630907			1529	1449	IP L= 80 TCP .AP... S=1818123864 L= 40 S= 916416003...	
1529	0.000000			1622	1528	IP L= 66 TCP .AP... 1818123104=A L= 26 S= 916416003... SMTP Server Returned Error	
1622	0.751080			1626	1529	IP L= 80 TCP .AP... S=1818123104 L= 40 S= 916416109...	
1626	0.010014			2109	1622	IP L= 118 TCP .AP... 1818123144=A L= 78 S= 916416109...	
1760	1.131627					IP L= 40 TCP .A.... 1818123184=A L= 0 S= 916416187...	
2109	2.613758			2132	1626	IP L= 67 TCP .AP... S=1818123184 L= 27 S= 916416234...	
2132	0.150216			2109	IP L= 40 TCP .A.... 1818123211=A L= 0 S= 916416234...		
2228	0.630507					IP L= 39 S= 916416234... SMTP Slow Response Time (0.781123 seconds)	
2271	0.330475					IP L= 6 S= 916416273...	
2274	0.030043					IP L= 0 S= 916416273...	
2280	0.030043					IP L= 50 S= 916416273...	
2328	0.360518					IP L= 0 S= 916416323...	
2352	0.200288					IP L= 0 S= 916416323...	
2429	0.520748					IP L= 8 S= 916416323...	
2440	0.000096						
2441	0.000000						
2453	0.070100						
2454	0.000000						
2459	0.030043						
2468	0.050072						

Go to Packet 2228
Decode Packet 2228
Save PacketVisualizer Data...
Absolute Seq/Ack Numbers
Relative Seq/Ack Numbers

Packet	Source	Destination	Size	Delta Time	Protocol	Summary
2109	169.199.29.5	192.216.124.1	85	2.613758	SMTP	C PORT=2778 RCPT TO:<tim@aggroup.com>
2132	192.216.124.1	169.199.29.5	64	0.150216	SMTP	Src= 25,Dst= 2778,.A....,S= 916416234,L= 0
2228	192.216.124.1	169.199.29.5	97	0.630507	SMTP	C PORT=2778 250 <tim@aggroup.com>... Recipient
2271	169.199.29.5	192.216.124.1	64	0.330475	SMTP	C PORT=2778 DATA
2274	192.216.124.1	169.199.29.5	64	0.030043	SMTP	Src= 25,Dst= 2778,.A....,S= 916416273,L= 0

Ethernet Type 2
Destination: 00:00:0C:5D:10:46 Cisco:5D:10:46 [0-5]
Source: 08:00:2B:1D:0D:9C DigitalEqu:1D:0D:9C [6-11]
Protocol Type: 0x0800 IP [12-13]

IP Version 4 Header - Internet Protocol Datagram
Version: 4 [14 Mask 0xF0]
Header Length: 5 (20 bytes) [14 Mask 0x0F]
Diff. Services: 00000000 [15]
Total Length: 79 [16-17]
Identifier: 33109 [18-19]
Fragmentation Flags: 0000 [20 Mask 0xE0]
Fragment Offset: 0 (0 bytes) [20-21 Mask 0x1FFF]
Time To Live: 60 [22]
Protocol: 6 TCP - Transmission Control Protocol [23]
Header Checksum: 0xF9AD [24-25]
Source IP Address: 192.216.124.1 [26-29]
Dest. IP Address: 169.199.29.5 [30-33]

Der Troubleshooting Prozess auf einen Blick: Vom Expert Event zum betroffenen Flow, in den betroffenen Flow und zu den relevanten Paketen!

OmniPeek Enterprise ist das Flaggschiff der Protokoll Analyser von Savvius und bietet die volle Funktionstiefe inklusive Informationsgewinnung aus nahezu jedem relevanten Netzwerk-Segment einschließlich 1/10/40 Gigabit, 802.11a/b/g/n und ac (über Access Points von Cisco und Aruba), via NetFlow, sFlow, TCP Dump, RPCAP, eigenem Capture Assistant, u.v.m.

umfassende Erkennung und Analyse von Applikationen. Darüber hinaus liefert OmniPeek Enterprise sehr detaillierte Metriken für Voice & Video, inkl. Jitter, Packet Loss, Netzwerk-Delay, Signalisierung, Sprach- und Bildqualität nach MOS, R-Faktor und verfügt über ausgeklügelte Funktionen zur Multi Segment Analyse.

OmniPeek bietet eine herausragende visuelle Aufbereitung der Verkehrsflüsse auf dem PHY- und IP-Layer, ein führendes Expertensystem für alle OSI-Schichten sowie eine

OmniPeek Enterprise ist das ideale Werkzeug für Techniker, die im operativen Betrieb für die Einhaltung der IT Dienstgüte verantwortlich sind.

