



Packets Don't Lie: LogRhythm NetMon Freemium Review



A SANS Product Review

Written by Dave Shackleford

January 2017

*Sponsored by
LogRhythm*

Introduction

Network monitoring has always been a priority for both operations and information security teams, but never have we been so focused on detection of unusual or malicious network behavior as we are today—and for good reason. Many more attackers are learning to blend in and disguise their malware command and control traffic with well-known applications and protocols like HTTPS, DNS and others.

At the same time, there are numerous examples of data leaking out of our environments right under our noses. Whether accidental or purposeful, data loss is at an all-time high, and organizations need tools that can help them identify sensitive data leaving the network and respond when loss occurs.

What's needed is deeper, more intelligent monitoring across the network to recognize malicious packets and traffic hiding within the real traffic, data exfiltration, protocol and port misuse, and other activities that many security tools today don't pick up.

To that end, we reviewed LogRhythm's Network Monitor Freemium (NetMon Freemium) Version 3.2.3 with several key areas of focus in mind:

- Usability
- Accurate traffic identification and profiling
- Detection of patterns and drilldown into sources
- Sensitive data identification and data loss prevention
- Network forensics
- Full packet capture and file reconstruction

After we took a look at the core capabilities, we walked through several use cases that illustrated a more real-world set of scenarios that any security analyst or operations team might encounter. Throughout the review, NetMon Freemium displayed powerful monitoring capabilities for enterprises of any size.

Its advanced monitoring features include traffic profiling, application identification and bandwidth usage (all the way down to the offending IP addresses), as well as lateral and ingress/egress traffic monitoring, full packet capture, port and protocol mismatch monitoring, and more. The interface of NetMon Freemium is incredibly intuitive, and we had no problem selecting traffic types, filtering out certain ports or services as needed to see specific patterns and follow up on details in the Alarms Table.



Getting Started: The Test Environment

To start the review, the SANS team downloaded a free ISO image from <https://logrhythm.com/freemium> (also available as a VirtualBox virtual machine). After installation in our test environment, we generated some sample traffic and used some previously captured packets to replay onto the test network.

The product was incredibly easy to configure, requiring slightly more than 20 minutes to configure network interfaces and ensure traffic was visible in real time. In an actual enterprise environment, a more traditional SPAN or tap architecture would likely be used to ensure the product could see the appropriate network traffic.

Exploring the NetMon Freemium User Interface

In our review of the NetMon Freemium interface, we found the web UI convenient to use, with dashboards that are easy to configure and a readily available search interface. The main dashboard is shown in Figure 1.

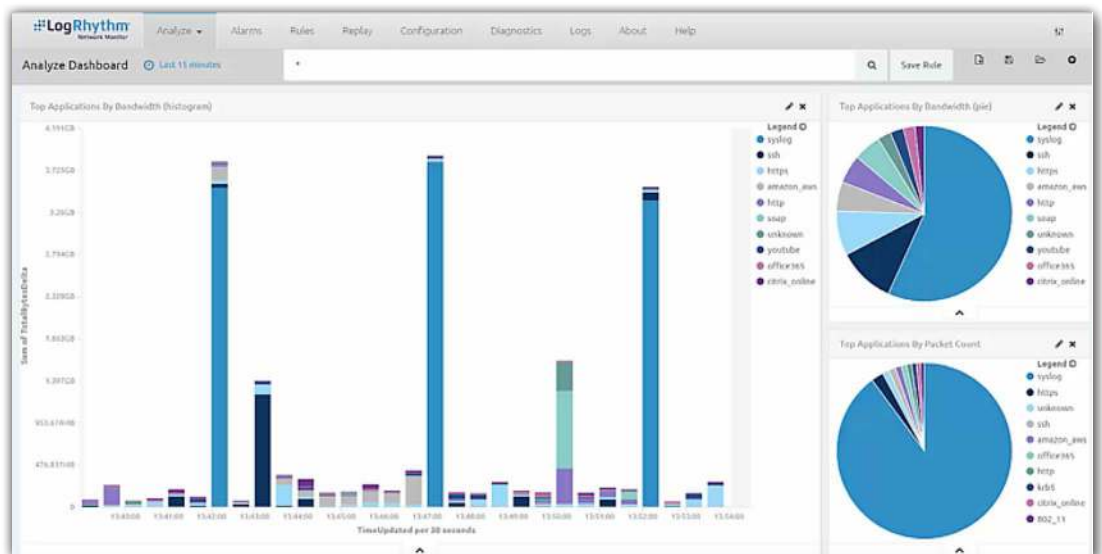


Figure 1. The NetMon Freemium Dashboard



Getting Started: The Test Environment (CONTINUED)

In the default Analyze view, we have the top applications by bandwidth and packet count as seen in the environment throughout time, updated as frequently as every 30 seconds. This view alone provides an enormous amount of detail about what is happening in the environment, and shows the past 15 minutes of traffic by default (although this can be easily customized):

- In the bottom half of the pane, you can see flows that correlate to the network traffic seen in the environment, with source, destination and more.
- You can easily drill into the traffic to see packet details and events.

In our main dashboard, we saw a lot of syslog traffic. When we highlighted and clicked on it, we were taken to a specific view of the syslog traffic, which can show both overall syslog traffic seen (if you click on the pie chart with syslog traffic) and syslog traffic within a specific time window (if you click on that time window's syslog traffic in the bar chart), as illustrated in Figure 2. Note that syslog was prevalent in our test traffic but has no significance other than our particular test environment.

