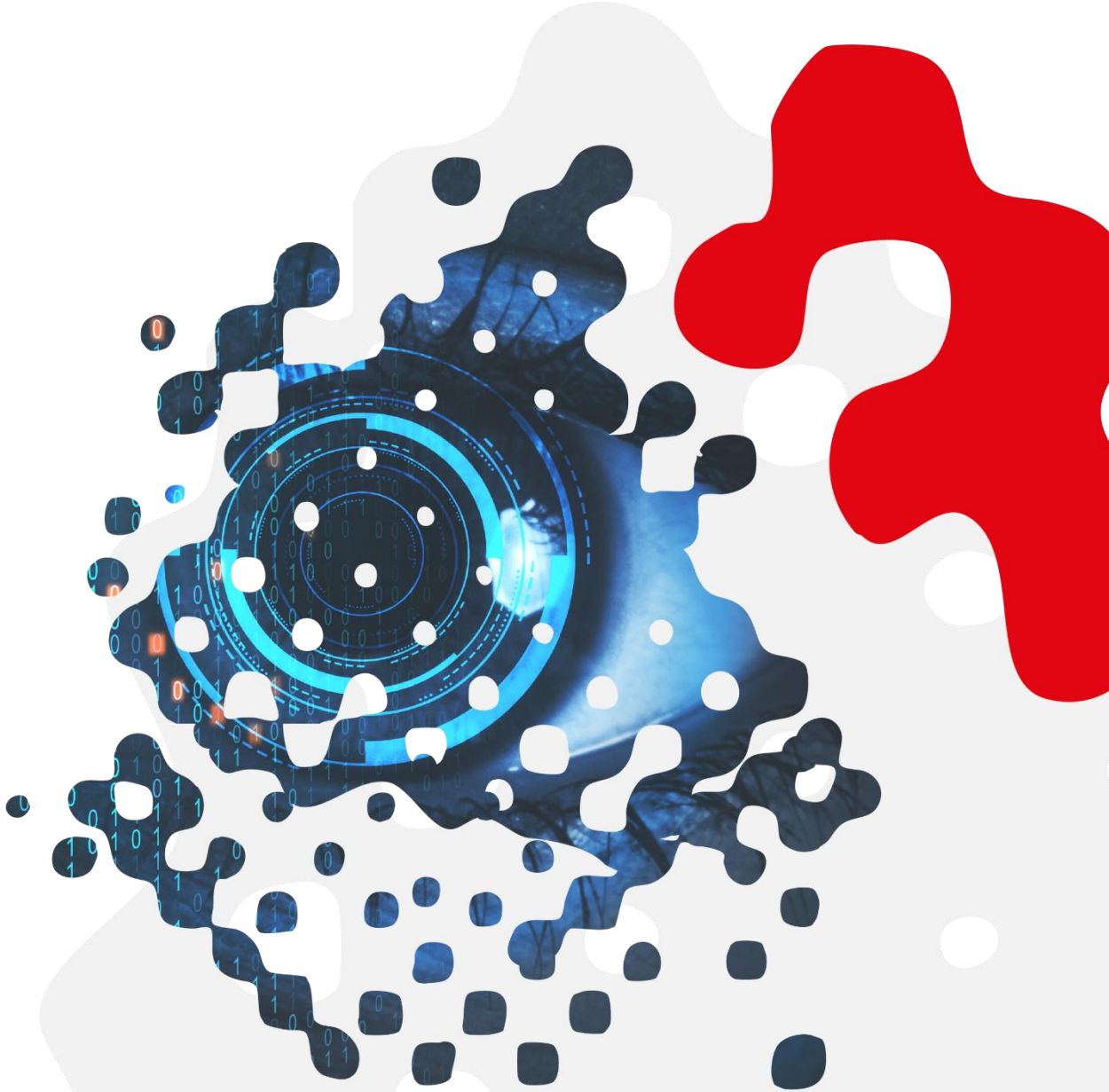
NetEye Conference DACH 2026

Network traffic visibility as a key component of modern IT and security architectures



Rob Cowart
Co-Founder & CEO, ElastiFlow Inc.

