

EndaceFlow

High-Performance NetFlow Generator for EndaceProbe™

EndaceFlow™ is a high-performance NetFlow Generator that significantly improves visibility for security and performance monitoring across the enterprise network. Capable of generating unsampled NetFlow from 40Gb/s of real-world traffic, EndaceFlow provides uncompromised visibility of every flow in your network.

Combining EndaceFlow with the EndaceProbe's always-on, continuous packet capture provides single-click access to complete network evidence that can reduce incident investigations from hours to minutes.

NetFlow and continuous network packet capture are highly complementary technologies that together provide both a high-level view of network activity and the precise detail of every activity. NetFlow provides the high-level view of traffic patterns, user behaviors, or potentially threatening activity and network packet capture provides the missing detailed data and payloads needed to confidently understand and resolve complex security threats, breaches or performance issues. Using packet data and NetFlow together provides complete visibility that enables faster, more accurate, incident investigation and resolution.






Powerful Performance, Total Visibility

Generating NetFlow data from switches, routers or firewalls can significantly compromise the core functions of those appliances (routing, management, threat detection etc.) due to the CPU resources consumed by NetFlow generation. As a result, these appliances are often configured to sample network traffic at rates of 1:100 or worse to reduce the burden of NetFlow generation. Sampling reduces CPU load but at the expense of visibility, putting you at risk of not detecting cybersecurity threats, breaches, interop issues, or performance problems.

Only 1:1 unsampled NetFlow provides a completely accurate summary of all network activity. Today's data centers, with advanced web-services, require uninterrupted, round the clock availability and robust cybersecurity. Sampled NetFlow doesn't provide the granular level of visibility necessary to achieve these goals. Moreover, the majority of data center flows are short-lived and sampled NetFlow fails to provide a complete picture for network trend analysis. Anything less than 100% visibility of all network activity is a compromise that teams can no longer afford to make.

EndaceFlow generates 1:1 unsampled NetFlow for unmatched full-stream flow visibility over any combination of IPv4 and IPv6 based networks. Deploying EndaceFlow on an EndaceProbe gives you complete visibility into all traffic, even on the fastest networks, without the performance impact that switches and routers suffer when generating NetFlow. Feeds generated by EndaceFlow can be secured with TLS or mutual TLS encryption, including certificate-based endpoint authentication.

SPECIFICATIONS

	Peak Traffic Rate	40 Gb/s per EndaceProbe 20 Gb/s per x2 Dock instance 2 Gb/s per x1 Dock Instance
	Maximum Flow Creation Rate	250 k Unidir flows/s per instance
	Maximum Concurrent Flows	12 M Unidir flows per instance
	Compatibility	NetFlow v5, v9 and IPFIX
	IP Version	Monitor IPv4 and IPv6 traffic
	Sampling	1:1 Unsampled or Flow Sampled
	Patented Flowsafe Load Balancing	Distribute load across up to 4 collectors per EndaceFlow instance
	Security	Optional TLS Encrypted NetFlow
	App Dock Sizes	x1, x2 or x4 Dock Sizes
	VM Install Size	20 GB

Note: All performance specifications are with 1:1 Unsampled NetFlow generation on G4 or G5 EndaceProbe.

KEY FEATURES

100% accurate 1:1 unsampled NetFlow Generation

Integrated with EndaceProbe Network Packet Capture

Custom templates with 140 record types

High performance, designed for demanding network traffic conditions

Easy deployment on any EndaceProbe, managed by EndaceCMS™

Advanced filters and patented, flowsafe load balancing to manage output and distribute across multiple collectors

Compatible with a wide variety of NetFlow collectors

Unparalleled visibility into both Flows and Packets

Together, the EndaceProbe's full packet capture and network-wide search capability, and EndaceFlow's 1:1 unsampled NetFlow generation, provide unmatched packet-and-flow visibility. This complete and accurate picture of network activity enables teams to quickly and definitively resolve even the most complex network security and performance issues.

Create Custom Templates

EndaceFlow lets you customize the information you send to your NetFlow collector from a selection of 140 different fields. Send only the information your team cares about and avoid burdening your collector with superfluous information that consumes collector storage and CPU resources.