Dashboards
Network
Voice & Video
Apdex
Compass
Capture
Packets
Log
Expert
Clients/Server
Flows
Applications
Web
Servers
Clients
Pages
Requests

Call Nu...	Name	Call Status	End Cause	Codec	Media Type	Packets	MOS-Low	Start	Duration
1	Unknown-->Unknown	Closed	over timeout	G.729A	Voice	823	1.62	16.04.2007 13:08:49	11.385303
2	Unknown-->Unknown	Closed	over timeout	G.729A	Voice	948	1.66	16.04.2007 13:08:49	12.443036
93	587391360-->0243671008	Closed	Busy here	G.729A	Voice	114	2.41	16.04.2007 13:27:47	1.574391
21	587391360-->0228333025	Closed	Not Found	G.729A	Voice	150	2.61	16.04.2007 13:11:42	1.905845
51	587391360-->0243671008	Closed	Busy here	G.729A	Voice	81	2.61	16.04.2007 13:16:27	1.214668
7	587391358-->0227371824	Closed	Request Terminated	G.729A	Voice	1117	2.96	16.04.2007 13:09:21	11.810553
14	Unknown-->Unknown	Closed	over timeout	G.729A	Voice	1856	3.01	16.04.2007 13:10:16	19.019471
15	587391360-->0226163394	Closed	BYE	G.729A	Voice	4629	3.01	16.04.2007 13:10:17	47.347988
29	587391358-->0227291695	Closed	Request Terminated	G.729A	Voice	7058	3.01	16.04.2007 13:12:32	00:01:12.443027
73	587391360-->0223320880	Closed	Service Unavailable	G.729A	Voice	153	3.01	16.04.2007 13:22:08	1.959748
87	587391358-->0227981809	Closed	Request Terminated	G.729A	Voice	3727	3.01	16.04.2007 13:25:43	38.318833
9	587391359-->0224364050	Closed	BYE	G.729A	Voice	7405	3.06	16.04.2007 13:09:40	00:01:15.450836
22	587391356-->0225347400	Closed	BYE	G.729A	Voice	7026	3.06	16.04.2007 13:11:50	00:01:11.961427
23	587391360-->0228275820	Closed	Not Found	G.729A	Voice	194	3.06	16.04.2007 13:11:58	2.545960
30	587391361-->0895339413	Closed	BYE	G.729A	Voice	3265	3.06	16.04.2007 13:12:38	33.532994

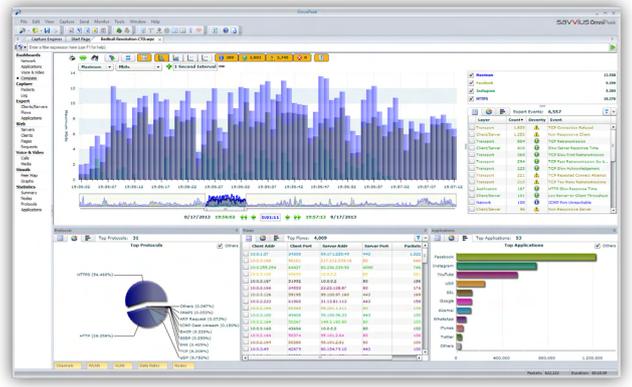
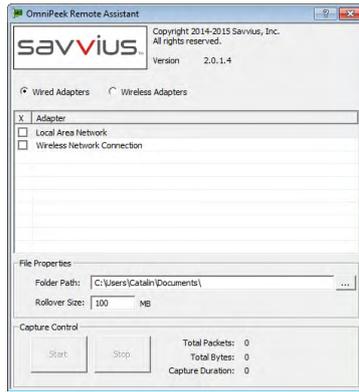
Details
Name Value
Call Number 21
Caller Address 193.24.221.138
Callee Address 217.119.66.231
Call ID cal-F1901AFB-10CE-2910-041E-3134@192.168.1.101
Call Status Closed
End Cause Not Found
Signaling SIP
Media Flows 2
Media Packets 141
Media Frames 282
Control Flows 1
Control Packets 1
Signaling Flows 1
Signaling Packets 8
Packets 150

Media Stream
Codec G.729A
Bit Rate 8000
Media Type Voice
Setup Time 0.029426
PDD 0.315453
Start 16.04.2007 13:11:42
Finish 16.04.2007 13:11:44
Duration 1.905845
MOS-Low 2.61

Call Nu...	SSRC	Name	End Cause	Codec	Media Type	Start	Duration	Jitter	Packet Loss %	MOS-CQ
93	00005DDB	G.729A 193.24.221.138:10962-->217.119.66.231:16660	Busy here	G.729A	Voice	16.04.2007 13:27:48	1.080	0.000	9.091	2.41
93	37A14B06	G.729A 193.24.221.138:10962<--217.119.66.231:16660	Busy here	G.729A	Voice	16.04.2007 13:27:48	1.079	0.000	0.000	3.87

Beispiel für Voice & Video Metriken, Übersicht Calls View und Eingrenzung der Fehlerursache nach RTP Media Stream (unten)

Capture Assistant for OmniPeek.