WÜRTH | IT

GRAVITATE

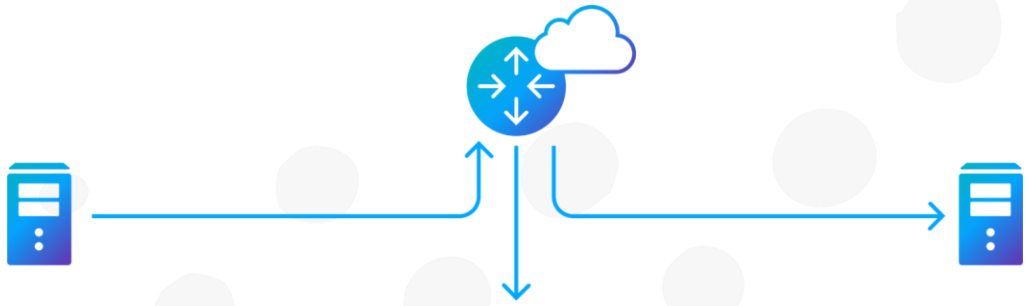
Who is ElastiFlow?

Whether for business, healthcare, entertainment or social connection, we all depend on the reliability, performance and security of network infrastructure to enable the modern world in which we live.

We created ElastiFlow to provide the visibility and insights necessary to make this world possible.



What is "Netflow"?



Source IP	Source Port	Destination IP	Destination Port	IP Protocol	Bytes	Packets
1. 1. 1. 1	53	192. 168. 100. 11	54321	UDP	123	1

Who is talking to Who and How

ElastiFlow

- Visibility
- Context
- Insight

A few statistics about flow data…

60%

flow data as an alternative to packet-based monitoring

61%

flow data for security monitoring

76%

using flow data for traffic monitoring

96%

expect to maintain or expand their use of flow data over the next 12-18 months

A few statistics about flow data… FROM 2011!!!

60%

using flow data as an alternative to packet-based monitoring

61%

using flow data for security monitoring

76%

using flow data for traffic monitoring

96%

expect to maintain or expand their use of flow data over the next 12-18 months

https://www.prnewswire.com/news-releases/ema-and-lancope-reveal-trends-in-netflow-adoption-and-usage-130557563.html

A few statistics about flow data… FROM 2011!!!

60%

using flow data as an alternative to packet-based monitoring

61%

using flow data for security monitoring

76%

using flow data for traffic monitoring

96%

expect to maintain or expand their use of flow data over the next 12-18 months

"using" netflow doesn't mean you are <u>really</u> *USING* netflow!

https://www.prnewswire.com/news-releases/ema-and-lancope-reveal-trends-in-netflow-adoption-and-usage-130557563.html