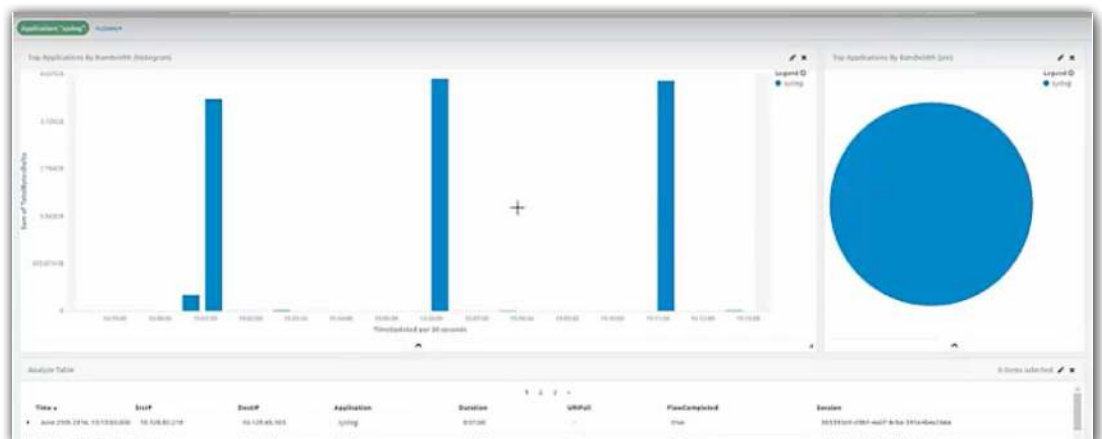


Figure 2. A Drilldown into Syslog Traffic



Getting Started: The Test Environment (CONTINUED)

We also experimented with a number of simple queries in the search window at the top. The Lucene query syntax was incredibly flexible, allowing us to query on everything (using a wildcard * operator) down to very granular searches on text strings, data quantities seen in particular time windows, and IP addresses that might be of interest. As shown in Figure 3, we entered a query for `DestIP: [10.0.0.0 to 10.3.255.255]` to see all traffic destined for that range.

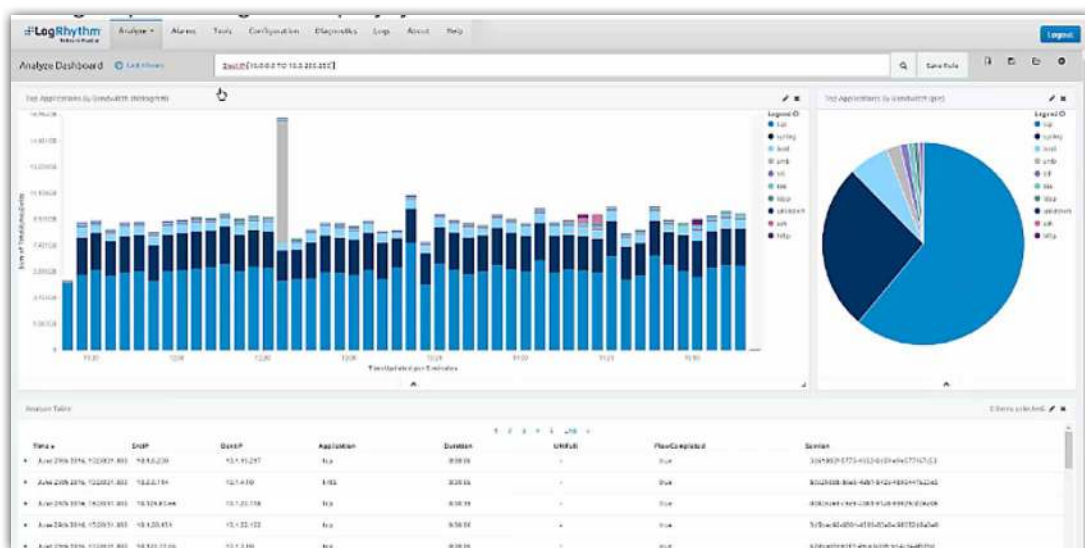


Figure 3. Searching for IP Activity

Traffic Identification and Profiling

NetMon Freemium has a number of additional dashboards available, many of which allow for much more targeted traffic identification and profiling. We explored a number of the other dashboards available within the product, including:

- The Capture dashboard, which shows us full packet capture content and allows for download and reconstruction of entire sessions
- The File Reconstruction dashboard, which can pull files out of captured SMTP traffic
- The Destination Port dashboard, which maps just the target application/service ports seen in the environment, possibly indicating attack patterns or trends



Getting Started: The Test Environment (CONTINUED)

An example of the Destination Port dashboard is shown in Figure 4.