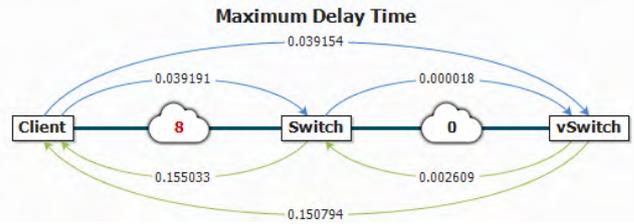


Kosteneffizienter Troubleshooting Prozess mit Capture Assistant für OmniPeek

Capture Assistant für OmniPeek ist ein Bestandteil der Enterprise Version und als solches ein kompaktes und sicheres Programm, das auch von Personen ohne größeren technischen Background betrieben werden kann. Der Anwender muss es nur ausführen (nicht installieren), die Aufzeichnung seines Problems starten (und stoppen) und anschließend die erzeugte Datei zum Analyse-Verantwortlichen zurückschicken.

Gleichzeitig könnte der Administrator bei Bedarf einen weiteren Capture Assistant auf dem jeweiligen (virtuellen) Server starten und so innerhalb kürzester Zeit eine Mehrpunkt Messung anstoßen.

Die Dateien sind vor Fremdzugriff durch öffentlich-private Verschlüsselung gesichert und können nur vom Erzeuger des jeweiligen Capture Assistant geöffnet werden, da sie an die Seriennummer seines OmniPeek gebunden sind. So garantiert der Capture Assistant höchstes Datenschutz Niveau.



Beispiel der Laufzeit Visualisierung einer Multi Segment Analyse nach einer Drei-Punkt-Messung