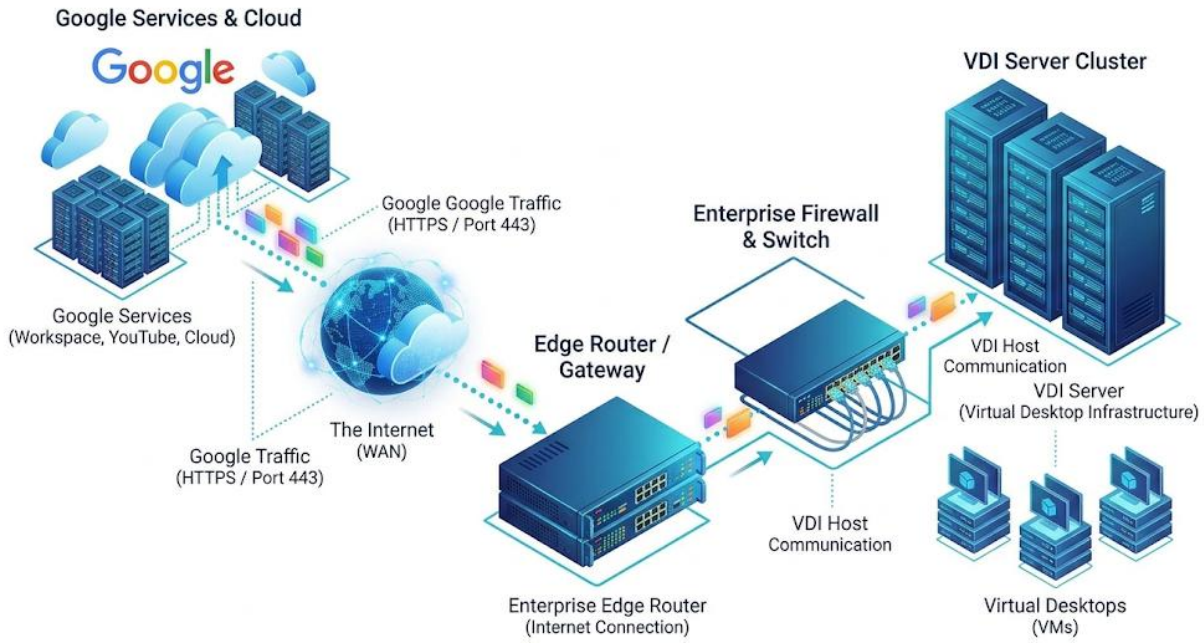
Network Performance



Use-Cases

- **Identifying "Top Talkers":** Instantly pinpoint which specific IPs, users, or applications are consuming the most bandwidth during a network slowdown.
- **Peering and Routing Optimization**: For ISPs and large enterprises, analyzing BGP (Border Gateway Protocol) routing alongside NetFlow data helps determine the most cost-effective and efficient peering arrangements with other networks.
- **SD-WAN Policy Verification**: While SD-WAN controllers make dynamic routing decisions, NetFlow acts as the independent auditor. It verifies that latency-sensitive traffic (like VoIP or video) is actually taking the premium MPLS link, while bulk backups are correctly pushed over cheaper broadband.
- **Cloud Migration Baselining & Validation**: Before moving workloads to the cloud, NetFlow maps all on-premises application dependencies so nothing breaks post-migration. Afterward, it verifies traffic flows to ensure routing isn't looping back on-premises unnecessarily, which can rack up massive cloud egress fees.

