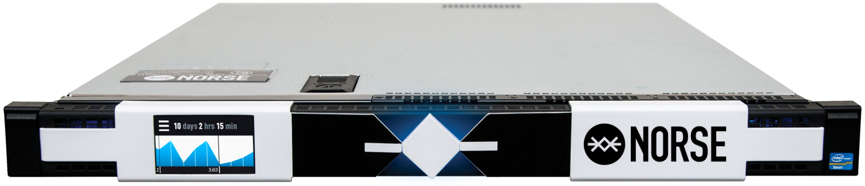
NORSE APPLIANCE™

PRODUCT DATA SHEET

Norse Intelligence Network: The Hardline to Top-Tier Security

Detect attacks before they target your network, and dramatically improve the ROI on your existing security infrastructure.



> *"This is the Cadillac of cyberthreat assessment tools."*
>
> SC MAGAZINE

Norse Appliance Use Cases:

- Detect attacks and virtualization-evading malware from darknets that most current systems miss
- Protect your organization from careless users clicking on dangerous links in phishing emails, risky websites, social media or IMs
- Stop organizational data theft via Tor or anonymous proxy
- Filter and correlate torrents of event data from your existing security systems to alert you to what's truly important

Perfect For:

- Large Financial Institutions
- Government & Intelligence Networks
- Fast-Growing, Billion-Dollar Tech Firms

In July 2014 benchmarks against 35 competing products, Norse Appliance™ identified ***3x more*** *malicious IPs and URLs. In fact,* ***74% of the threats*** *identified by Norse Appliance were not discovered from any other offering, commercial or open source.*

After all the resources devoted to security, why are there still so many breaches?

Here's one good reason: The layers of security built into the infrastructure generate thousands of lines of event logs that nobody has the time to review. That's a real problem, because your existing security appliances, next-generation firewalls, intrusion prevention systems and SIEMs can defend only against attacks they've seen before. Unknown threats get buried in endless log files of 'unusual events.'

The Problem: Your Unknown Unknowns

The balance of power is shifting against the defender. The threat landscape is rapidly changing, from generally understood attack vectors to those entirely new—the unknown unknown. Threats like virtualization-evading malware, stealthy anonymous proxies like Tor, polymorphic malware and URLs, and a growing onslaught of attacks from millions of compromised embedded devices represent the dark underbelly of the 'Internet of Things.' To make matters worse, these threats increasingly incubate on darknets—a region where traditional threat intelligence tools give little or no visibility.

The Solution: Norse Appliance™

Meet the Norse Appliance™, the first live attack intelligence appliance to detects and defend against the newest, most advanced threats on the Internet—yes, even darknets. During benchmark testing in July 2014 against 35 other popular commercial and open source threat intelligence offerings, at least 74% of the threats identified by Norse Appliance were not caught by any other offering, commercial or open source.

Superior, More Actionable Intelligence

Norse Appliance doesn't just identify more new threats—it tells you which threats are actually worth worrying about. Norse Appliance uses an advanced artificial intelligence engine built into the Norse Intelligence Network platform to distill thousands of risk factors on millions of IPs, URLs and domains—live—to deliver a single, actionable risk score. You can easily configure automatic actions based on the Norse Appliance risk score for each IP. Furthermore, Norse Appliance protects against malicious traffic—even when it's encrypted—and scales up to even the largest networks.

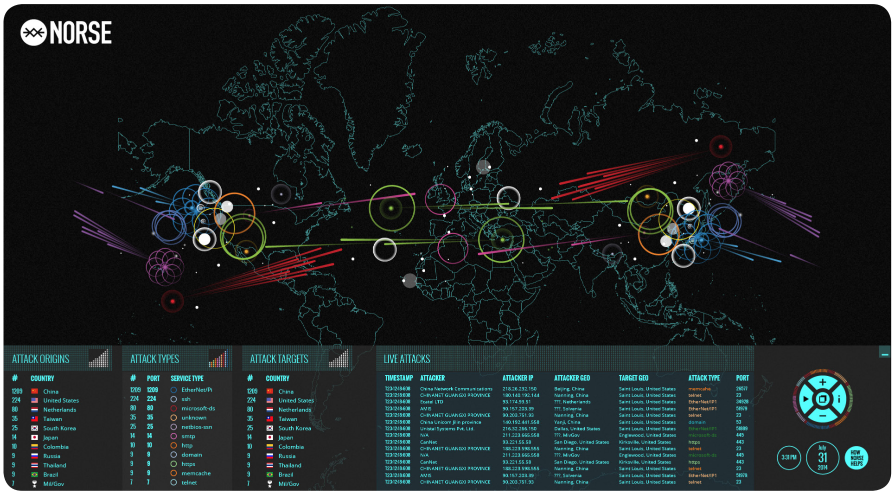
Deployed inline or out of band, Norse Appliance leverages the global Norse Intelligence Network™ to alert you in real-time to malicious URLs, botnets, anonymous proxies, bogus IPs, and infected embedded devices operating anywhere in the world, before they target your networks. Best of all, Norse Appliance works with existing next-generation firewalls, intrusion prevention systems, and SIEMs to dramatically improve the ROI on your entire security investment by lightening their loads and stopping attacks they miss. That means deferring expensive equipment purchases as the network grows.

