NORSE

PRODUCT DATA SHEET

Preventing Advanced Attacks with McAfee Next Generation Firewall and Norse Live Dark Intelligence

Integrating dark intelligence into edge security for rapid detection and prevention of advanced threats

McAfee
Security Innovation Alliance

Use Cases:

- Proactive blocking or alerting on high risk connections for advanced malware and targeted attack detection
- Risk-based threat prioritization for improved incident response
- Post-attack forensics to quickly detect and mitigate compromises reducing risk of breach

Key Features:

- Centralized management of threat feed data to meet business objectives
- Automated deployment to remote firewalls

Solution Benefits:

- Highlights advanced threats and other high risk activity
- Identification of targeted attacks missed by today's security point products
- Automated blocking or alerting through Norse dark threat intelligence integration with
- McAfee NGFW

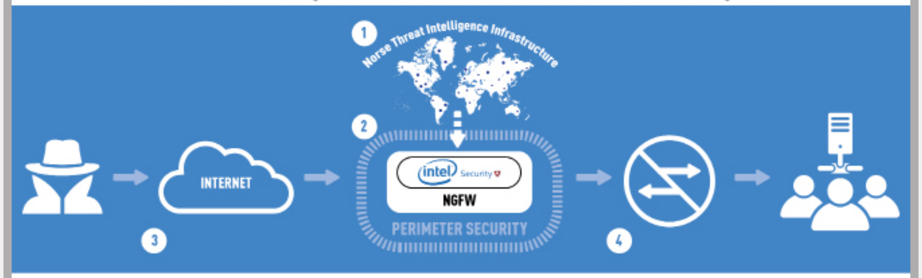
Norse's live dark intelligence combined with McAfee Next Generation Firewall (NGFW) provides enhanced capabilities for detecting and preventing advanced threats. Integrating Norse threat intelligence into McAfee NGFW enables the firewall to proactively block known and unknown attacks. Norse provides contextual, risk-weighted, and continuously updated threat intelligence collected from its global infrastructure, including anonymous darknets and the deep web from where many bad actors operate. The integration adds critical external context to internal security events enabling rapid advanced threat detection risk-based prioritization of threats and incident response, and reduction of the time for analysts to get from data to insight to resolution.

Norse provides threat intelligence via two complementary methods:

Norse DarkList, a list of the 3 million highest risk IPs on the Internet with basic context. DarkList is imported into McAfee NGFW through automated scripts run on the management server that enable users to set threat thresholds and distribute rules to multiple firewalls. DarkList includes a 0-100 risk score for each IP, the risk category (such as "botnet" or "Tor proxy") to provide context to the score, and highly accurate geolocation.

Norse DarkViking, a real-time lookup-based solution that provides live data, deeper threat context, and years of history for individual IP addresses. Norse users have access to the DarkViking portal which lets them retrieve detailed data about any IP including full context and historical information.

USE CASE: Connecting Internal Events with External Threats Via Firewall Integration



1 Norse Darklist of the Internet's highest risk IPs retrieved regularly via API from Norse
2 Norse Darklist score thresholds configured by customer to meet business objectives and pushed out to NGFW
3 Cybercriminal targets externally facing IP addresses using compromised systems / Tor / botnet network
4 Incoming connection from attacker/high risk IP identified and blocked or mitigated by McAfee NGFW

Silicon Valley
1825 South Grant Street, Suite 635
San Mateo, CA 94402 | 650.513.2881

Saint Louis
101 South Hanley Road, Suite 1300
St. Louis, MO 63105 | 314.480.6450

ABOUT NORSE

Norse is the global leader in live attack intelligence. Norse delivers continuously-updated and unique Internet and darknet intel that helps organizations detect and block attacks that other systems miss. The superior Norse DarkMatter™ platform detects new threats and tags nascent hazards long before they're spotted by traditional "threat intelligence" tools. Norse's globally distributed "distant early warning" grid of millions of sensors, honeypots, crawlers and agents deliver unique visibility into the Internet – especially the darknets, where bad actors operate. The Norse DarkMatter™ network processes hundreds of terabytes daily and computes over 1,500 distinct risk factors, live, for millions of IP addresses every day. Norse products tightly integrate with popular SIEM, IPS and next-generation Firewall products to dramatically improve the performance, catch-rate and security return-on-investment of your existing infrastructure.