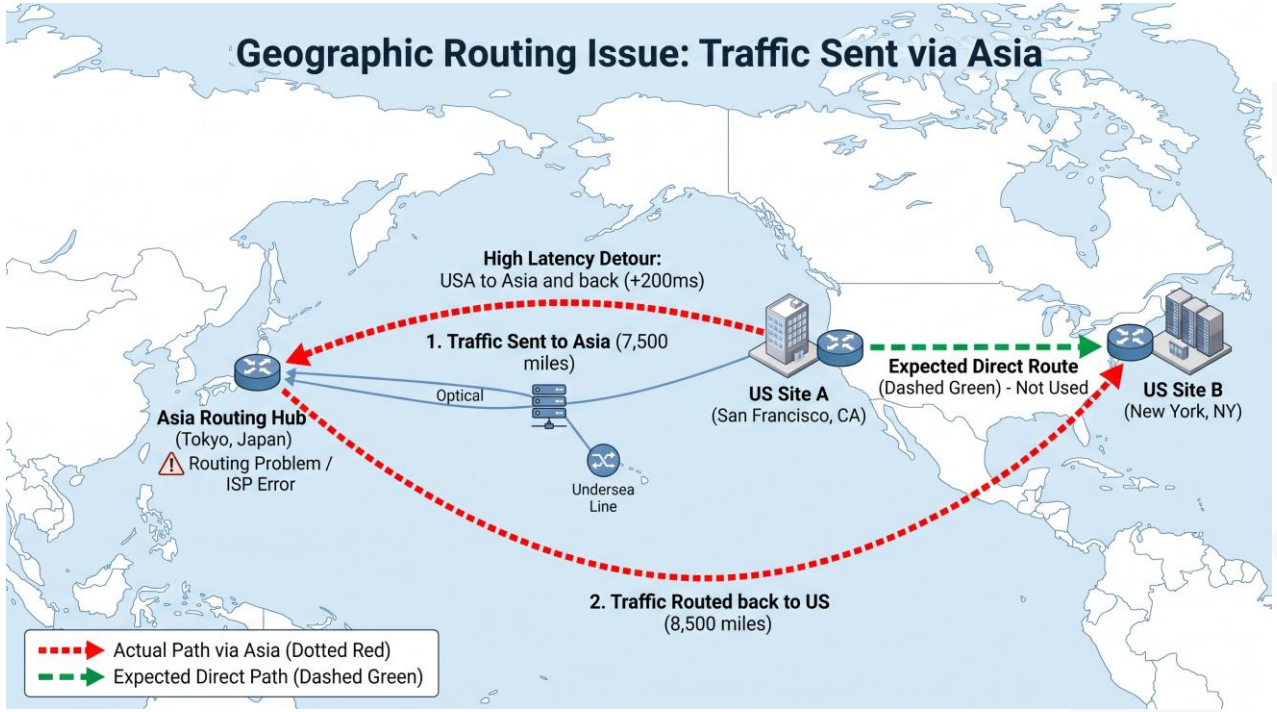
Network Performance



Use-Cases

- **Identifying "Top Talkers":** Instantly pinpoint which specific IPs, users, or applications are consuming the most bandwidth during a network slowdown.
- **Peering and Routing Optimization**: For ISPs and large enterprises, analyzing BGP (Border Gateway Protocol) routing alongside NetFlow data helps determine the most cost-effective and efficient peering arrangements with other networks.
- **SD-WAN Policy Verification**: While SD-WAN controllers make dynamic routing decisions, NetFlow acts as the independent auditor. It verifies that latency-sensitive traffic (like VoIP or video) is actually taking the premium MPLS link, while bulk backups are correctly pushed over cheaper broadband.
- **Cloud Migration Baselining & Validation**: Before moving workloads to the cloud, NetFlow maps all on-premises application dependencies so nothing breaks post-migration. Afterward, it verifies traffic flows to ensure routing isn't looping back on-premises unnecessarily, which can rack up massive cloud egress fees.

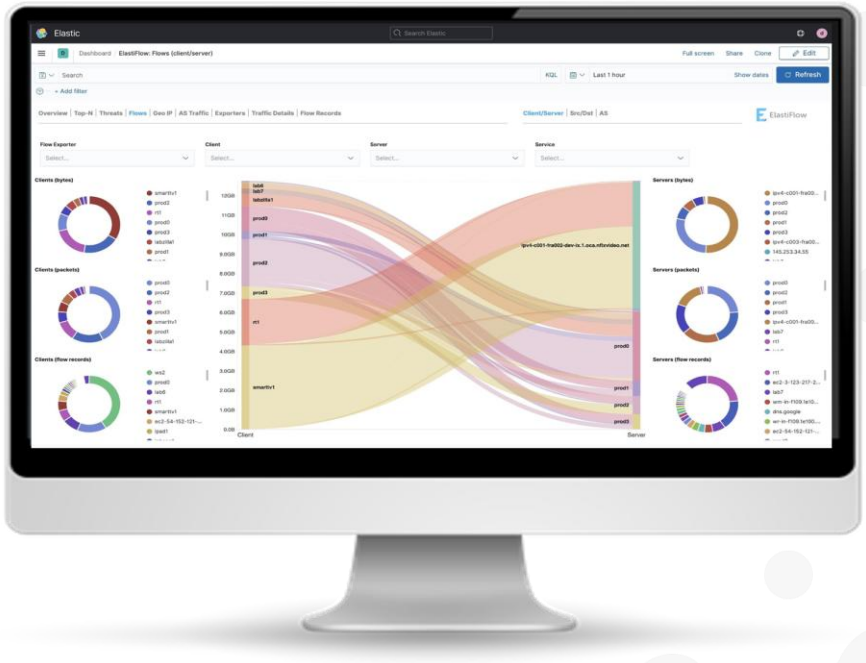
Network Performance



Use-Cases

- **Identifying "Top Talkers":** Instantly pinpoint which specific IPs, users, or applications are consuming the most bandwidth during a network slowdown.
- **Peering and Routing Optimization**: For ISPs and large enterprises, analyzing BGP (Border Gateway Protocol) routing alongside NetFlow data helps determine the most cost-effective and efficient peering arrangements with other networks.
- **SD-WAN Policy Verification**: While SD-WAN controllers make dynamic routing decisions, NetFlow acts as the independent auditor. It verifies that latency-sensitive traffic (like VoIP or video) is actually taking the premium MPLS link, while bulk backups are correctly pushed over cheaper broadband.
- **Cloud Migration Baselining & Validation**: Before moving workloads to the cloud, NetFlow maps all on-premises application dependencies so nothing breaks post-migration. Afterward, it verifies traffic flows to ensure routing isn't looping back on-premises unnecessarily, which can rack up massive cloud egress fees.