Take advantage of built-in AS support in EndaceFlow to map IP addresses to their related Autonomous System Numbers. An AS to IP mapping table can be uploaded to EndaceFlow to ensure the most up-to-date AS number allocations are reflected in EndaceFlow output.

Export flows to multiple NetFlow collectors

For deployments requiring multiple NetFlow collectors, EndaceFlow can filter and load balance NetFlow feeds across multiple collectors. This is useful in cases where specific network flows (e.g. specific web services) must be sent and analyzed on a particular collector or where multiple collectors are used to handle the flow data on very large networks. EndaceFlow supports up to 130 filters across four collectors with patented, flow-safe, IP load-balancing that is easy to configure.

Unified Management

EndaceFlow uses Endace OSm™ software, a purpose-built operating system based on a hardened Linux distribution. Configuration and management via GUI and CLI is identical to managing any other Endace appliance. For large deployments, you can also manage EndaceFlow instances using EndaceCMS (Endace Central Management) as part of your EndaceProbe estate.

BENEFITS

Fast and effective incident response when you have full visibility of every Flow, Packet and Payload on your network.

Resolve performance, security and IT issues conclusively.

Accurately understand network traffic patterns and bottlenecks.

Free up precious CPU resources on switches, routers, and firewalls.

Easily scale up visibility as your network grows.

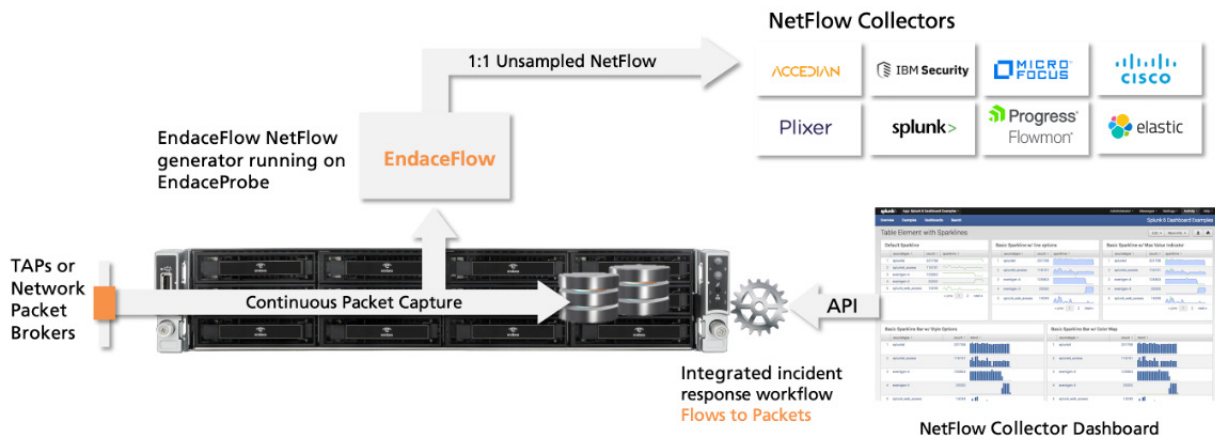
Reduce cost by leveraging EndaceProbe for deployment and EndaceCMS for management.

Technology Integrations

EndaceFlow can be easily configured to feed any of the leading NetFlow collectors, including Endace Fusion partners such as Plixer®, Cisco Stealthwatch®, Progress Flowmon® and others. Workflow integrations enable one-click access to packets recorded by EndaceProbe from any flow event in your NetFlow collector dashboard.

Conclusion

In today's environment of rapidly evolving threats, increasing threat volumes and ever more demanding network speeds and loads, accurate and reliable visibility into network activity is crucial. The combination of EndaceProbe and EndaceFlow provides an unmatched network evidence source that you can rely on. It provides both an accurate high-level, summary view of all network activity, and the detailed packet level evidence SecOps and NetOps teams need to get to the root cause of security and performance issues to remediate them quickly and accurately.



For more information on the Endace portfolio of products, visit: endace.com/products For further information, email: sales@endace.com