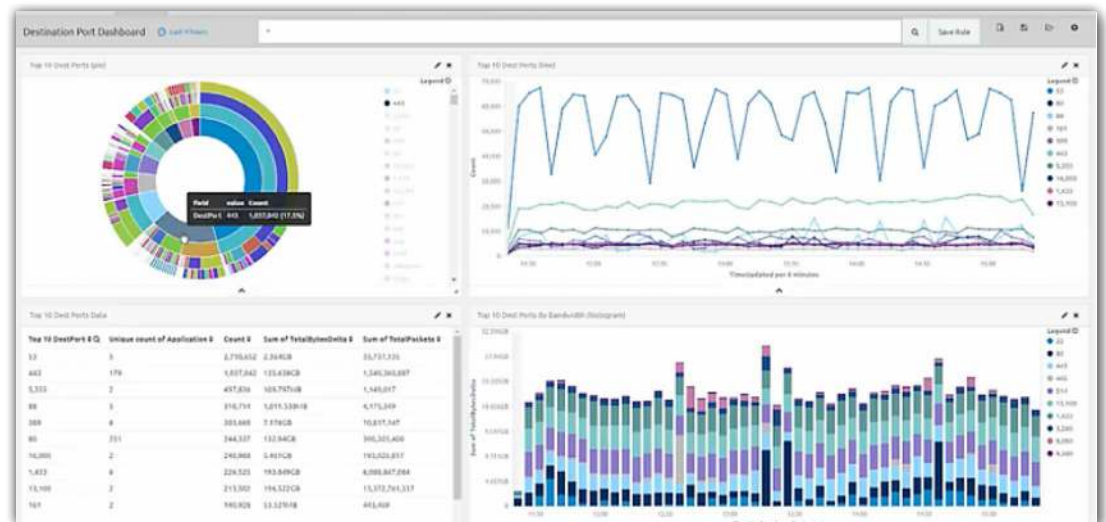


Figure 4. Destination Port Dashboard

In our review, we drilled into numerous traffic types through these additional dashboards. We could see obvious patterns of traffic throughout time, differentiating between HTTP and HTTPS sessions and sites. This is critical for any security team, to help build network traffic pattern baselines, detect common protocols and applications, and quickly spot anomalies, which may indicate malicious activity.

Full Packet Capture and File Reconstruction

While exploring the product, one of the features we looked into was full packet capture. The advantage of full packet capture with NetMon Freemium is the ability to capture all packets or use its SmartCapture feature to selectively capture and save traffic based on application, packet content, IP address, etc.

All packet captures are stored in industry-standard PCAP formats that can be downloaded and imported into local analysis tools such as TCPDump or Wireshark. The Freemium product can store as much as 1GB of packet capture data.

In our review, we perused the Capture and File Reconstruction dashboards to download traffic capture files and extract file content from packet streams. In the packet capture dashboard, we were able to easily download any captured file streams by clicking the download button next to a capture stream in the lower half of the dashboard. We were then able to open the PCAP file we downloaded with a local install of Wireshark for analysis.



Getting Started: The Test Environment (CONTINUED)

The File Reconstruction dashboard includes the top attachment types seen in email (SMTP) traffic, as well as the top senders and receivers, attachment names, and more. We were able to monitor which files were being sent and save them locally for forensic analysis or evidence retention. The File Reconstruction dashboard is shown in Figure 5.



Figure 5. NetMon Freemium File Reconstruction Dashboard

Upon initial examination, we found NetMon Freemium to be extremely simple to navigate, with many built-in dashboards and tools for detecting and alerting on traffic patterns within the environment.

In the next sections, we take NetMon Freemium through hypothetical use cases to gauge its effectiveness in catching unapproved traffic, malicious traffic and data leakage.



Use Cases: Bandwidth, Malware, Data Leakage

When it comes to network monitoring, there are essentially three families of traffic to worry about: unnecessary bandwidth-hogging traffic, malicious traffic, and sensitive data flow (particularly for heavily regulated industries). We reviewed NetMon Freemium against all three use cases.

Case 1: Nuisance Apps and Bandwidth Hogs

In the first scenario, we focused on a use case familiar to everyone in network operations: discovering application traffic that is unnecessary and potentially hogging bandwidth. This use case is focused on availability because, in the age of streaming and social media, bandwidth monitoring is actually more important than ever.

Keyword Search for Hogs

We started by looking for all bandwidth use in the dashboard by clicking the *Top Applications by Bandwidth* chart and then searching for a wildcard * in the interface. This showed us all the traffic on a bar histogram chart, which we easily drilled into and explored what was going on.

In this case, we wanted to look for specific bandwidth-hogging application traffic in our environment, so we searched for `Application:pandora` in the search interface, as shown in Figure 6.



Figure 6. Searching for Pandora Bandwidth Use



Use Cases: Bandwidth, Malware, Data Leakage (CONTINUED)

Pie charts showed top applications by bandwidth as well. In the test environment we set up, syslog traffic was the top bandwidth consumer, as shown in Figure 7.



Figure 7. Syslog as the Top Bandwidth Application

NetMon Freemium lets you see which applications take up the most bandwidth at a glance. You can also perform searches to seek out specific applications or exclude certain applications.

Finding Rogue Apps

While investigating the various types of traffic in the environment, we noted one of the top bandwidth consumers was YouTube. This is an undesirable application (not only does it consume bandwidth, but employees could be uploading content and violating policy), so we switched to a different dashboard that focuses explicitly on ingress and egress traffic direction (that included stats on bandwidth and specific applications).

The Ingress-Egress Traffic Dashboard allowed us to purposefully exclude all lateral traffic (traffic between internal systems) so we could look at only the inbound and outbound (north-south) traffic in the test environment, which showed only traffic coming into and leaving our enterprise network (or what our users and systems were communicating with on the Internet and elsewhere).



Tying Activity to Users

By entering the query `Application:youtube`, we were then able to see how much data was coming in as well as what IP addresses were accessing YouTube and when, as seen in Figure 8.



Figure 8. YouTube Traffic in Our Environment

Although tracking YouTube traffic makes sense for detecting people wasting time (and bandwidth) at work, we might be more concerned about people uploading content over the YouTube application. To detect this, we created an alarm to specifically alert us to this event. In our search window, we entered a pattern match of `application:youtube AND TrafficDirection_NM:"egress"`, which we then converted to a rule by clicking Save Rule to the right of the search window. When we saved the rule, NetMon also informed us that the rule would have triggered 944 times in the past 24 hours and asked if we'd still like to confirm the rule. This is a fairly high number, indicating the need to delve into firewall rules and other traffic-blocking controls if we were concerned about too much YouTube traffic.

