

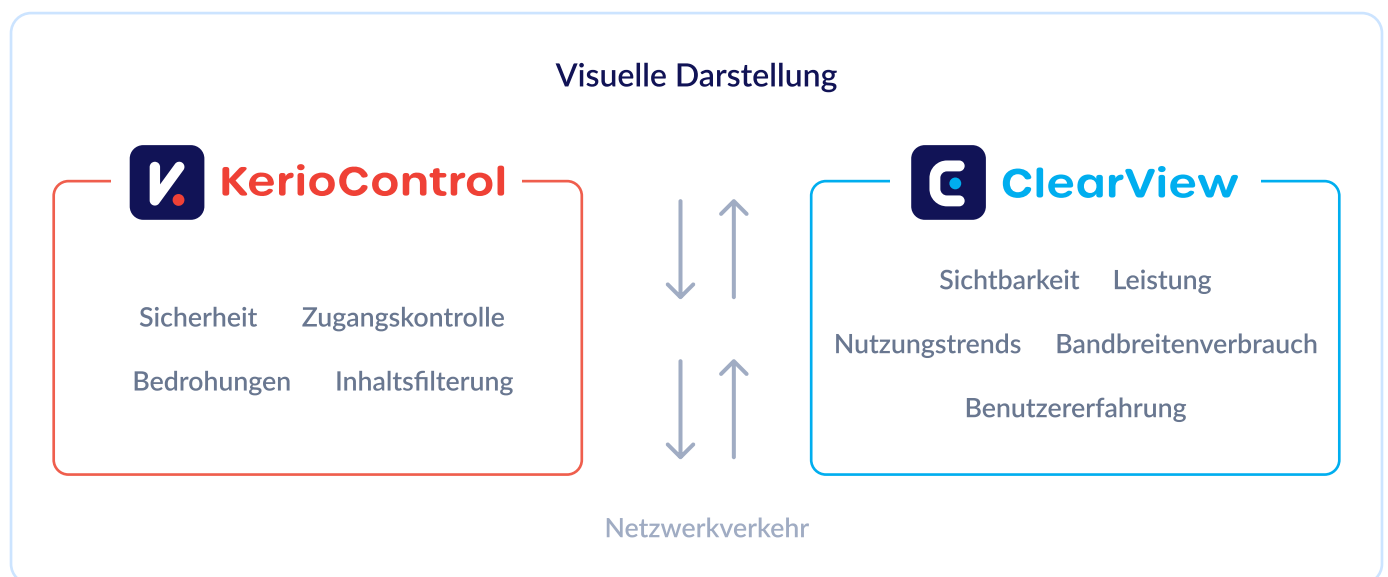


# Wie GFI ClearView GFI KerioControl (Firewalls) ergänzt

In der dynamischen Welt des Netzwerkmanagements durchläuft ein einzelnes Datenpaket mehrere kritische Netzwerkgeräte, die jeweils unterschiedliche Aufgaben erfüllen. Dieses Dokument untersucht, wie GFI ClearView GFI KerioControl wunderbar ergänzt und Organisationen einen integrierten Ansatz für verbesserte Netzwerksicherheit, Leistung und Effizienz bietet.

## Das Leben eines Pakets

Die Reise jedes Datenpakets durch das Netzwerk umfasst entscheidende Berührungspunkte wie Router, Switch, Firewall (GFI KerioControl), Bandbreitenformer und mehr. An jeder Station führen diese Geräte ihre spezialisierten Aufgaben aus, um eine nahtlose Paketzustellung zu gewährleisten. Die Firewall, die auf Sicherheit fokussiert ist, prüft das Paket auf potenzielle Bedrohungen, während GFI ClearView, das die Sichtbarkeit repräsentiert, wertvolle Einblicke liefert, die es Ihnen ermöglichen, die Netzwerkleistung zu optimieren.