NORSE APPLIANCE™

PRODUCT DATA SHEET

Over-the-Horizon Malware Detection

The Norse Appliance leverages the Norse Intelligence Network to protect against new and unknown malware. . .even malware still in development. The Norse Intelligence Network checks millions of domains daily for malware, identifying new binaries even before they're released into the wild. Many security appliances use virtual machines to try and 'trap' malware before it reaches targeted systems. But today's malware variants are savvy to those approaches and can stay 'dormant' while it passes through virtual machine-based malware detection systems. The Norse Appliance works differently: It doesn't depend on signatures or virtual machines, so it catches malware other products miss.



ATTACK ORIGINS

#	COUNTRY
1209	China
224	United States
80	Netherlands
35	Taiwan
25	South Korea
14	Japan
10	Colombia
9	Russia
9	Thailand
9	Brazil
7	Mil/Gov

ATTACK TYPES

#	PORT	SERVICE TYPE
1209	1209	○ EtherNet/Pi
224	224	○ ssh
80	80	○ microsoft-ds
35	35	○ unknown
25	25	○ netbios-ssn
14	14	○ smtp
10	10	○ http
9	9	○ domain
9	9	○ https
9	9	○ memcache
7	7	○ telnet

ATTACK TARGETS

#	COUNTRY
1209	China
224	United States
80	Netherlands
35	Taiwan
25	South Korea
14	Japan
10	Colombia
9	Russia
9	Thailand
9	Brazil
7	Mil/Gov

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
T23:12:18:608	China Network Communications	218.26.232.150	Beijing, China	Saint Louis, United States	memcahe	26577
T23:12:18:608	CHINANET GUANGXI PROVINCE	180.140.192.144	Nanning, China	Saint Louis, United States	telnet	23
T23:12:18:608	Ecatel LTD	93.174.93.51	???, Netherlands	Saint Louis, United States	EtherNet/IP1	34928
T23:12:18:608	AMIS	90.157.203.39	???, Solvenia	Saint Louis, United States	EtherNet/IP1	51979
T23:12:18:608	CHINANET GUANGXI PROVINCE	90.203.751.93	Nanning, China	Saint Louis, United States	telnet	23
T23:12:18:608	China Unicom Jilin province	140.192.441.558	Yanji, China	Saint Louis, United States	domain	53
T23:12:18:608	Unistal Systems Pvt. Ltd.	216.32.266.150	Dallas, United States	Saint Louis, United States	EtherNet/IP1	51889
T23:12:18:608	N/A	211.223.665.558	???, MivGov	Englewood, United States	microsoft-ds	445
T23:12:18:608	CanNet	93.221.55.58	San Diego, United States	Kirksville, United States	https	443
T23:12:18:608	CHINANET GUANGXI PROVINCE	188.223.598.555	Nanning, China	Saint Louis, United States	telnet	23
T23:12:18:608	N/A	211.223.665.558	???, MivGov	Englewood, United States	microsoft-ds	445
T23:12:18:608	CanNet	93.221.55.58	San Diego, United States	Kirksville, United States	https	443
T23:12:18:608	CHINANET GUANGXI PROVINCE	188.223.598.555	Nanning, China	Saint Louis, United States	telnet	23
T23:12:18:608	AMIS	90.157.203.39	???, Solvenia	Saint Louis, United States	EtherNet/IP1	51979
T23:12:18:608	CHINANET GUANGXI PROVINCE	90.203.751.93	Nanning, China	Saint Louis, United States	telnet	23

The Norse Appliance Live Attack Map provides a detailed view of previously-unknown threats traversing your networks, including anonymous proxy traffic, cloud vectors, advanced malware threats, and compromised embedded device traffic.

Easy Setup, Fast Deployment: HW or Virtual

Setup is fast and easy—most businesses are up and running the day their Norse appliance arrives. Just configure the Norse Appliance through the integrated touchscreen LCD, and it's ready to go.

Key Features:

- Continuous second-by-second updates of dark intelligence from the global Norse Intelligence Network
- Deploys inline or out-of-band offloading expensive SIEMs and catching what you're missing now
- Detects incoming and outgoing IP- and URL-based attacks
- Works even if traffic is encrypted
- Detects virtualization-evading malware
- Available in 10 Gbps and 16 Gbps models

How to Buy

Call Norse at +1 972.333.0622 for a demonstration or quote, or email us at sales@norsecorp.com

Silicon Valley
333 Hatch Drive
Foster City, CA 94404
650.513.2881

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.

NORSE norsecorp.com