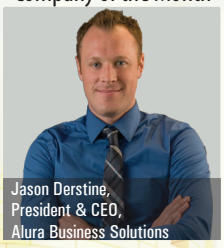
ENTERPRISE SECURITY SPECIAL

CIOReview

The Navigator for Enterprise Solutions

MARCH 13 - 2015 CIOREVIEW.COM

Company of the Month



Jason Derstine,
President & CEO,
Alura Business Solutions

Entrepreneur of the Month

Daniel Field, CEO,
AtomAMPD

NopSec: Adaptive Intelligence for Enterprise Security Needs

Lisa Xu, CEO,
NopSec

$ 15US SE 12
0 74470 91626 0

CIO REVIEW
44790, S Grimmer Blvd.
#202, Fremont, CA-94538

Lisa Xu, CEO

NopSec Adaptive Intelligence for Enterprise Security Needs

By Yeshwanth H V

The most dangerous burglars these days never pull out a gun. They lie in wait and study, looking for the right opportunity to seize upon a weakness to inject malicious code into the IT infrastructure and siphon out troves of financial and personal data, intellectual property, and other highly sensitive information.

This is one among many scenarios that keep chief information security officers awake at night, and forcing them to shell out nearly $76.9 billion on information security, an increase of 8.2 percent from the previous year, according to leading analyst firm, Gartner. It is also a reason why the cybersecurity industry is becoming a land of opportunity for futurists like Lisa Xu, CEO, NopSec. Leveraging her hunger to transform disruptive technology into leading solutions, Xu is pushing her team to 'Think like a hacker,' and in the process help fellow executives make informed decisions to reduce security risks.

Last year, the number of security vulnerabilities identified nearly doubled from the previous year. On average, 22 new vulnerabilities were identified per day. While it does not appear alarming at face value, when multiplied by the servers, applications and endpoints across the IT environment, the number is staggering. This rapid increase in vulnerabilities only adds further pressure to IT teams tasked with minimizing enterprise security risk.

"We focus on closing the window of opportunity for hackers," affirms Xu. "A bank with numerous hosts under management and security vulnerabilities has two major issues. First, they need to identify the vulnerabilities and areas they are most at risk for a data breach, and second, they need to know how to fix them—both of which are made easy with NopSec," she explains. Designed as a SaaS solution, NopSec's flagship product—Unified VRM—helps organizations find, focus, and fix the most business-critical vulnerabilities across IT infrastructure and applications.

With Unified VRM, organizations can gain control over the process of vulnerability risk management. In short, the solution eliminates the manual tasks involved with verifying the most critical threats to the business, thereby freeing up IT and security teams to focus more effort on remediation. "We don't have the staff or financial resources to dig through the noise and the false positives," notes a CSO of an international banking institution who is a customer of NopSec. "However with NopSec, even in the current environment of increased threats to our customer data, we are able to confidently report the levels of risk and the progress that we are making on remediation initiatives."


Lisa Xu, CEO

Unified VRM—From Identification to Remediation Faster

The NopSec Unified VRM SaaS solution was developed in response to increasing customer complaints about the challenges within existing vulnerability risk management processes. "Our focus is to help our customers reduce the time between identification and remediation of security vulnerabilities," states Xu.

"A mature program requires awareness of the organization's risk posture, and prioritization of remediation based on risk and business impact factors," explains Xu. This requires a streamlined process involving collaboration between different stakeholders in the workflow of identifying and classifying assets, scanning and testing these assets for vulnerabilities, analyzing the risk the vulnerabilities represent, and finally addressing these vulnerabilities on an ongoing basis. The Unified VRM platform supports all these processes to help organizations mature their security operations, and provides the tools to scan and import scans, using artificial intelligence and machine learning to forecast the likelihood of a data breach.

> Our solutions are designed to close the window of opportunity for hackers faster and with more precision

"Unified VRM is equipped with the best attributes such as an adaptive self-learning expert engine that correlates customers' IT infrastructure against attack patterns in the wild, powering a 'new era' for enterprise threat protection," says Xu. The platform works for singular applications as well as huge infrastructures that reside on-premises and in the cloud.

Unified VRM leverages vulnerability data across networks, applications and endpoints and correlates that information with external threat, exploit, malware, patching and social media feeds. Beyond just using the Common Vulnerability Scoring System (CVSS) base score, Unified VRM leverages over 500 rules and dynamic data feeds to determine the true risk of a vulnerability. By considering factors such as the business impact of breach on the asset data, the exploitability of the vulnerability through publicly available exploits, and the presence of active malware and attacks using the detected vulnerability, IT and security teams are provided with more actionable security intelligence to make better decisions on where to dedicate their remediation efforts. Beyond deep analytics, the solution also delivers out-of-the-box workflow automation capabilities, rich visualizations for improved reporting, and other built-in capabilities that allow IT teams to stay connected throughout the remediation lifecycle.

