NORSE INTELLIGENCE SERVICE™

PRODUCT DATA SHEET

Timely and Relevant Global Threat Intelligence—In Context

The Norse Intelligence Service continuous threat monitoring program provides the depth and breadth of visibility needed to identify relevant malicious activity across each enterprise and its connected partners' networks. This enables a truly proactive security posture and rapid threat mitigation.

Features:

- Continuous threat monitoring with local, partner/supply chain, and global relevance
- Perimeter monitoring combined with deep web visibility for extraordinary context
- Flash reports deliver actionable findings for agile security
- Monthly reports deliver actionable trends, actor analysis and recommended actions
- Incident response and hunting support shorten time to resolution
- Enterprise GUI to display relevant activity, provide report access and support customer-analyst collaboration

Benefits:

- Gain immediate threat intelligence partner without the time and cost delays of building internal and organic capabilities
- Receive early warnings of threat activity
- Identify compromises in corporate and connected partner networks
- Eliminates signal-to-noise ratio of traditional threat intelligence programs
- Gain the power of Norse Live Attack Intelligence specifically tailored to your organization

Threat Intelligence use is growing rapidly, but organizations still can't get actionable context. Feeds of varying degrees of accuracy, high-level reports without actionable recommendations, and a shortage of security analysts remain weak spots despite heavy investment. The Norse Intelligence Service cuts through the Threat Intelligence signal-to-noise ratio by continuously monitoring relevant client activity and comparing it to the global threat trends that only Norse can identify. The result is contextual intelligence for a true early warning system.

Deep Visibility, Relevant Intelligence

Unlike high-level threat reporting services that deliver global views without actionable findings, Norse combines local threat monitoring with a custom global view to understand precisely when an adversary has pivoted from scanning to targeting. Norse fusion analysts continuously monitor global and customer-specific activity and correlate this traffic to the vulnerability landscape to immediately notify companies of the remediation actions needed. We combine this analysis with continuous monitoring of our customers' critical assets to detect beaconing and other bot activity emanating inside a customer's (and connected partners') perimeter to pinpoint internal infections early.

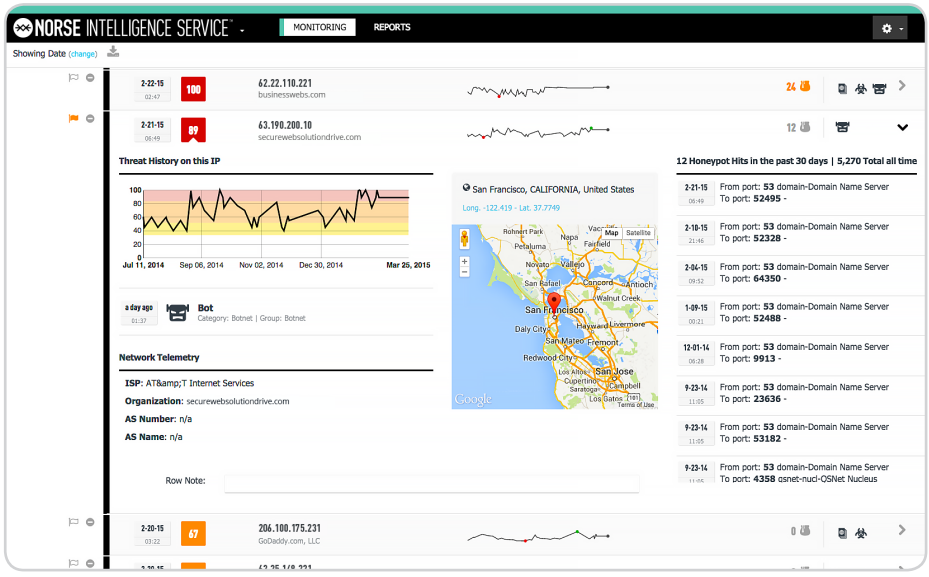
Urgent findings are delivered via flash reports that outline specific remediation actions that must be taken to defeat these threats before they lead to a larger compromise or breach. Monthly reports provide deep dives into critical trending and actor behavior, allowing organizations to gain strategic ground and greater agility in threat prevention. Norse augments the offering with investigation and hunting support that allows companies to leverage our sophisticated fusion and malware analysts to shorten the mean time to respond (MTTR).

NORSE INTELLIGENCE SERVICE™

PRODUCT DATA SHEET

The Secure Portal for a Common View

All findings are delivered via the Norse Intelligence Service (NIS) Portal. This includes important events that indicate compromise or direct targeting and associated analyst reports that present urgent findings and actions. All events are annotated using the Norse Live Attack Intelligence taxonomy, historical trending and detailed activity analysis for additional context.



Powered by the Norse Intelligence Network

The Norse Intelligence Service is powered by our trained analysts using the Norse Intelligence Network – a massive system of sensors, crawlers and malware analysis systems that provides unprecedented visibility into Live Attack Intelligence.

Norse Intelligence Service Sample Findings

- Global activity from China focusing in on a customer on a port after an associated vulnerability was released.
- Beaconing from compromised VoIP phone in Chief Executive's office
- In-depth malware analysis found at client site that identified a large breach in progress

Norse Intelligence Service provides 24x7 monitoring for indicators of compromise and threat targeting.

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.