NORSE APPLIANCE™ LE

PRODUCT DATA SHEET

The Global Threat Intelligence™ System

The richest data available to monitor network traffic and deliver pre-filtered threat events—with full context—to your favorite SIEM

FEATURES

- » Enterprise-specific GUI with a custom dashboard
- » Analyzes global range of data sources to send only pre-filtered and pre-vetted events
- » Injects pre-filtered and pre-vetted logs into your SIEM with full context

BENEFITS

- » Offers context-sensitive global threat intelligence in real time
- » Empowers organizations to be pre-emptive rather than reactive
- » Delivers enhanced threat context for installed base of SIEMs
- » Offloads expensive SIEMs to help avoid purchasing new hardware

Norse Appliance LE 2.0 empowers organizations with the highest level of protection through rich threat intelligence and the critical context your SIEM needs to make faster and better decisions about incidents that truly deserve attention. Norse Appliance LE 2.0 records interactions with malicious IPs and URLs from a global range of data sources and sends pre-filtered and pre-vetted events—with lower false positives—to your SIEM. Norse Appliance LE 2.0 builds on the broadest sensor network worldwide to enable faster and better incident response than any threat intelligence system available.

The live Norse threat intelligence data stream covers millions of malicious and suspicious IP and URL addresses to match threats with client-specific concerns such as geolocation, threat type, risk score, launch and target organizations, and more. This is a dynamic environment, with data points changing second-by-second. Most enterprise SIEM systems aren't built to process these vast data loads, let alone manage a dynamic live stream.

Norse uses innovative technologies—including emulation, mousetrap and pcap data capture from attacks and reconnaissance—to filter out extraneous data and prioritize up-to-the-second attack warnings. Norse Appliance LE 2.0 features an enterprise-specific GUI with a custom dashboard, 10GB bandwidth, UDP, all ports/all protocols, directionality (in vs. out source) and targeted data analysis.

Powered by the Norse Intelligence Network

The Norse Intelligence Network is a globally distributed ‘distant early warning’ grid built on millions of sensors, honeypots, crawlers, and agents that deliver unique visibility into the darknets where bad actors operate. Processing hundreds of terabytes daily—encompassing social media, categorization, malware augmentation, 5 million to 20 million emails a day, whois and whowas for all domains seen, URL/IP context and threat taxonomy—Norse computes over 1,500 distinct risk factors for millions of IP addresses every day. The Norse network continuously analyzes traffic to organically monitor the world’s most comprehensive data library to identify compromised hosts, malicious botnets, anonymous proxies, and other threat sources and attack originators that SIEMS miss on their own.

How to Buy

Call Norse at +1 972.333.0622 for a demonstration or quote, or email us at http://www.norsecorp.com/products/norse-appliance

ABOUT NORSE

Norse is the global leader in live attack intelligence, helping companies block the threats that other systems miss. Serving the world’s largest financial, government and technology organizations, Norse intelligence offerings dramatically improve the performance, catch-rate, and return-on-investment of the entire security infrastructure. The Norse Intelligence Network, a globally-distributed “distant early warning” grid of millions of sensors, honeypots, crawlers, and agents, delivers unmatched visibility into difficult-to-penetrate geographies and darknets, where bad actors operate. Norse processes hundreds of terabytes daily against a 7 petabyte attack history database, and weighs over 1,500 variables to compute real-time risk scores for millions of IP addresses and URLs every day.