OmniPeek Professional

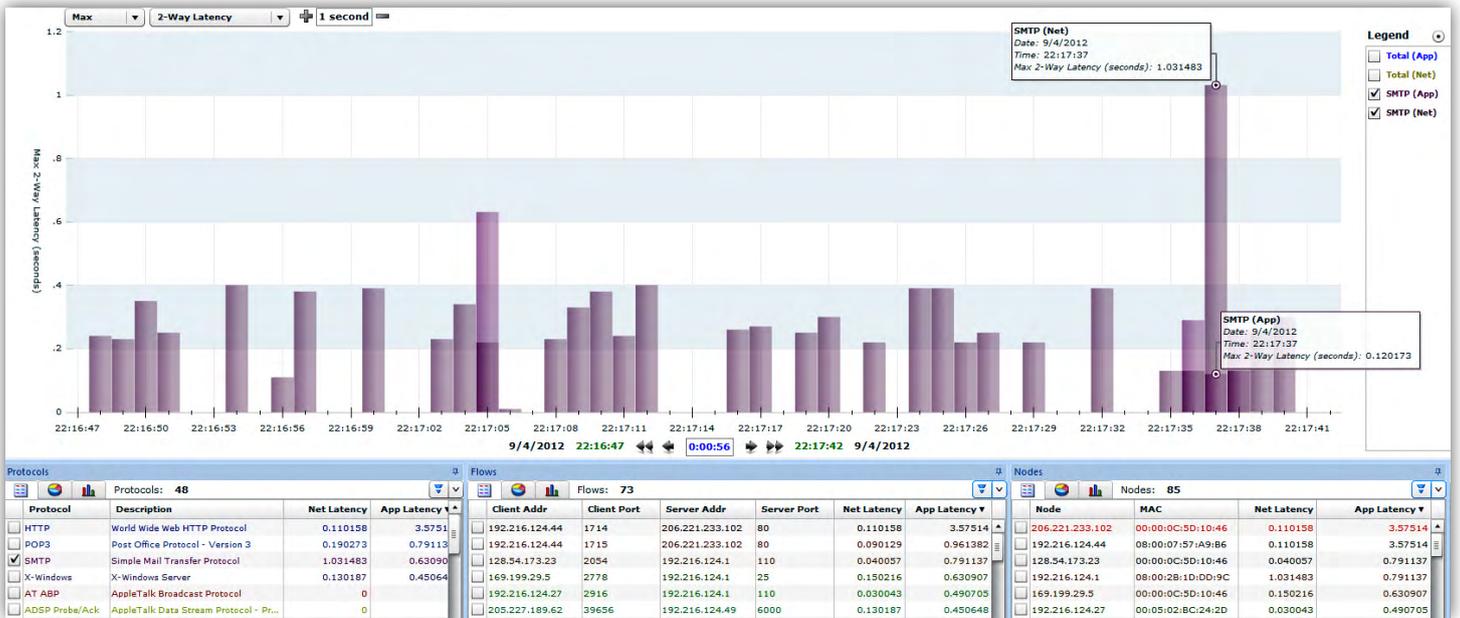
Node	Type	Channel	Frequency	Band	Trust	Cur. Signal	Cur. Noise	Total Bytes	Total Packets	Retry Packets
Red Bull Free WiFi	ESSID	1, 5, 9, 13, ...								
Xirrus:88:60:91	AP	104	5520 MHz	802.11a	Unknown	26	20	1,242,288	4,977	4,133
00:88:65:BA:57:50	STA	104	5520 MHz	802.11a	Unknown	42	23	75,156	436	16
00:88:65:BA:57:50	STA	108	5540 MHz	802.11a	Unknown	31	7	2,995	31	0
20:64:32:76:1F:D9	STA	104	5510 MHz	802.11n	Unknown			1,036	41	25
38:48:4C:26:90:87	STA	108	5540 MHz	802.11n	Unknown			596	8	0
38:48:4C:26:90:87	STA	104	5520 MHz	802.11a	Unknown			60,944	392	24
4C:8D:79:8A:AB:DA	STA	108	5540 MHz	802.11a	Unknown			18,209	66	0
4C:8D:79:8A:AB:DA	STA	104	5520 MHz	802.11a	Unknown			52,736	218	1
90:18:7C:5C:96:FD	STA	104	5520 MHz	802.11a	Unknown			2,197	24	0
94:CE:2C:7F:76:8C	STA	104	5520 MHz	802.11a	Unknown			1,156	47	0
F4:F1:5A:42:23:57	STA	104	5520 MHz	802.11a	Unknown			135,034	551	0
Xirrus:88:60:A1	AP	132	5660 MHz	802.11a	Unknown			34,448	139	42
00:88:65:BA:57:50	STA	132	5660 MHz	802.11n	Unknown			408	12	2
F4:1B:A1:CC:74:68	STA	132	5660 MHz	802.11a	Unknown			308	11	10
Xirrus:88:60:B1	AP	116	5580 MHz	802.11a	Unknown			1,021,770	4,580	3,690
SamsungE1:38:AC:F0	STA	116	5580 MHz	802.11n	Unknown			1,186	32	5
00:88:65:BA:57:50	STA	120	5600 MHz	802.11a	Unknown			364	14	8
00:88:65:BA:57:50	STA	116	5580 MHz	802.11a	Unknown			62,525	602	92
40:B3:95:C7:3E:83	STA	116	5580 MHz	802.11a	Unknown			317,642	1,052	4
40:B3:95:C7:3E:83	STA	128	5640 MHz	802.11a	Unknown			28	1	1
98:08:E3:F0:A8:E7	STA	120	5600 MHz	802.11a	Unknown			140	5	4
98:08:E3:F0:A8:E7	STA	116	5580 MHz	802.11a	Unknown			1,204	43	36
98:FE:94:36:BD:48	STA	116	5580 MHz	802.11a	Unknown			77,411	474	19
Xirrus:88:60:C1	AP	13	2472 MHz	802.11bg	Unknown			19,258	145	7
Apple:44:23:92	STA	13	2472 MHz	802.11bg	Unknown			789	6	1
Apple:63:89:86	STA	36	5180 MHz	802.11n	Unknown			42	2	0
Apple:6E:B3:F2	STA	13	2472 MHz	802.11bg	Unknown			3,595	57	18
Apple:99:86:13	STA	13	2472 MHz	802.11bg	Unknown			32,427	159	24

WLAN View in OmniPeek – nur ein Beispiel für die vielfältigen Analyse Möglichkeiten für 802.11 a/b/g/n/ac

Robuster Analyzer analog OmniPeek Enterprise, jedoch ohne erweiterte Web, Voice- & Video-Analyse. Ideal für Netzwerker und Dienstleister im klassischen Umfeld, ohne dedizierten Einsatzzweck für neue Medien.

Einzigartig ist die Möglichkeit, Verkehrsflüsse gleichzeitig auf Wireless und Ethernet Seite aufzuzeichnen, um sofort zu klären: Ist es ein WLAN Problem oder nicht?