When the new alarm rule was created to catch data leaving the network over YouTube, we saw it would have triggered 944 times in the past 24 hours.



Deep Packet Analysis

If you are more concerned about data leaving the organization via peer-to-peer apps or file transfers from chat applications, you can easily set an alarm on either of these by turning on one of NetMon Freemium's out-of-the-box Deep Packet Analytics (DPA) rules. These rules allowed us to identify traffic in a more granular way. Figure 9 shows some of the DPA rules available on NetMon Freemium. These rules are also customizable.

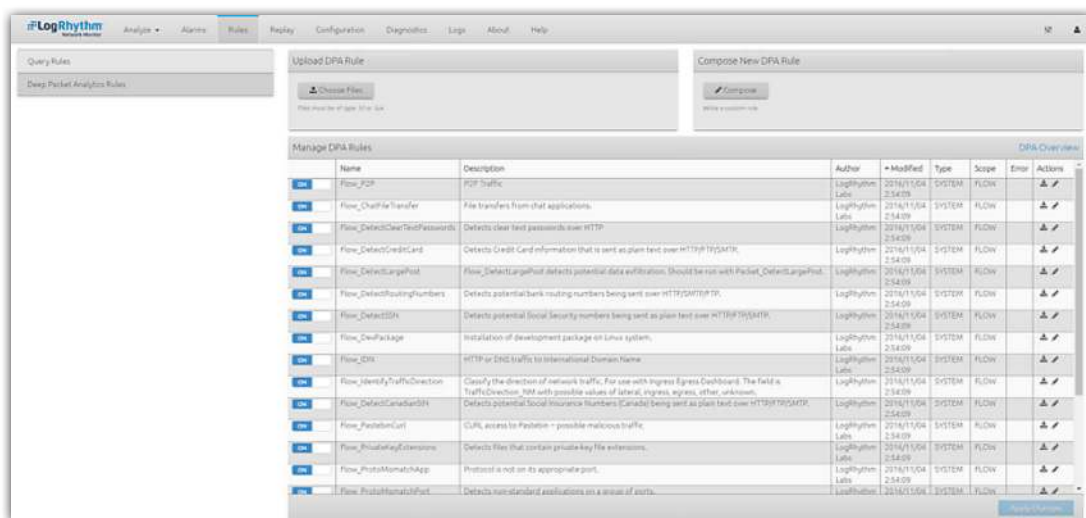


Figure 9. Out-of-the-Box DPA Rules Available with NetMon Freemium

PCAP Replay

One of the coolest features we tested was the built-in rule-testing function: the Replay PCAPs tab within the interface. Here, we were able to upload PCAP files directly to the platform and run them through rules to ensure they triggered properly. This allows security teams to test rules under development immediately against known malicious or interesting traffic they would like to identify. Figure 10 shows a couple PCAPs uploaded and about to be replayed, which then immediately showed up in the main Alarms dashboard with alerts from the built-in Peer 2 Peer and Chat File Transfer rules that have fired.

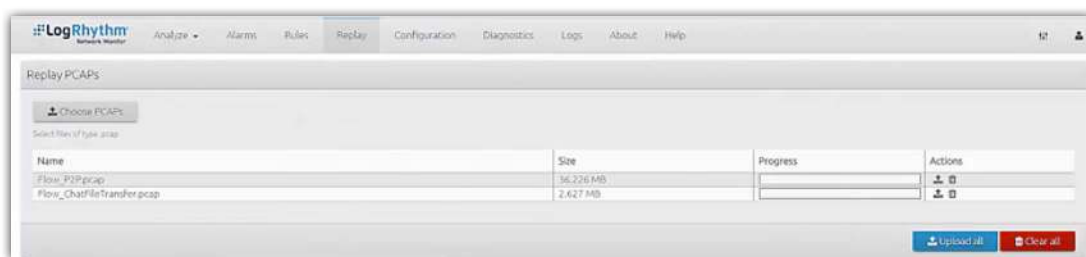


Figure 10. Suspicious PCAP Traffic Replay and Alarms

The PCAP Capture and Replay capabilities were particularly useful, and any security operations team would likely find these tools invaluable when building more advanced rules for detection.



Case 2: Network Malware Indicators

Our second case involved looking for port and protocol misuse as indicators of malware traffic and command and control (C2) activity.

We started this scenario with NetMon's Destination Port dashboard. This case, in particular, gave us the opportunity to explore the details of this dashboard, which showed us not only the top destination ports, but also the specific services noted on those ports in granular detail. In our review environment, we saw that a majority of traffic by session count appeared to be DNS, quite a bit of HTTP and HTTPS, and a fair amount of Kerberos traffic (see Figure 11).