## Die Kombination der Linsen



Wenn die beiden Linsen kombiniert werden, verschmelzen sie zu einer leistungsstarken und umfassenden Lösung. Die wachsamen Sicherheitsmaßnahmen von GFI KerioControl passen perfekt zu der tiefen Sichtbarkeit von GFI ClearView und bilden zusammen die ideale Kombination für Netzwerkadministratoren, um einen ganzheitlichen Überblick über die Gesundheit ihres Netzwerks zu erhalten.

## Echtzeit-Szenario - Gregs Netzwerkprobleme

Um die Beziehung zwischen GFI KerioControl und GFI ClearView besser zu verstehen, folgen wir Greg, dem Vertriebsleiter eines Softwareunternehmens. In den letzten Wochen hatte Greg während kritischer Videoanrufe mit Kunden Probleme, da die Audio- und Videoqualität bei fast 50 % seiner Anrufe abnahm. Das Netzwerkteam konnte beim Untersuchen durch die Firewall die Ursache nicht identifizieren, da die Verbindungsdiagramme nicht genügend Informationen oder Kontext lieferten.

Traffic Rule ▲	Service	Source IP	Destination IP	Destination Hostname	Destination Cou...
Internet access (NAT)	HTTPS	10.10.10.11	142.250.181.142	clients4.google.com	United States
Internet access (NAT)	HTTPS	10.10.10.11	170.114.52.2	zoom.us	United States
Internet access (NAT)	HTTPS	10.10.10.11	170.114.15.223	logfiles.zoom.us	United States
Internet access (NAT)	HTTPS	10.10.10.11	170.114.52.2	zoom.us	United States
Internet access (NAT)	HTTPS	10.10.10.11	170.114.52.2	zoom.us	United States
Internet access (NAT)	HTTPS	10.10.10.11	142.250.181.74	presence.googleapis.com	United States
Internet access (NAT)	443/UDP	10.10.10.11	172.217.17.46	clients6.google.com	United States
Internet access (NAT)	8009/TCP	10.10.10.11	192.168.18.97	192.168.18.97	

Active since ▲	Event Type	Description
13:31:09	 HTTP connection	Connection to timecard-server.crossovertool.com, service HTTPS (1.18 MB transferred)
13:32:18	 Large data transfer	Unknown connection to zoomsinqp23mmr.sin.zoom.us, service 8801/UDP (8.32 MB transferred)

## Einführung von GFI ClearView ins Netzwerk

Um ihre Sichtbarkeit zu erhöhen, beschloss das Netzwerkteam, GFI ClearView einzuführen. Die Implementierung verlief reibungslos und störungsfrei, dank der:

- Out-of-Path-Bereitstellung
- Keine Ausfallzeit erforderlich
- Keine HTTPS-Dekodierung erforderlich
- Kompatibilität mit gängigen Hypervisoren.

## Ziele des Netzwerkadministrators mit GFI ClearView

Die drei Hauptziele, die sie im Kopf hatten, waren:

### 1. Echtzeit-Anwendungsleistungsanalysen

Mit der Echtzeit-Anwendungsüberwachung von GFI ClearView konnten sie schnell die Ursache für die schlechte Leistung identifizieren. Sie beobachteten detaillierte Daten zur Anwendungsnutzung und zum Durchsatz in Echtzeit, was es ihnen ermöglichte, festzustellen, dass YouTube und Netflix erhebliche Bandbreite verbrauchten.

External IP (User)	Internal IP (User)	Application	Transfer Rate (kbps)	Packet Rate (pps)	Flows
40.67.254.36	10.10.10.11	Microsoft Services[*..wms.windows.com]	0.523	0	1
162.125.19.131	10.10.10.11	DropBox[bolt.dropbox.com]	0.311	0	1
18.205.93.209	10.10.10.11	Zoom[*..zoom.us]	0.295	0	1
172.217.23.206	10.10.10.11	udp ports 443 -> 53786	0.194	0	1
213.227.162.108	10.10.10.11	TeamViewer	0.158	0	1