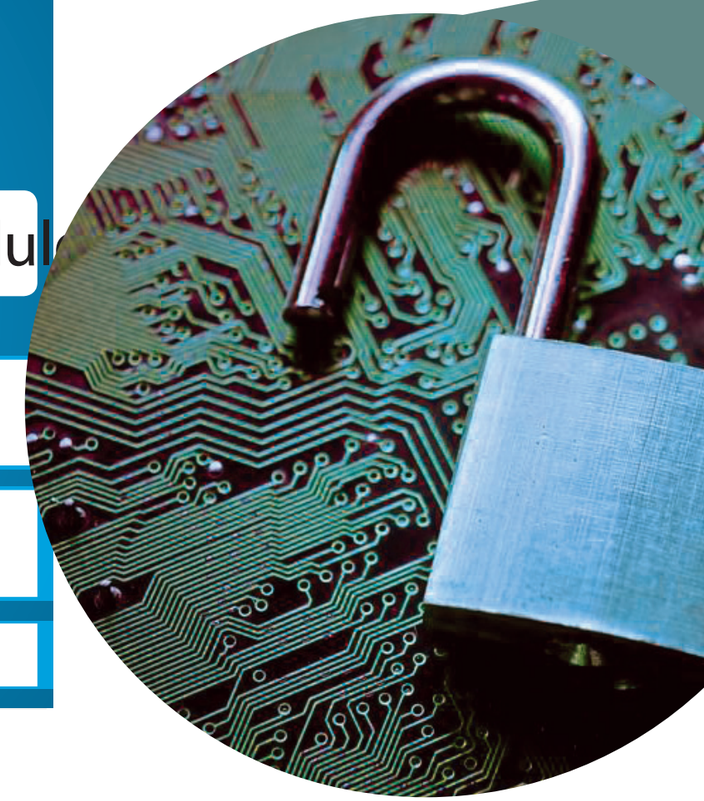
For instance, consider the case involving a large global energy company that was struggling to gain a consolidated view of IT risk across multiple geographic locations. The organization was conducting vulnerability scans on a regular basis, but without a unified view. They adopted NopSec Unified VRM to aggregate the data from various vulnerability testing tools across multiple sources.

Unified VRM Modul

1. Web Application Module: This module helps identify critical vulnerabilities and predict the likelihood of exploitation in Internet-facing applications.

2. External Network Module: This module helps identify critical vulnerabilities across Internet-facing and perimeter networks and gain visibility into external network threats.

3. Internal Network Module: This module helps identify critical vulnerabilities across internal networks.



> Our focus is to help our customers reduce the time between identification and remediation of security vulnerabilities

By having visibility into infrastructure and applications in one place with a risk scorecard that showed the comparative risk across several global locations, the customer saved the expense of deploying IT security teams in each geography, and performed comparative systems evaluation from the corporate head office.

NopSec also provides penetration testing services that simulate real-world attacks to identify weaknesses across IT infrastructure and the areas most open to exploit by hackers. "This offering, along with the Unified VRM platform, are the two key components of our integrated approach to vulnerability risk management," reveals Xu. "This is also a real advantage for NopSec as the insight and knowledge gained from penetration testing is fed back into our expert engine as a way to continuously improve our products."

Unlocking Innovation

"We are passionate about keeping our customers secure, and our team is always curious about innovation and best-of-breed data science practices, which help us lead the competition," adds Xu. NopSec is also working to continuously extend their partner ecosystem, including leading providers of network and application vulnerability scanners and patch management systems. Through direct integration with companies like Qualys, Rapid7, and AlienVault, NopSec brings rich contextual insight to its customers' vulnerability risk management program.

Going forward, NopSec aims to extend their leadership position in the vulnerability risk management space through ongoing enhancement of their data science practice and workflow automation. "Coupled with our data science initiatives, we are expanding our capabilities to automate workflow between Security Teams and IT/DevOps/Developers during the 'Fix' cycle," claims Xu. "Today, NopSec provides a robust, out-of-the-box workflow management system which includes ticketing and dashboards. And as we move further into 2015, we plan to deliver advanced decision support features which will enable customers to close the window of opportunity for hackers faster and with more precision," she explains. CR

CIOReview
The Navigator for Enterprise Solutions
CIOREVIEW.COM MARCH 13 - 2015

20 Most Promising Enterprise Security Companies 2015

Enterprises from all around the globe are dedicating increasing amount of resources and investment on security. Nevertheless, there seems to be no respite in the frequency and sophistication of attacks. Advanced targeted attacks and security vulnerabilities in software are making the matters worse. This is because they are adding to the chaos brought by the disruptiveness of the Nexus of Forces, which brings mobile, cloud, social and Big Data together to deliver new business opportunities. All these factors are forcing CIOs to shell out nearly $76.9 billion on information security, an increase of 8.2 percent from the previous year as per Gartner.

In such a scenario, it is essential for CIOs to fully engage with the latest technology trends if they are to define, achieve and maintain effective security and risk management programs that simultaneously enable business opportunities. Also they need to better understand the security threats by using contextual information and other security intelligence. To help industry leaders accomplish this objective and be successful in their security endeavors, CIO Review presents "20 Most Promising Enterprise Security Companies 2015."

A distinguished panel comprising of CEOs, CIOs, CMOs, VCs, analysts and CIO Review editorial board have selected the list of Top Enterprise Security Companies from over thousand entries. The companies featured here provide a look into how their solutions work in the real world, so that you can gain a comprehensive understanding of what technologies are available, which are right for you, and how they shape up against the competition.

We present to you CIO Review's "20 Most Promising Enterprise Security Companies 2015."

Company:
NopSec

Key Person:
Lisa Xu
CEO

Website:
nopsec.com

Description:
Helping businesses to reduce the risk of cyber attacks with improved detection, analysis, and remediation of IT security vulnerabilities