OmniPeek Connect

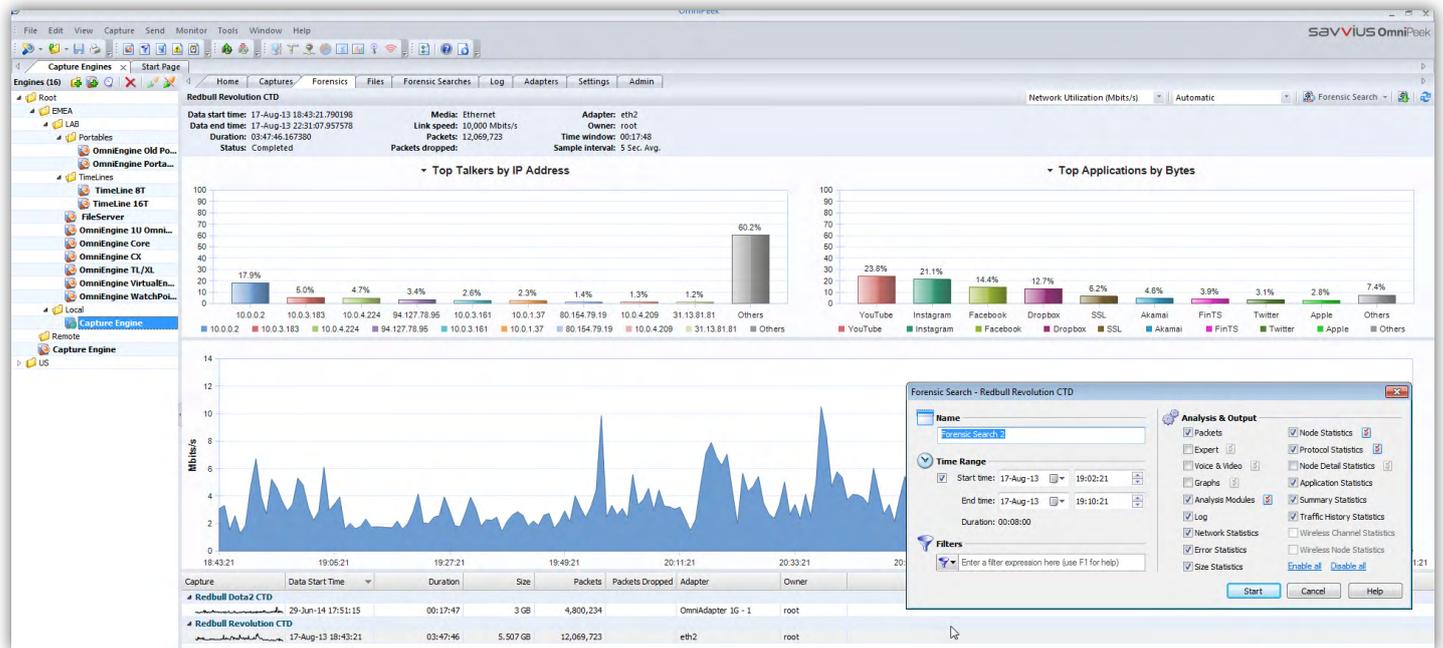


Ansicht für 2 Way Latency: Compass zeigt die Antwortzeiten getrennt nach Netzwerk und Applikation auf! Auch per Protokoll, per Flow oder IP Adresse

OmniPeek Connect ist die Konsole zum Verbinden auf Remote Agenten (OmniEngines) und die bevorzugte Lösung für Mitarbeiter in einem Network Operation Center (NOC).

In Verbindung mit einer OmniEngine Enterprise bietet OmniPeek Connect in etwa die gleichen Features wie OmniPeek Enterprise.

Capture Engine for OmniPeek



OmniEngine ist für 24/7 Monitoring optimiert und bietet beste Funktionalitäten um große Datenvolumina verlustfrei aufzuzeichnen und zu analysieren

Mit der Capture Engine für OmniPeek können Techniker komfortabel das gesamte unternehmensweite Netzwerk im 24/7 Modus überwachen, Fehler schnell identifizieren und Performance-Engpässe beheben, ohne dabei das eigene Büro verlassen zu müssen.

Die Capture Engine läuft auf Standard-Windows-Servern ebenso wie auf schlüsselfertigen Omnipliance Network Recorder von Savvius. Installiert man die Engines an jedem Standort, erhält man Echtzeit-Analysen der IT-Dienstgüte in den jeweiligen Segmenten der Niederlassungen.

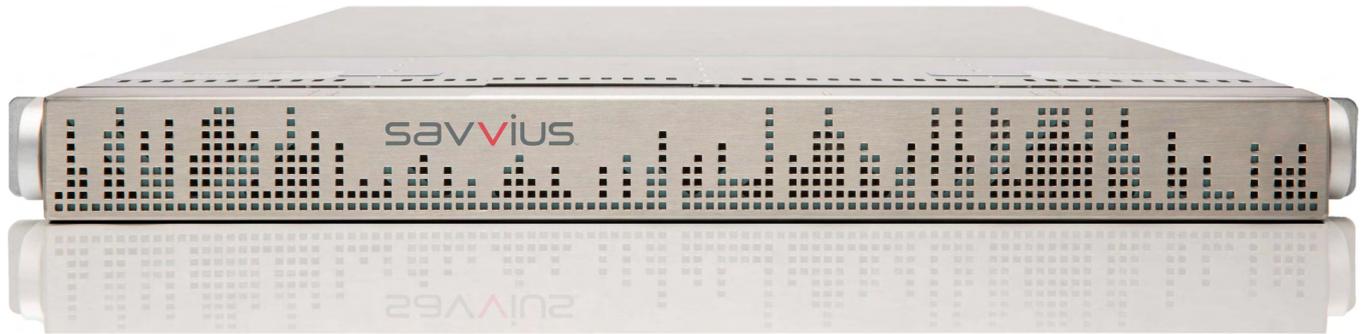
Die Remote Agenten sind zentral verwaltbar, verfügen über ein hierarchisches Benutzersystem (wer darf was?) mit