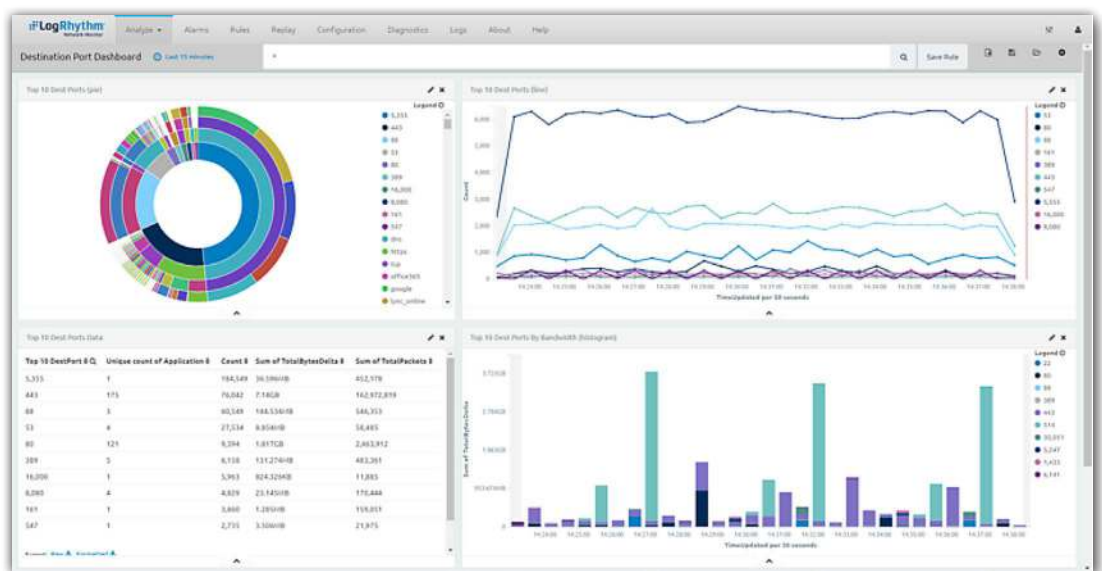


Figure 11. Investigating Traffic and Services on Specific Ports

However, when we drilled into the dashboard's "Top 10 Destination Ports" pie chart, we noted some of the port 53 traffic was not DNS, by looking at the number of applications or services using port 53 in the lower left-hand pane of the window. We also saw multiple services/applications associated with Kerberos on port 88 (also noted in the data section in the lower left of the dashboard in Figure 11). Because Kerberos is an authentication protocol, this could indicate some sort of tunneled communication by an attacker or simply a misconfigured application.



Powerful Filtering

To narrow down what we were seeing, we used some of the interface's powerful filtering capabilities, selecting the destination port of 53 and then stripping out DNS so we could focus on the other applications using the port. In Figure 12, we highlighted one of the remaining services only to find it's actually Kerberos! We would have to investigate more to find out what that means, but changing Kerberos to use a different port might indicate that an attacker or insider is setting up a shadow infrastructure. It could also indicate that credentials or data are being leaked.

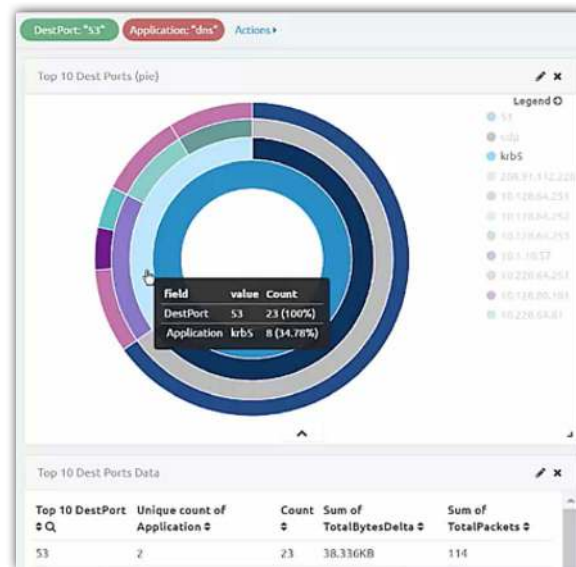


Figure 12. Kerberos Traffic Using Port 53

Repeating this same process for the traffic on port 88 (excluding Kerberos traffic specifically), we noted it was some unspecified TCP traffic primarily heading to a single IP internal address, as highlighted in Figure 13.

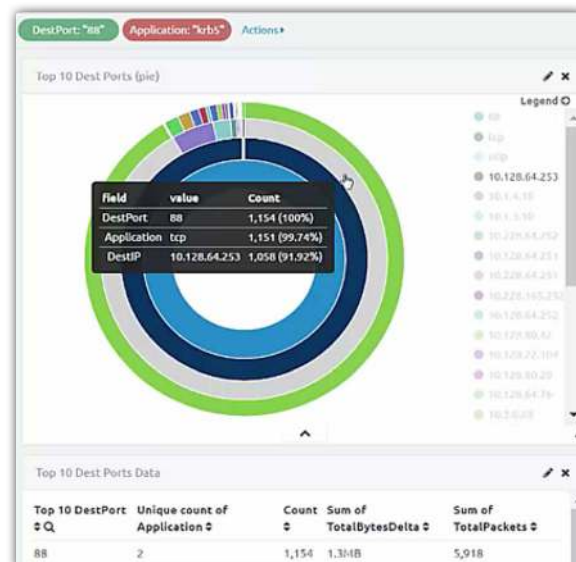


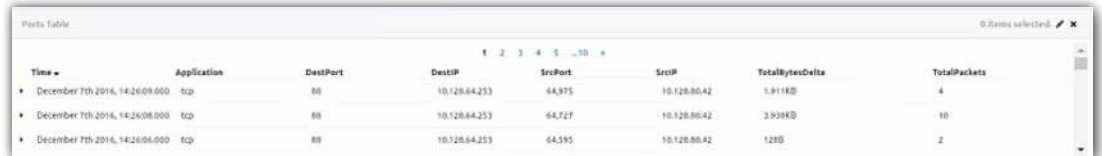
Figure 13. Unusual Port 88 TCP Traffic



Use Cases: Bandwidth, Malware, Data Leakage (CONTINUED)

With this address, we could now investigate the destination system communicating to determine what was happening.

