NORSE

INDUSTRY BRIEF

The New Threat Intelligence — For Higher Education

Educational institutions must look beyond traditional defenses to protect against advanced attacks, data breach and fraud.

> "We are already seeing universities being the target of attacks and being conduits for attacks. They have information that people want, whether it's their faculty and student names and credit card numbers and social security numbers or it's the research that they're doing."
>
> **Daniel Berger**
> President and CEO of Redspin,
> a security assessment vendor

Education Continues To Be a High Value

While financial services, retail, and government organizations generate most of the media headlines, higher education is high on the list for reported security incidents, according to recent research by The Open Security Foundation. Online attacks against educational institutions that incur security incidents and data breaches often mirror the types of losses experienced by the private sector:

- **Direct financial costs** of incident response, IT forensics, remediation, and services provided to victims
- **Theft** of research and intellectual property
- **Loss of reputation** with students, alumni, faculty and the greater community.

Rapidly Changing Attacks Add To Defense

Universities are prime targets for a variety of bad actors each with different motivations and attack vectors including:

- **Cybercriminals** motivated by financial gain targeting valuable personal and financial information
- **Hacktivists** motivated by political and social causes
- **Industry and nation state** sponsored actors targeting confidential research and intellectual property.

With multiple new attack vectors and a rapidly evolving threat landscape, bad actors now use advanced malware and highly targeted attack techniques such as:

- **Targeting** known and zero day vulnerabilities in the institution's website
- **Breaching** perimeter security defenses to directly access critical servers and systems
- **Compromising** user accounts through phishing and credential-stealing malware

Cybercriminals today use a combination of advanced and targeted attacks such as spear-phishing, Trojans, Man-in-the-Browser attacks, and the use of anonymous proxies such as TOR to mask the true origin of an attack and the locations of botnet command and control servers.

Traditional Controls Not Keeping Up

Traditional security controls used in a layered security strategy have not fully protected educational institutions and have proven to be static in their defense. They lack the adaptability to proactively defend against the speed and sophistication of new advanced malware, insider and zero-day threats, and the use of Tor and anonymous proxies to hide and anonymize malicious network activity.

IP reputation-based technology are sometimes utilized as a means to identify and block connections from known bad IP addresses, however, these solutions have a binary approach to blocking risky IPs and are frequently out of date. Security intelligence traditionally collected by vendors via customer logs and aggregation of open source blocking lists prevents them from keeping pace with the multitude of attack vectors or the speed with which IP addresses can change their risk level, threat characteristics and profile.

Threat Intelligence to Accurately Assess True Risk

To effectively combat this ever-changing threat landscape requires security intelligence beyond static rules and policies and traditional IP and URL blocklists. It requires threat and attack intelligence that is live, contextual, and that provides visibility into network traffic from darknets and anonymous proxy services such as Tor – identifying the sources of threats and malicious attacks as they happen.

NORSE

INDUSTRY BRIEF

The Norse Live Attack Intelligence platform continuously detects millions of in-the-wild IP risk factors from the Internet's darknets and the deep web. Up to 1,500 data points are used by Norse to identify threats in as they happen. Within 5 seconds this data is analyzed, processed and available to organizations via API.

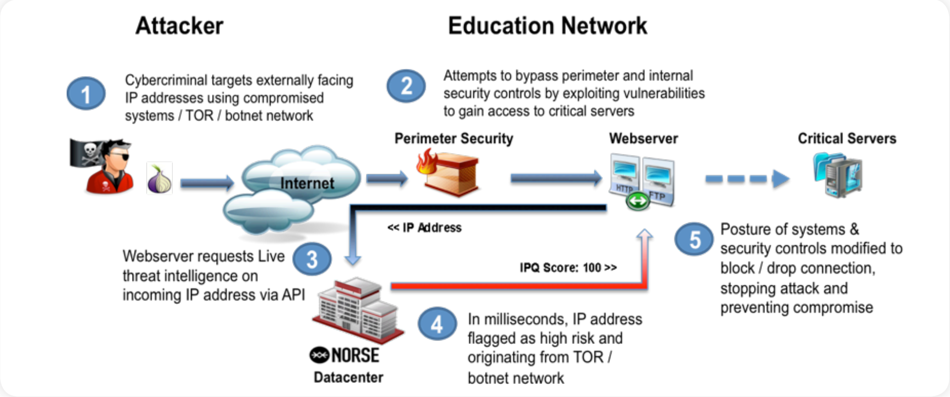
The end result is a new proactive layer in the security stack that proactively adapts to the evolving threat landscape, enhancing existing perimeter, web, and authentication security controls. When integrated with a SIEM or big data security analytics system Norse enables the correlation of internal network events with external threats to rapidly detect advanced malware and threats missed by conventional signature-based anti-malware solutions.

Key Features of Norse Solutions

- SaaS-based solution delivers live dark threat intelligence
- Configurable IPQ Risk Score allows easy implementation of risk-weighted decisions controls
- Contextual risk categories enable the creation of rules and polices unique to your organization
- Deployment via direct integration with many 3rd party security controls or a flexible RESTful API enabling rapid, light-weight web services integration
- Geofilter and GeoMatch scoring identifies account takeover fraud and security risks by IP geolocation

Key Benefits for Educational Institutions

- Enables a risk-aware and proactive security posture when integrated with traditional security controls
- Reduces the time and cost of cyber incident response, resolution, and forensics
- Improves the efficacy and ROI of existing security controls and investments
- Reduces the risk of breach from stolen user account credentials and insider threats


Attacker
Education Network
1
Cybercriminal targets externally facing IP addresses using compromised systems / TOR / botnet network
2
Attempts to bypass perimeter and internal security controls by exploiting vulnerabilities to gain access to critical servers
Internet
Perimeter Security
Webserver
HTTP
FTP
Critical Servers
<< IP Address
3
Webserver requests Live threat intelligence on incoming IP address via API
IPQ Score: 100 >>
5
Posture of systems & security controls modified to block / drop connection, stopping attack and preventing compromise
4
In milliseconds, IP address flagged as high risk and originating from TOR / botnet network
NORSE
Datacenter

How to Buy

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

Norse Live Threat Intelligence is easily integrated at virtually any point in an education institution's IT infrastructure via its flexible RESTful API, or direct product level integrations with many leading security controls.

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.

NORSE norse-corp.com