Inbound Applications				
Application Name	Transfer Rate (Mbps)	Packet Rate (pps)	Flows	Distribution (%)
<b>Total</b>	<b>32.833</b>	<b>3524</b>	<b>120</b>	
YouTube	32.217	3123	7	<div style="width: 96%;"></div>
Netflix	0.458	247	1	<div style="width: 0%;"></div>
Zoom	0.090	106	5	<div style="width: 0%;"></div>
RDP	0.057	40	46	<div style="width: 0%;"></div>
Google Analytics	0.006	1	2	<div style="width: 0%;"></div>

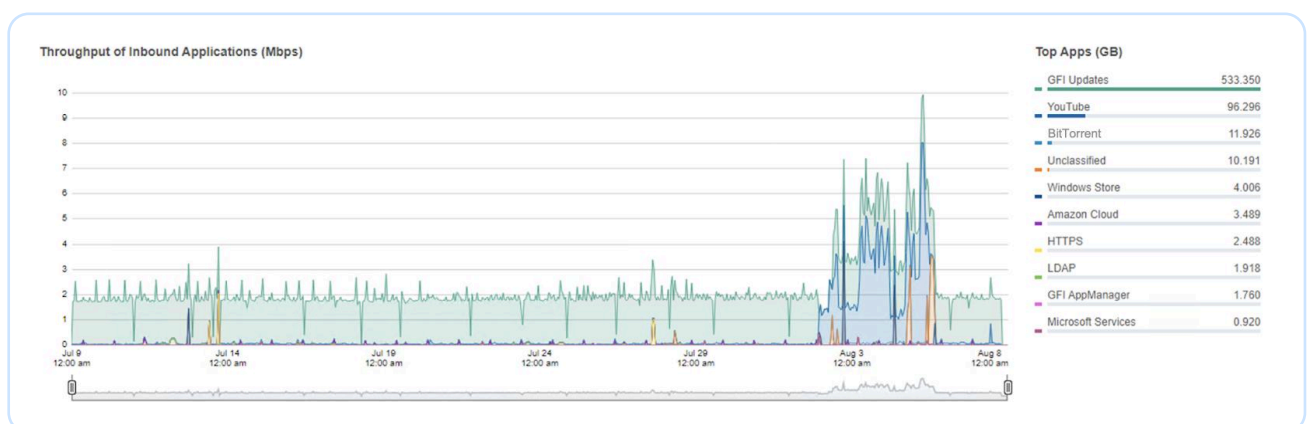
Outbound Applications				
Application Name	Transfer Rate (Mbps)	Packet Rate (pps)	Flows	Distribution (%)
<b>Total</b>	<b>34.350</b>	<b>3395</b>	<b>118</b>	
Netflix	33.982	3063	7	<div style="width: 98%;"></div>
YouTube	0.268	239	7	<div style="width: 0%;"></div>
Zoom	0.062	30	46	<div style="width: 0%;"></div>
RDP	0.030	57	5	<div style="width: 0%;"></div>
Google Analytics	0.004	2	2	<div style="width: 0%;"></div>

Inbound Hosts/Users				
IP Address (User)	Transfer Rate (Mbps)	Packet Rate (pps)	Flows	Distribution (%)
<b>Total</b>	<b>32.166</b>	<b>3407</b>	<b>106</b>	
65.109.95.28 (public_IP)	32.165	3406	91	<div style="width: 99%;"></div>
65.109.95.57	0.000	0	4	<div style="width: 0%;"></div>

Outbound Hosts/Users				
IP Address (User)	Transfer Rate (Mbps)	Packet Rate (pps)	Flows	Distribution (%)
<b>Total</b>	<b>34.321</b>	<b>3373</b>	<b>103</b>	
65.109.95.28 (public_IP)	34.321	3373	91	<div style="width: 99%;"></div>
62.152.2.83	0.000	0	1	<div style="width: 0%;"></div>

### 2. Historische Datenanalyse

Bei der Analyse historischer Daten entdeckten sie zusätzliche Netzwerkbelastungen, wie GFI-Updates und Torrent-Verkehr, die zu Leistungsproblemen zu verschiedenen Zeiten beitrugen.