exaktem Logging (wer was wann?) und können zudem in gängige Sicherheitslösungen (Radius, TACACS, Active Directory, etc.) integriert werden.

Die Capture Engine analysiert den aufgezeichneten Datenverkehr vor Ort (im Rechenzentrum, in der Niederlassung, etc.) und stellt die Ergebnisse bandbreitenschonend der OmniPeek Konsole zur Verfügung.

Die Capture Engine für OmniPeek ist wahlweise als Version für Windows basierte Systeme zum Eigenbau oder als komplett konfigurierte Linux Appliance verfügbar.

Omniplance Network Recorder



Die Omniplance Turnkey Lösungen bieten einen unschlagbar schnellen Workflow für die Analyse von 1/10/40G Ethernet Segmenten und benötigen im Vergleich zu manchem Mitbewerber nur die Hälfte an Platz, Kühlung und Strom. Management, Konfiguration und Version Updates können bestechend einfach durchgeführt werden. Allgemein ist der unkomplizierte Support von Savvius dafür bekannt, ausschließlich zufriedene Kunden zu hinterlassen.

Omniplance[®] CX

Omniplance CX ist die Einstiegslösung in die Welt der Savvius Turnkey Lösungen mit einer Höheneinheit und 4/8/16 TB Speicherplatz. Omniplance CX kommt mit einem 1G High Performance Adapter und ist empfohlen für Gigabit Ethernet mit einer durchschnittlichen Auslastung von ca. 1-2 Gbit/s (Spitze 3,8 Gbit/s)

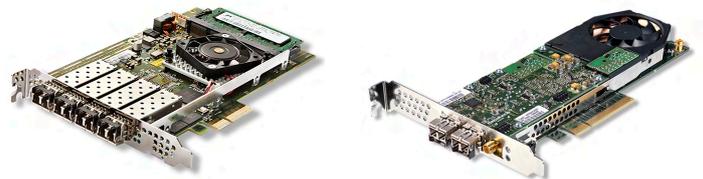
Omniplance[®] MX

Omniplance MX ist das Mittelklasse Modell mit drei Höheneinheiten und mit 16 oder 32 TB Speicherplatz verfügbar. Die Omniplance MX kann mit bis zu vier 1G oder 10G High Performance Adapter in jeglicher Kombination bestückt werden. Empfohlen für das Monitoring von aggregierten Leitungen mit einer durchschnittlichen Auslastung von ca. 5 Gbit/s, wobei noch weitere 3-4 Gbit/s Puffer für das Abfangen von Lastspitzen zur Verfügung stehen.

Omniplance[®] TL

Omniplance TL ist das Flaggschiff Produkt von Savvius und bis zu 20 Gbit/s Aufzeichnungsrate aktuell sicherlich Spitzenreiter bei Performance/Kostenbetrachtungen im HighEnd Bereich. Omniplance TL ist in Variationen von 32, 48 und 64 TB Speicherplatz verfügbar und kann mit bis zu vier High Performance 1G, 10G oder 40G Adapter in jeglicher Kombination bestückt werden. Zusätzlicher externer Storage ist in Einheiten von 32, 48 und 64 TB erhältlich.

Adapter Versionen



1G (High Performance) Adapter for Omniplance ist eine PCI Express Netzwerk Analyse Karte mit 4 Ports, welche bis zu zwei Gigabit Links im Full Duplex oder vier Gigabit Links im Halb Duplex Modus aufnehmen kann. Der High Performance 1G Adapter kann wahlweise mit SR, LR oder Kupfer SFP bestückt werden.

10G (High Performance) Adapter for Omniplance ist eine PCI Express Netzwerk Analyse Karte, wahlweise mit zwei oder vier optischen 10G Schnittstellen verfügbar und kann dementsprechend viele 10G Links aufnehmen. Der High Performance 10G Adapter kann wahlweise mit SR oder LR SFP+ bestückt werden.

40G (High Performance) Adapter for Omniplance ist eine Ein-Port PCI Express Netzwerk Analyse Karte kommt mit einem optischen QSFP+.