Finally, we dug into the specifics of the traffic itself, looking in the ports table to see source IP, destination IP, the number of packets and bytes sent, and more (see Figure 14).



Time	Application	DestPort	DestIP	SrcPort	SrcIP	TotalBytesDelta	TotalPackets
December 7th 2016, 14:26:09.000	tcp	88	10.128.64.253	64,975	10.128.88.42	1,911KB	4
December 7th 2016, 14:26:08.000	tcp	88	10.128.64.253	64,727	10.128.88.42	3,939KB	10
December 7th 2016, 14:26:06.000	tcp	88	10.128.64.253	64,595	10.128.88.42	128B	2

Figure 14. Port 88 Traffic Details

From this point, we narrowed down our investigation to particular systems and destinations to determine what was happening.

Traffic Spikes

For our second investigation into unusual traffic patterns, we looked at a 24-hour window of HTTPS traffic (TCP port 443) and noted an unusual spike of traffic at midnight, as seen in Figure 15.

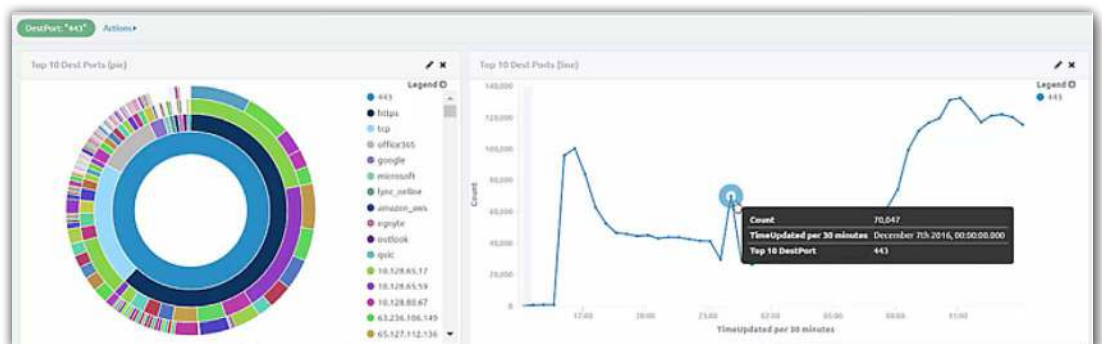


Figure 15. An Unusual HTTPS Spike at Midnight

Upon investigation, this traffic turned out to be a development server simply checking for updates to packages on a schedule, but our ability to pinpoint the anomaly in seconds was critical in making that determination.



Mismatched Protocols

Just as we discovered Kerberos running over the DNS protocol, we continued the review to find more such mismatches. We looked into several additional DPA rules that flag service and protocol mismatches with ports in use, and then used the Replay tool to check these rules and found a significant number of mismatches in the environment. Figure 16 shows the alarms related to one of these DPA rules, `ProtoMismatchPort`, which alerts on nonstandard applications on a group of ports.

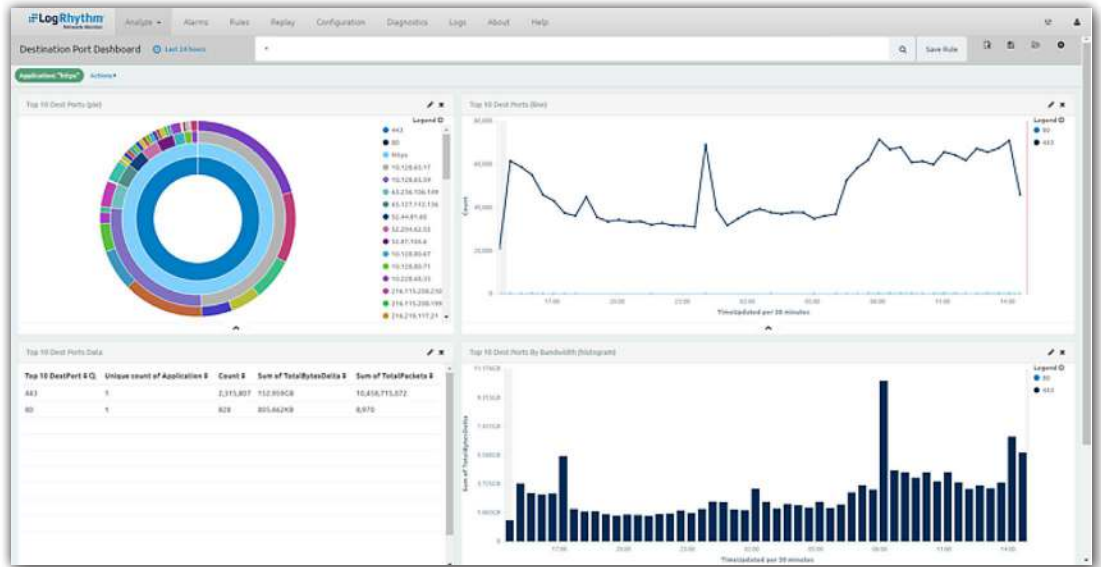


Figure 16. Port and Protocol Mismatches

Upon investigation, it seemed to be a set of switch anomalies or misconfigurations that were likely operations issues, not security issues (shown in Figure 17).