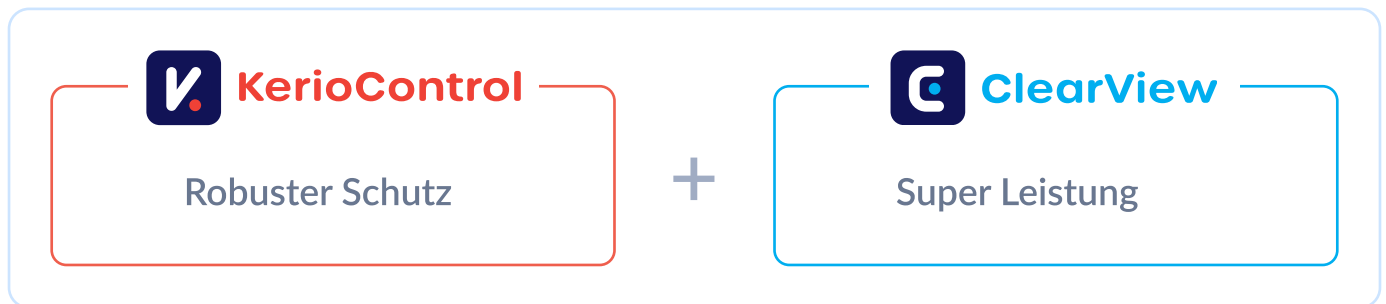
### 3. Proaktive Anwendungsleistungsüberwachung

Nachdem sie die Ursache identifiziert hatten, konnten sie Richtlinien in der Firewall hinzufügen, um die Bandbreitennutzung durch unkontrollierte Anwendungen zu begrenzen. Für zukünftige Fälle wollten sie jedoch proaktiv sein. Daher richteten sie die Anwendungsleistungsüberwachung innerhalb von GFI ClearView für alle kritischen Anwendungen im Unternehmen ein und konfigurierten Akzeptanzschwellen, sodass sie benachrichtigt wurden, wenn die Leistung unter dieses Niveau fiel. Im folgenden Bild sehen Sie, dass Zoom gut funktioniert, da es in einem 5-Minuten-Intervall 9,10 auf einer Skala von 10 erzielt hat.

Name	Score	APS Scores						Loss (%)		RTT (ms)
		Normalized Delays (ms/kb)		Transaction Delays (ms)		Jitter (ms)	Inbound	Outbound		
		Network	Server	Network	Server					
✓ Microsoft Teams Solution Center (8388951)	9.68	30.76	2.43	82.38	3.43	5.56	0.00	0.00	82.28	
✓ YouTube Solution Center (205)	9.26	29.47	23853.11	104.77	2624.64	21.95	0.30	1.30	38.67	
✓ Zoom Solution Center (1007)	9.10	421.40	197.98	199.46	41.65	58.01	0.00	0.00	119.29	

## Verschiedene Linsen, gemeinsamer Boden

Zusammenfassend lässt sich sagen, dass GFI KerioControl (Firewall) und GFI ClearView (Sichtbarkeitstool) die gleichen Daten durch unterschiedliche Linsen betrachten. Sie sind nicht wettbewerbsfähig, sondern ergänzen sich gegenseitig. Die Kombination ihrer spezialisierten Perspektiven befähigt Netzwerkadministratoren, ein vollständiges Bild der Sicherheit, Leistung und Effizienz ihres Netzwerks zu erhalten.



Mit GFI ClearView und GFI KerioControl, die Hand in Hand arbeiten, können Organisationen ein robustes, sicheres und optimiertes Netzwerkumfeld gewährleisten, das den Anforderungen moderner Geschäftsabläufe gerecht wird. Gemeinsam heben sie das Netzwerkmanagement auf neue Höhen und ermöglichen nahtlose Benutzererfahrungen und effiziente Abläufe.

Haben Sie die gleichen Probleme wie Greg?

Kontaktieren Sie uns unter [sales@gfi.com](mailto:sales@gfi.com), um noch heute Ihre GFI ClearView-Testversion zu erhalten.

[Testversion anfordern](#)