WLAN USB Capture Adapter

Der WLAN USB Capture Adapter für OmniPeek unterstützt die Aufzeichnung auf allen obligatorischen 802.11a/b/g/n Kanälen (auch 3-stream bis zu 450 mbit/s). Mit mehreren USB Capture Adaptern kann man auf entsprechend vielen Kanälen gleichzeitig aufzeichnen und eine Roaming Analyse sowohl auf Layer 2 (Zeit des Verbindungsaufbaus) als auch Layer 7 (wann fließt tatsächlich wieder Datenverkehr?) durchführen. Für empfohlene Adapter zur Aufzeichnung von 802.11ac Verkehr kontaktieren Sie uns bitte – die Technik schreitet hier sehr schnell voran.



Omnipliance® Portable



Die Omnipliance Portable wird von führenden Netzwerk-Analyse-Profis unumstritten als das derzeit attraktivste mobile Analyse Gerät betrachtet. Entwickelt für den Service eines führenden deutschen Telekommunikationsunternehmens, vereint das Gerät alle Eigenschaften und Fähigkeiten der in über 25 Jahren Entwicklungsarbeit gereiften Savvius-Technologien. Das Gerät kommt aktuell mit 6 TB und je einem 1G und 10G Adapter. Ausreichend für durchschnittlich 10 Gbit/s Auslastung. Wir empfehlen, die Omnipliance einfach unverbindlich zu testen.

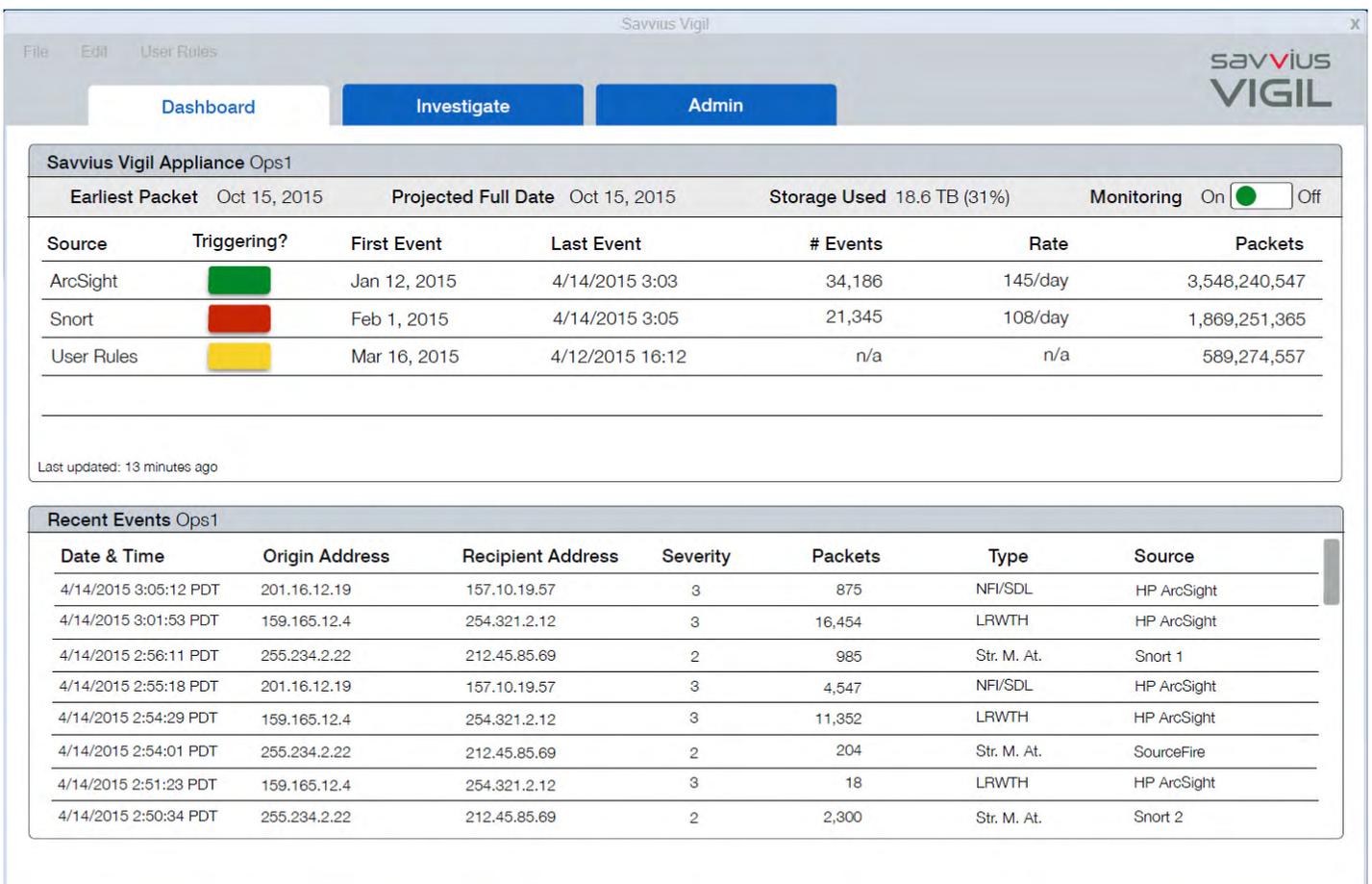
savvius VIGIL



Einbrüche in Firmennetze bzw. Datenklau und -manipulation finden oft unbemerkt statt und werden erst später (im Schnitt 229 Tage), wenn die Auswirkungen sichtbar werden, von der Security Abteilung entdeckt. Savvius Vigil kann in bestehende SIEM IDS/IPS Ressourcen integriert werden, um nicht nur die auslösenden Pakete von verdächtigen Events, sondern die komplette Kommunikation dazu zu speichern. Insbesondere den Verbindungsaufbau mit den für Netzwerk Forensiker relevanten Informationen. Savvius Vigil kombiniert dazu frei konfigurierbar Ereignisse aus verschiedenen Quellen (FireSIGHT, ArcSight, Intel Security, Snort, Suricata, etc.). Der Verkehr zwischen relevanten Knoten wird vor, während und nach den auslösenden Ereignissen erfasst. Optional wird auch jeglicher mit der IP-Adresse eines Ereignisses in Zusammenhang stehende Verkehr behalten und für die forensische Analyse aufbereitet.

Highlight:

Durch die jahrzehntelange Erfahrung von Savvius mit der Speicherung von relevantem Netzwerkverkehr wird hier der Arbeitsprozess von operativen SOC Mitarbeitern mindestens um den Faktor 10 beschleunigt.



The screenshot shows the Savvius Vigil web interface. At the top, there are navigation tabs for 'Dashboard', 'Investigate', and 'Admin'. The main content area is titled 'Savvius Vigil Appliance Ops1' and displays monitoring status: 'Earliest Packet Oct 15, 2015', 'Projected Full Date Oct 15, 2015', 'Storage Used 18.6 TB (31%)', and 'Monitoring On'. Below this is a table with columns for Source, Triggering?, First Event, Last Event, # Events, Rate, and Packets. The 'Recent Events Ops1' section at the bottom contains a table with columns for Date & Time, Origin Address, Recipient Address, Severity, Packets, Type, and Source.

Source	Triggering?	First Event	Last Event	# Events	Rate	Packets
ArcSight	Green	Jan 12, 2015	4/14/2015 3:03	34,186	145/day	3,548,240,547
Snort	Red	Feb 1, 2015	4/14/2015 3:05	21,345	108/day	1,869,251,365
User Rules	Yellow	Mar 16, 2015	4/12/2015 16:12	n/a	n/a	589,274,557

Date & Time	Origin Address	Recipient Address	Severity	Packets	Type	Source
4/14/2015 3:05:12 PDT	201.16.12.19	157.10.19.57	3	875	NFI/SDL	HP ArcSight
4/14/2015 3:01:53 PDT	159.165.12.4	254.321.2.12	3	16,454	LRWTH	HP ArcSight
4/14/2015 2:56:11 PDT	255.234.2.22	212.45.85.69	2	985	Str. M. At.	Snort 1
4/14/2015 2:55:18 PDT	201.16.12.19	157.10.19.57	3	4,547	NFI/SDL	HP ArcSight
4/14/2015 2:54:29 PDT	159.165.12.4	254.321.2.12	3	11,352	LRWTH	HP ArcSight
4/14/2015 2:54:01 PDT	255.234.2.22	212.45.85.69	2	204	Str. M. At.	SourceFire
4/14/2015 2:51:23 PDT	159.165.12.4	254.321.2.12	3	18	LRWTH	HP ArcSight
4/14/2015 2:50:34 PDT	255.234.2.22	212.45.85.69	2	2,300	Str. M. At.	Snort 2

Wir identifizieren jedes Netzwerk-, Security und Applikationsproblem!

www.savvius.com

Savvius (ehemals WildPackets) entwickelt seit 1990 Produkte für Netzwerk Analyse und Monitoring, die in über 60 Länder verkauft und in allen Industriebereichen eingesetzt werden. Zu den Kunden zählen in D-A-CH unter anderem A1, Daimler, Deutsche Telekom, Fiducia, Migros, Postbank, Unicredit, VW sowie international Apple, Boeing, Cisco, Microsoft, NTT etc.

savvius[™]

Savvius D-A-CH | Paul-Heyse-Straße 28 | D-80336 München
Contact: emeasales@savvius.com | Phone: +49 89 32 67 64-86