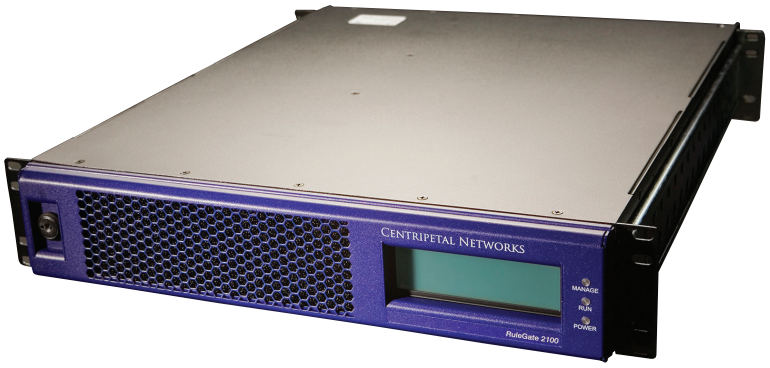


## Centripetal Networks

# Network Protection System v2.1

### DETAILS

**Product** Network Protection System v2.1

**Company** Centripetal Networks
*http: www.centripetalnetworks.com/*

**Price** Starts at $60,000.

**What it does** Active network defense merging cyber threat intelligence and security stack management.

### OUR BOTTOM LINE

This is an industrial-strength integration of cyber threat intelligence with system management. It plays well with other network security tools because it was designed from the ground up to do exactly that. As well, it consumes threat intelligence and converts that into actionable intelligence that can be applied to a SIEM or other tool. It is easy to configure and has a rich feature set at the executive, system operator and analyst levels.

There is a lot to do and see here, and the complexity of the threatspace is reflected somewhat in the system and its tools.

So, our bottom line here is this is a notable tool and certainly one of the best integrations of intelligence and security stack management we've seen. However, it is not for the faint-hearted. But then, playing in today's threatscape isn't either.

This is an interesting product. It collects threat intelligence data from a variety of sources, including its own organization, and applies that intelligence to manage network protection at the enterprise. By partnering with a number of threat intelligence providers and several technology vendors, Centripetal's Network Protection System (NPS) provides what the company refers to as Active Network Defense.

NPS operates in such a way as to provide support for analysts, systems operators, CxOs and executive management. That means that it produces the sorts of outputs that are uniquely useful to each of these groups. Because the difference between actionable intelligence and the flow of threat data from internet sensors is noise, the object is to get rid of the noise so that the actionable data is exposed. That is an important layer of NPS functionality.

In each of the cases above, NPS not only provides the unique kind of data needed by the particular audience, it focuses that data in the ways most useful at that level. So, for example, for the analyst, NPS focuses on the data, matching the analysis to the expected analyst workflow. For the system operator, the focus is on managing the security stack. And for the executive, NPS provides situational awareness and presents data in the form of effective use of resources and budget. These varying perspectives result in a completely unique approach to actionable cyberthreat intelligence.

The heart of the NPS is the RuleGate threat intelligence security layer. This is an appliance that manages five million threat indicators at wire speeds up to 10Gbps. It is policy driven and enforces its policies across the enterprise correlating internal hosts and external threats. It is not intended to be a standalone solution to the security challenges of the enterprise. Rather, NPS works with other network security components to improve its overall security posture.

There are some intelligence feeds from external sources, including open source and Centripetal's own, but you can purchase commercial feeds through the platform itself. Those feeds integrate into the system, which consumes, integrates and correlates the data as part of QuickThreat.

Rule sets are easy to use and the user interface is comprehensive. The system looks at both inbound and outbound data flows and tracks TOR exit nodes. The UI is web technology, but it is a custom implementation that uses a wrapper for browser compatibility. This is a serious system built from the ground up – no customized off-the-shelf appliances here – by Centripetal in the United States.

CENTRIPETAL NETWORKS

2251 Corporate Park Drive, Suite 150
Herndon, VA 20171
571-252-5080
info@centripetalnetworks.com
www.centripetalnetworks.com