Technical Brief

STAMUS NETWORKS

Optimizing Clear NDR™ Storage with Conditional Logging

Maximize Data Retention Without Sacrificing Security

Executive Summary

Clear NDR's conditional logging feature solves a critical challenge for organizations deploying network detection and response solutions by dramatically reducing storage requirements while maintaining security effectiveness. Unlike the "verbose" mode that captures extensive metadata from every network transaction, conditional logging selectively stores only data associated with critical detection events like alerts and policy violations. Test deployments demonstrate up to 97% reduction in storage needs, extending data retention periods by up to 46 times with the same storage capacity—all without compromising threat detection capabilities or incurring additional costs. This enables organizations monitoring high-speed networks to balance comprehensive security visibility with practical storage constraints

Introduction

In addition to security events, Clear NDR extracts and stores a wealth of network data logs in their 'verbose' mode (full logging). These logs include detailed metadata associated with every network protocol transaction, flow records, file exchanges, and more. The complete data set can be found in the data schema section of the user documentation for Clear NDR here >>.

For many organizations, this extensive metadata is crucial to their security practice. For others – particularly those who have deployed Clear NDR to monitor very high-speed networks – the storage requirements associated with this verbose logging make it impractical to retain historical logs for long enough to satisfy their data retention needs.

What is Conditional Logging

Clear NDR offers a "conditional logging" option which can dramatically reduce the storage burden while still retaining critical evidence needed for event triage and incident response.

With conditional logging enabled, Clear NDR stores the protocol transactions, flow records, protocol error/anomaly detection events, and file transactions only when they are associated with critical detection events, such as alerts, Sightings™, DoCs, and DoPVs. This allows users to retain evidence associated with detection events for extended periods without investing in additional storage costs to retain every protocol transaction or flow record. Without conditional logging, every transaction, protocol error/anomaly event, and flow record is stored.

Importantly, conditional logging does not impact Clear NDR's ability to detect threats or impact the wealth of data captured associated with threat and policy violation detection events.

Note: Conditional logging should not be confused with the "conditional packet capture" feature in which Clear NDR captures all of the raw packets associated with any detection event, logging them as PCAP files. Unlike conditional logging described above, there is no "verbose" or "full logging" mode for packet capture.

Reducing Storage and Extending Data Retention

Conditional logging can dramatically reduce the storage requirements, and – by association – dramatically extend the time for which log data is retained in Clear NDR.

The table below illustrates the impact of conditional logging on a real-world example deployment.

	10 Day Results					
	Traffic Rate	Hosts Observed	Events (all) per second	Detection Events	Log Volume	PCAP Volume
Verbose (full logging)	5 Gbps	130,000	101,100	21,000,000	4.5 TB	250 GB
With Conditional Logging	5 Gbps	130,000	600	5,300,000	115 GB	250 GB
		Savings	99 %	75 %	97 %	0 %

And the table below summarizes the savings under several scenarios extrapolated from the above.

Network Data Rate	Example Total Storage (gigabytes) Required for 10 Days			Data Retention (days) with 2 TB of Log Storage		
	Verbose (full logging)	With Conditional Logging	% Savings	Verbose (full logging)	With Conditional Logging	% Extension
1 Gbps	900	40	95.56%	2.22	50.00	2150%
5 Gbps	4500	115	97.44%	0.44	17.39	3813%
10 Gbps	9000	250	97.22%	0.22	8.00	3500%
25 Gbps	23500	600	97.45%	0.09	3.33	3817%
40 Gbps	37000	1000	97.30%	0.05	2.00	3600%
100 Gbps	95000	2000	97.89%	0.02	1.00	4650%

Licensing

Conditional logging is included in the standard license for Clear NDR – at no additional cost.

Summary

Conditional logging can dramatically reduce the storage requirements and dramatically extend the time for which log data is retained in Clear NDR.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

