NORSE

INDUSTRY BRIEF

Health Care Fraud and Patient Data Exposure: Live Attack Intelligence-based Strategies to Reduce Risk

> "Security architects in the financial world [have] a very black and white transaction model. If you compare that to medical records, to healthcare insurance…there is almost no uniformity, no standardization in how many of these interactions work. Much of that organizational mess translates to the technical protocols that we have to use. You pick whatever you think is going to solve your problem."
>
> **Gunnar Peterson**
>
> Security expert, managing principal at Minneapolis-based Arctec Group

In addition to high costs of time and financial loss, health care organizations experiencing a data breach can expect severe penalties imposed by the government for violating the HIPAA mandate, costs for investigation and administration of fraud claims, and loss of customer loyalty and brand reputation.

Health Care Organizations a Multi-Tiered Window of Risk

Health care organizations present a uniquely appealing target for fraudsters. These organizations typically store highly valuable data, including patient Social Security number, insurance and/or financial account data, birth date, name, billing address, and phone. At the same time, to maintain connection with patients, employees, insurers, and business partners, health care organizations must provide access to an unusually large number of external networks and web applications. This multi-tiered window of exposure makes health care organizations increasingly vulnerable to online attack.

Conventional signature and policy-based defenses such as firewalls, IPS, anti-malware, and authentication systems have become less and less effective as the speed and sophistication of advanced malware and hacker attacks has continued to accelerate. These solutions meet basic standards required for securing stored data, controlling access to data, ensuring availability of data and applications, and monitoring system and network events to reduce the risk of compromise – but it is in many cases not enough to combat the constantly changing threats and techniques used by cybercriminals.

Traditional Defenses Lack Depth to Make Automated Decisions

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 health care organization's website, breaching perimeter security to directly access critical systems, or compromising the site user 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

While traditional security controls used in a layered security strategy have largely met the needs of health care organizations, they have proven to be virtually static in their defense and lack the knowledge and flexibility to proactively defend against the speed and sophistication of new advanced and zero-day threats.

Internet protocol (IP) reputation-based technology can be implemented into the layered security model as a means to identify and block connections to critical servers from IP addresses known or suspected of being associated with fraudulent activity. However, IP Reputation Services have a binary approach to blocking risky IPs and have become less effective over the last few years, many 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 Attack 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 geo-location information to block the sources of threats and fraudulent transactions as they happen.

NORSE

INDUSTRY BRIEF

Norse live attack 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 DarkMatter live attack 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.

Up to 1,500 data points are compiled by Norse per IP address and can be used to identify threats in near real-time, giving financial organizations a new layer to their security and anti-fraud controls that proactively adapts to the evolving threat landscape to enhance existing perimeter security, website security, eCommerce fraud prevention, and zero-day threat migration.

Key Features of Norse Solutions

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

Key Benefits for Health Care Organizations

- Maximize efficacy of existing security investments with Live Threat Intelligence
- Reduce customer account takeover fraud via stolen credentials
- Lower the cost of direct fraud, customer service, and fraud investigation
- Reduce costs from fraudulent account creations

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.