NORSE

SOLUTION BRIEF

Meeting FFIEC Supplemental Guidance: Assessing Risk Using Live Threat Intelligence

Increasing the Efficacy of Existing Anti-Fraud Detection and Prevention Systems to Reduce Operational and Fraud Related Risk

In 2011, the Federal Financial Institutions Examination Council (FFIEC) issued a supplement to the "Authentication in an Internet Banking Environment" to promote security practices in electronic banking with formal assessments of financial institutions beginning in January 2012.

Sophistication of Fraud Attacks Increase

The FFIEC supplemental guidelines highlight the need of Financial Services organizations such as banks, online trading services and credit unions to enhance existing anti-fraud solutions with formal risk assessments, adjustments to customer authentication controls in response to new online account threats, the implementation of effective strategies for mitigating risk, and raising the customer awareness of threats associated with electronic banking.

At a basic level, threats can be broken down into 3 main target categories:

» Threats Targeting the Financial Institution

» Threats Targeting the Business Banking Customer

» Threats Targeting the Consumer Banking Customer

Financial institutions and their customers have seen a significant increase in risk and experienced substantial losses from direct institutions attacks, online account takeovers, account origination fraud, as well as business-related ACH and wire fraud.

Traditional Defenses Need to Adapt

The nature of institution and transaction attacks has rapidly changed over the last decade. With multiple attack vectors and a rapidly evolving threat landscape, the use of advanced techniques and attacks to perpetrate fraud can be achieved by targeting the financial institution's website, breaching perimeter security to directly access critical systems, or compromising the consumer or business customer directly.

Cybercriminals today use a combination of advanced attacks such as phishing, trojans, man-in-the-browser attacks, and the use of anonymous proxies such as TOR (The Onion Router) to help mask the true origin of an attack and the locations of botnet command and control servers.

Leveraging New Technologies to Enhance Existing Security Investments

The FFIEC supplemental guidance specifically identifies Internet Protocol (IP) reputation-based technology as a primary recommendation in the layered security model as a means to identify and block connections to critical banking servers from IP addresses known or suspected to be associated with fraudulent activities. However, IP reputation services have become less effective over the last few years, unable to keep pace with the different attack vectors or the speed with which IP addresses can change their risk, threat characteristics, and profile.

Using Norse Live Threat Intelligence to Accurately Assess True Risk

The depth of intelligence required to combat this ever-changing threat landscape must move beyond blanket flagging of suspicious IP addresses to a fully-fledged, contextual IP intelligence service using multi-factor risk scores and geolocation information to block the sources of threats and fraudulent transactions as they happen.

Norse Live threat intelligence enables organizations to instantly assess the risk level and threat profiles of any IP address visiting a web page, attempting an account log-in, originating a new account application, or initiating an online transaction. The Norse Live Intelligence Platform continuously detects millions of in the wild IP risk factors. Within 5 seconds each risk factor is systematically analyzed, categorized, added to an IP's timeline and history, and available as IP Intelligence for customers.

The end result is a trail of information and history for any given IP address to reveal negative, unethical, or illegal behavior. 1,500 factors are analyzed by Norse per IP address and are used to identify threats within milliseconds, giving financial organizations a new layer to their security and anti-fraud controls that proactively adapts to the evolving threat landscape and enhancing existing perimeter security, website security, eCommerce fraud protection, and zero day threat mitigation.

Key Features of Norse Solutions

- SaaS based delivery of live threat and fraud intelligence
- Configurable IPQ Risk Score allows easy implementation of risk-weighted decisions and controls
- Contextual risk categories enable creation of rules and polices unique to your business
- Geofilter and GeoMatch scoring identify fraud by geographical attributes
- Flexible REST API enables rapid lightweight integration and deployment
- Powerful analytics that provide rich and comprehensive reporting data

Key Benefits for Financial Services Organizations

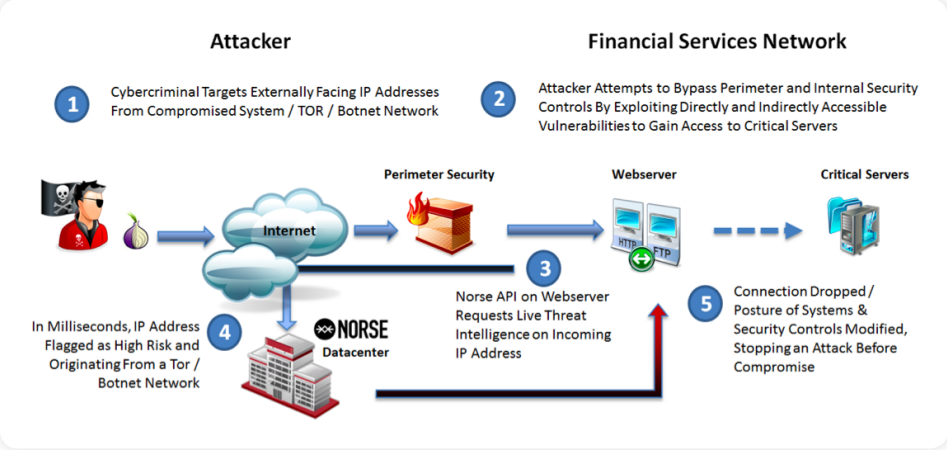
- Reduced customer account takeover fraud via stolen credentials
- Lowers the cost of direct fraud, customer service, and fraud investigation
- Reduced costs from fraudulent account creations
- Improved customer experience by minimizing out of band authentications

How to Buy

DarkList is available as an annual subscription based on company size. Call Norse sales at +1 972.333.0622 for a demonstration or quote, or email us at sales@norse-corp.com

DarkViking is available as an annual subscription based on company size. Call Norse sales at +1 972.333.0622 for a demonstration or quote, or email us at sales@norse-corp.com

DarkWatch is available as a bundled 1U hardware and virtual appliance, and volume discounts are available. Call Norse sales at +1 972.333.0622 for a demonstration or quote, or email us a sales@norse-corp.com



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.