December 7th 2016, 14:26:05.000	DPA:Flow_ProtocolMismatchApp	medium	smtp	80211q-1f1e-980e-da7296a6377	10.128.64.220	169.45.89.184	11,656	587	/80211q/1f1e-980e-da7296a6377
December 7th 2016, 14:26:03.000	DPA:Flow_ProtocolMismatchApp	medium	smtp	80211q-1f1e-980e-da7296a6377	10.128.64.220	169.45.89.184	10,895	587	/80211q/1f1e-980e-da7296a6377
December 7th 2016, 14:26:03.000	DPA:Flow_ProtocolMismatchApp	medium	smtp	80211q-1f1e-980e-da7296a6377	10.128.64.220	169.45.89.184	10,660	587	/80211q/1f1e-980e-da7296a6377
December 7th 2016, 14:26:03.000	DPA:Flow_ProtocolMismatchApp	medium	smtp	80211q-1f1e-980e-da7296a6377	10.128.64.220	169.45.89.184	9,329	587	/80211q/1f1e-980e-da7296a6377
December 7th 2016, 14:26:03.000	DPA:Flow_ProtocolMismatchApp	medium	smtp	80211q-1f1e-980e-da7296a6377	10.128.64.220	169.45.89.184	10,056	587	/80211q/1f1e-980e-da7296a6377
December 7th 2016, 14:26:03.000	DPA:Flow_ProtocolMismatchApp	medium	smtp	80211q-1f1e-980e-da7296a6377	10.128.64.220	169.45.89.184	10,523	587	/80211q/1f1e-980e-da7296a6377

Figure 17. 802.1Q Configuration Issues Causing Alarms

In a span of just a few minutes, we were able to look at the primary traffic leaving the environment, drill into ports and services seen in this traffic, and isolate different services and traffic that might warrant additional investigation through network forensics or endpoint analysis.



Case 3: Sensitive Data Identification

The third case we evaluated with NetMon Freemium was centered on sensitive data identification using more in-depth traffic analysis and detection rules. In this scenario, we started by exploring the DPA rules LogRhythm has in place, which include templates for credit cards and bank routing information (financial content), Social Security and other personal identifier numbers, and cleartext passwords.

The first rule we looked at was monitoring for payment card data in HTTP, SMTP and FTP (cleartext communication protocols). A snippet of the rule is shown in Figure 18, with parameters specific to each major credit card type seen today.

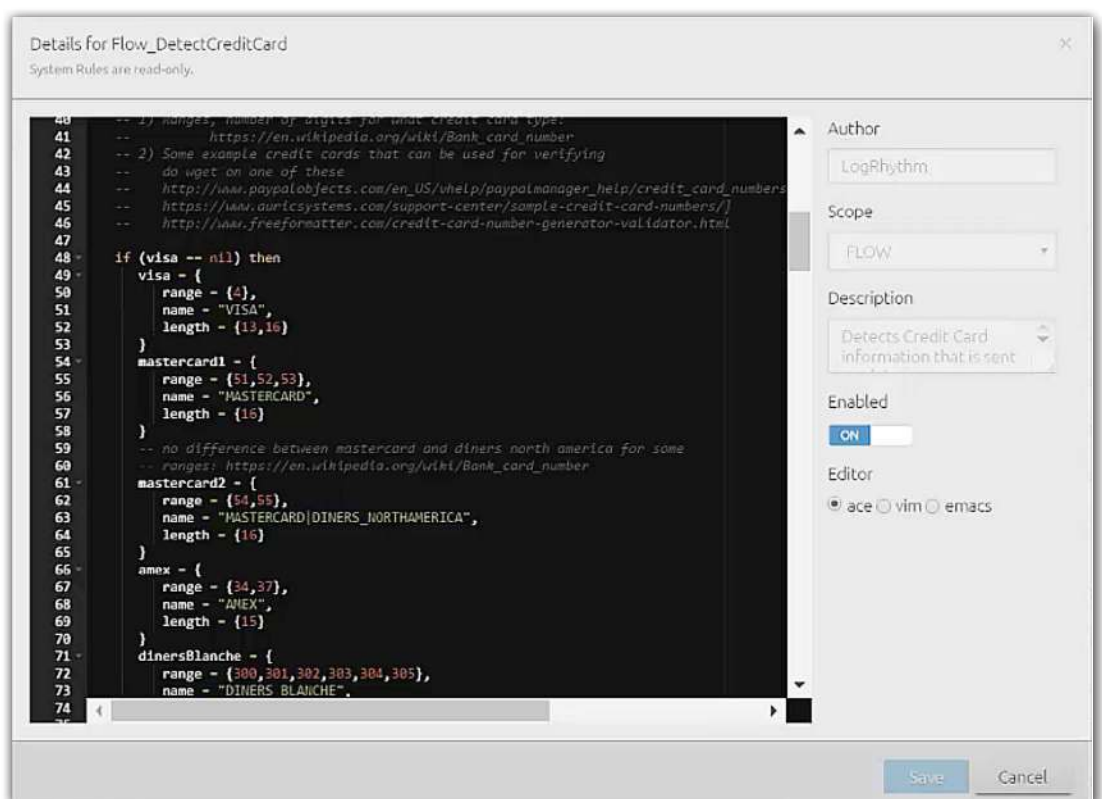


Figure 18. DPA Rule for Payment Card Number Identification



Use Cases: Bandwidth, Malware, Data Leakage (CONTINUED)

After exploring some of the DPA rules available, we used the Replay function to load and fire a PCAP that included credit card information. This showed up quickly within the Alarms dashboard, and we drilled into the event as shown in Figure 19.