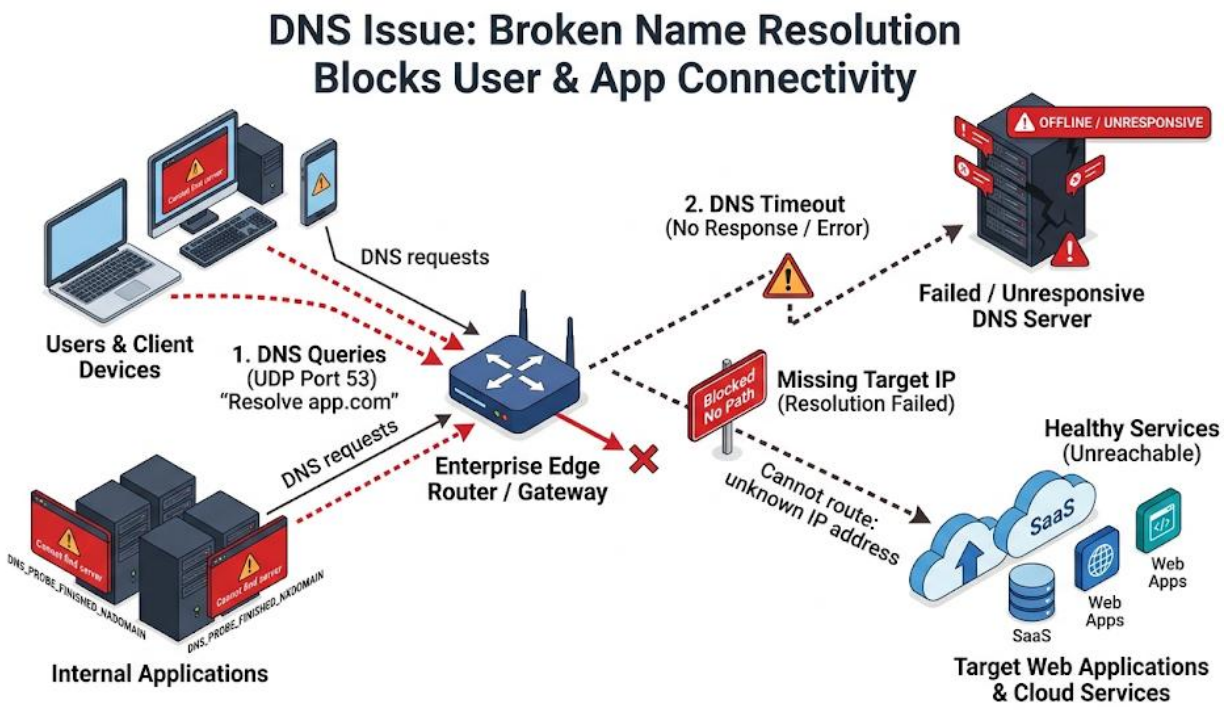
Network Application Troubleshooting



Use-Cases

- **Network Service Availability (DNS, DHCP, LDAP)**: Monitoring flow asymmetry and request/response packet ratios to detect silent outages, server pool exhaustion, or service lockups on foundational infrastructure. Instantly see if an application failure is actually a secondary symptom of a core DNS or LDAP timeout.
- **Application Misconfigurations**: Misconfigured apps (e.g., hitting dead IPs or load-balancer loops) usually enter aggressive retry loops rather than failing quietly. NetFlow exposes this via massive spikes in flow records (connections per second) with minimal byte counts or floods of unanswered TCP SYN packets or RST flags rejecting invalid connections.
- **Poor Application Design**: Apps that fail to reuse HTTP sessions (ignoring keep-alives) force a completely new TCP handshake for every single API call or resource request. NetFlow exposes this inefficiency by showing a massive volume of extremely short, low-byte TCP flows between the client and server, proving to developers that connection setup overhead, not network latency, is causing the sluggish performance.

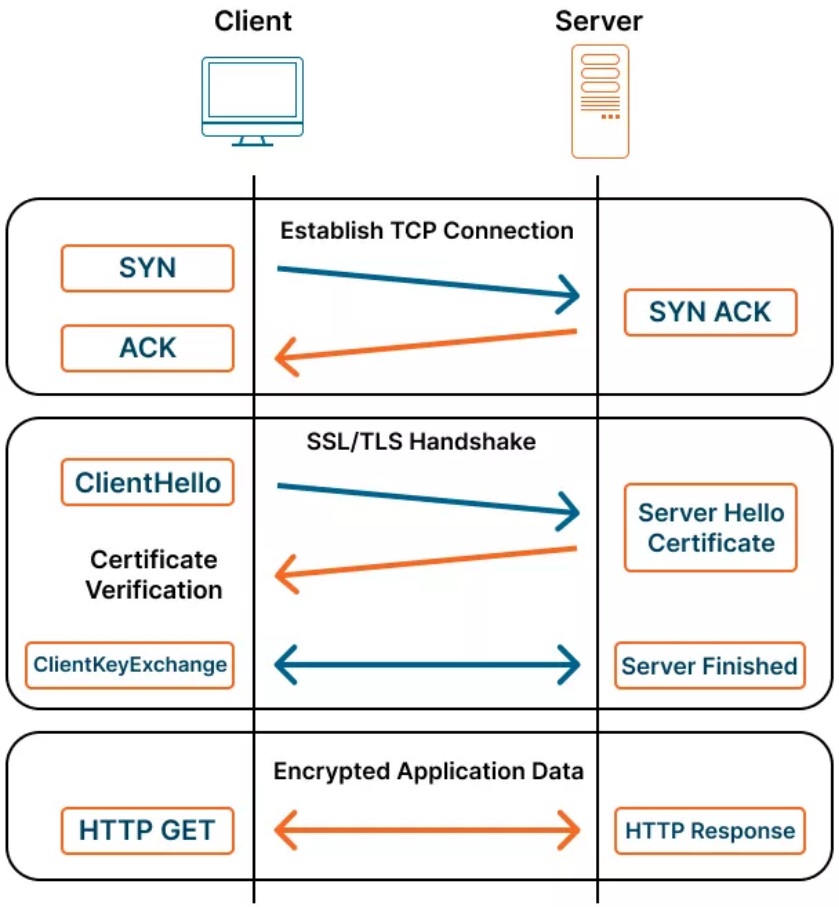
Network Application Troubleshooting



Use-Cases

- **Network Service Availability (DNS, DHCP, LDAP)**: Monitoring flow asymmetry and request/response packet ratios to detect silent outages, server pool exhaustion, or service lockups on foundational infrastructure. Instantly see if an application failure is actually a secondary symptom of a core DNS or LDAP timeout.
- **Application Misconfigurations**: Misconfigured apps (e.g., hitting dead IPs or load-balancer loops) usually enter aggressive retry loops rather than failing quietly. NetFlow exposes this via massive spikes in flow records (connections per second) with minimal byte counts or floods of unanswered TCP SYN packets or RST flags rejecting invalid connections.
- **Poor Application Design**: Apps that fail to reuse HTTP sessions (ignoring keep-alives) force a completely new TCP handshake for every single API call or resource request. NetFlow exposes this inefficiency by showing a massive volume of extremely short, low-byte TCP flows between the client and server, proving to developers that connection setup overhead, not network latency, is causing the sluggish performance.

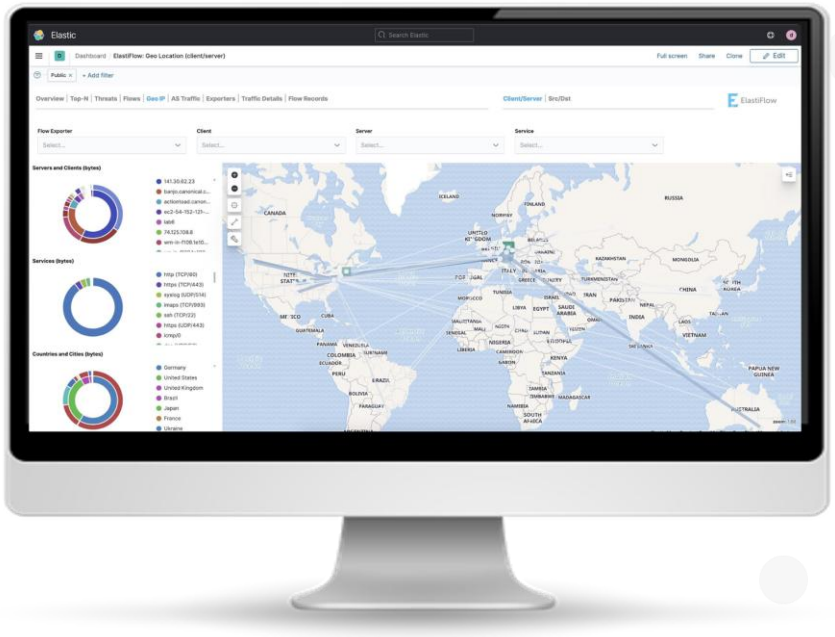
Network Application Troubleshooting



Use-Cases

- **Network Service Availability (DNS, DHCP, LDAP)**: Monitoring flow asymmetry and request/response packet ratios to detect silent outages, server pool exhaustion, or service lockups on foundational infrastructure. Instantly see if an application failure is actually a secondary symptom of a core DNS or LDAP timeout.
- **Application Misconfigurations**: Misconfigured apps (e.g., hitting dead IPs or load-balancer loops) usually enter aggressive retry loops rather than failing quietly. NetFlow exposes this via massive spikes in flow records (connections per second) with minimal byte counts or floods of unanswered TCP SYN packets or RST flags rejecting invalid connections.
- **Poor Application Design**: Apps that fail to reuse HTTP sessions (ignoring keep-alives) force a completely new TCP handshake for every single API call or resource request. NetFlow exposes this inefficiency by showing a massive volume of extremely short, low-byte TCP flows between the client and server, proving to developers that connection setup overhead, not network latency, is causing the sluggish performance.

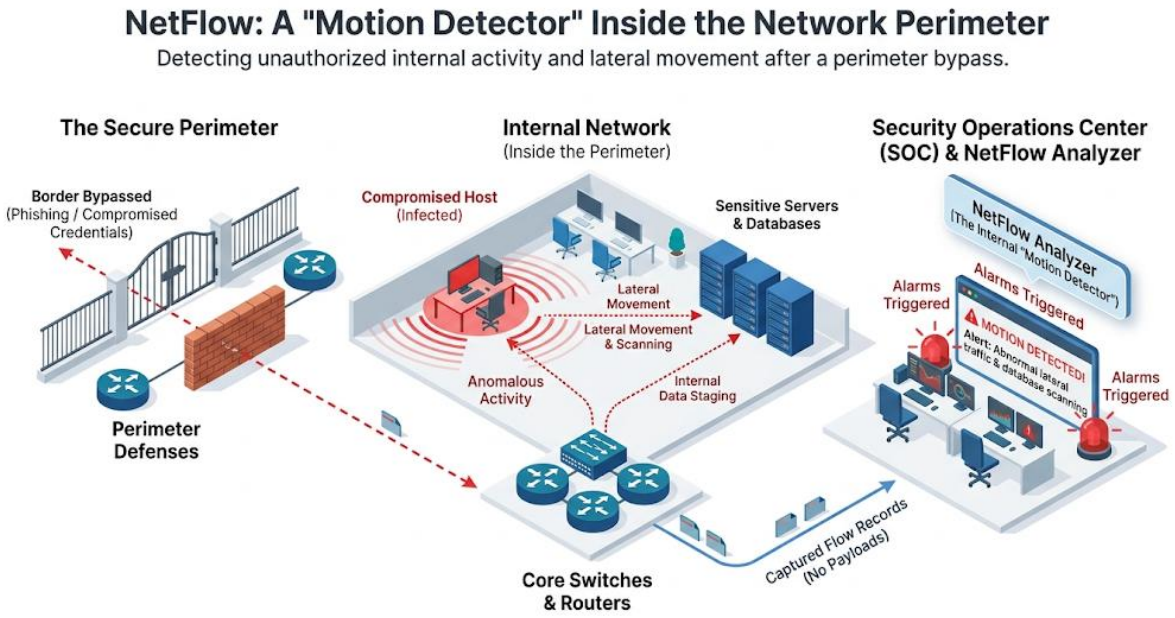
Network Security



Use-Cases

- **DDoS Detection and Mitigation**: By analyzing sudden, massive spikes in inbound traffic from unexpected sources or targeted at specific ports, security tools can detect Distributed Denial of Service (DDoS) attacks and trigger automated scrubbing or blackholing.
- **Data Exfiltration Tracking**: Large outbound data transfers to unknown or suspicious external IP addresses often indicate data theft, even if the payload itself is encrypted.
- **Shadow IT Discovery**: Detect unauthorized applications, cloud services, or VPNs being used by employees by monitoring the ports and destination IPs of outbound traffic.
- **Compliance Auditing**: Flow logs provide historical proof that network segmentation rules are functioning correctly and that no unauthorized connections are bridging secure and non-secure environments.

Network Security

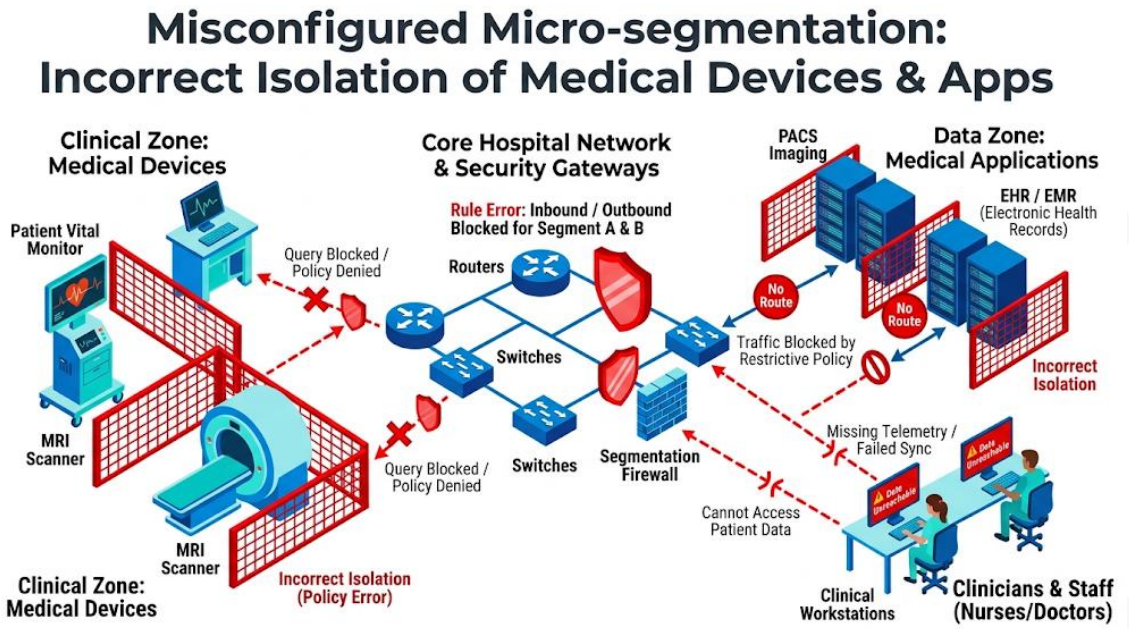


"FYI, this item made it to the security-group meeting today with the government and because of all the items that have been signaled and identified so far using ElastiFlow, we have received the request to expand the capture-net as wide as we can."

Use-Cases

- **DDoS Detection and Mitigation**: By analyzing sudden, massive spikes in inbound traffic from unexpected sources or targeted at specific ports, security tools can detect Distributed Denial of Service (DDoS) attacks and trigger automated scrubbing or blackholing.
- **Data Exfiltration Tracking**: Large outbound data transfers to unknown or suspicious external IP addresses often indicate data theft, even if the payload itself is encrypted.
- **Shadow IT Discovery**: Detect unauthorized applications, cloud services, or VPNs being used by employees by monitoring the ports and destination IPs of outbound traffic.
- **Compliance Auditing**: Flow logs provide historical proof that network segmentation rules are functioning correctly and that no unauthorized connections are bridging secure and non-secure environments.

Network Security



Use-Cases

- **DDoS Detection and Mitigation**: By analyzing sudden, massive spikes in inbound traffic from unexpected sources or targeted at specific ports, security tools can detect Distributed Denial of Service (DDoS) attacks and trigger automated scrubbing or blackholing.
- **Data Exfiltration Tracking**: Large outbound data transfers to unknown or suspicious external IP addresses often indicate data theft, even if the payload itself is encrypted.
- **Shadow IT Discovery**: Detect unauthorized applications, cloud services, or VPNs being used by employees by monitoring the ports and destination IPs of outbound traffic.
- **Compliance Auditing**: Flow logs provide historical proof that network segmentation rules are functioning correctly and that no unauthorized connections are bridging secure and non-secure environments.

NetEye and ElastiFlow

Providing real visibility into network activity.



NetEye