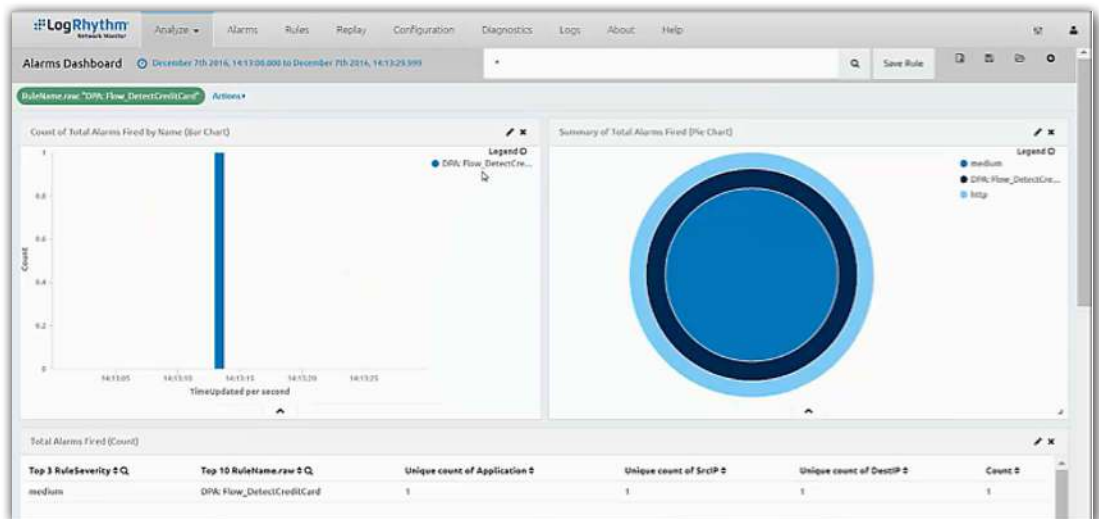


Figure 19. Credit Card DPA Rule Alarm

As expected, the Flow_DetectCreditCard rule triggered the alarm. By drilling into the details of the alarm, we saw what content triggered the rule. We could then determine whether the alarm was a false positive or worthy of further investigation by examining the packet details (see Figure 20).

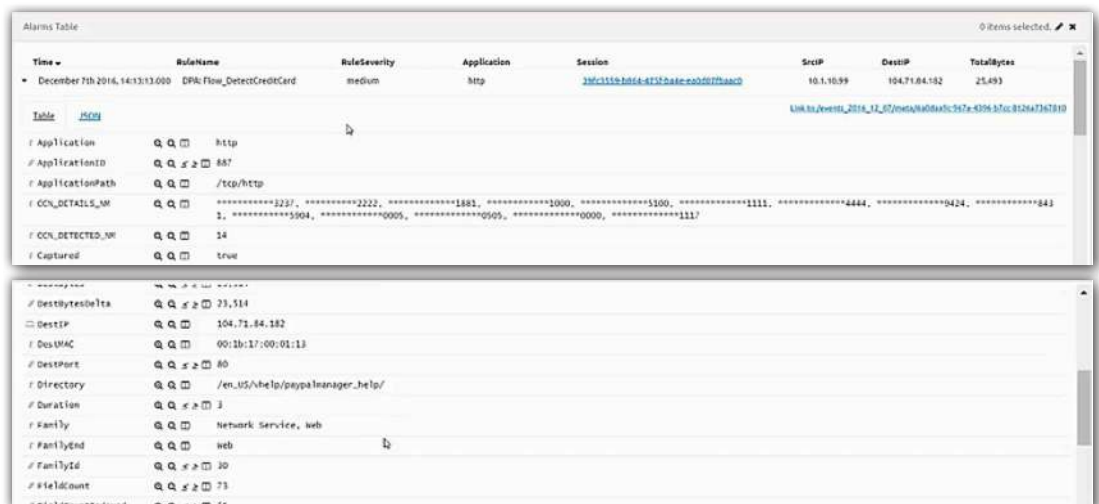


Figure 20. Credit Card DPA Alarm Details



Based on the data, this certainly looked like credit card information, so we would want to follow up on why it was being sent across the network.

We repeated the same test for several other DPA rules and categories, including cleartext passwords and Social Security numbers, with similar results (detection on the expected rules). While we did not create custom DPA rules ourselves, LogRhythm has provided a number of these “out of the box” for many sensitive data types. Using these DPA rules to trigger custom DLP alarms for detection and incident response was easy to do, and any analyst could adapt this strategy to improve the state of sensitive content monitoring strategies internally.



Conclusion

LogRhythm's NetMon Freemium provides a good example of how intelligent network monitoring is—and should be—in detecting rogue applications, data leakage, lateral movement and more important indicators of compromise that normally go undetected.

The NetMon web interface setup is simple, the interface is intuitive, the capabilities are powerful and robust, and the price—free—can't be beat!

In our review, we got the chance to take a look at the product's dashboards and filtering, and within 30 minutes, we felt as though we knew exactly what we were doing and how to drill down into reports and packets, set new rules, and more. The filter syntax is easy to learn, but much more advanced filters can also be created and easily turned into rules as well.

We had no problem identifying interesting and unusual traffic in the test environment. We were particularly impressed with the ability to capture traffic and then replay it to test filter rules. This, in our minds, makes NetMon Freemium an analysts' tool as much as a pure network detection tool.

With more traffic than ever passing through our environments, and adversaries who know how to blend in, network security analysts need all the help they can get. When that help is free, that's even better. But free or not, the tool impressed us, and we can easily see how this would improve detection and response capabilities in any major security operations center today.



About the Author

Dave Shackleford, a SANS analyst, instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsor

SANS would like to thank this paper's sponsor:

