

# CORE IMPACT CUSTOMER SUCCESS STORY

## SOLUTION SUMMARY

CUSTOMER TYPE | Health Care Services Provider

CHALLENGE | Improving overall security standing and protecting patient data.

SOLUTION | CORE IMPACT Pro, the first comprehensive penetration testing software solution for assessing organizations' most significant IT vulnerabilities and information security threats.

## THE COMPANY



### Visiting Nurse Service of New York

Based in New York City, the Visiting Nurse Service of New York is the largest not-for-profit home health care organization in the country, employing over 10,000 nurses, rehab therapists, home health aides and social workers, as well as operational and business staff.

Founded in the mid-1940s, the medical assistance specialist provides a wide range of in-home services to more than 131,000 patients per year in the New York metro area via over 2 million residential visits. This work includes some \$24 million in charitable care offered to uninsured and underinsured New Yorkers.

As CISO of Visiting Nurse Service of New York (VNSNY), Larry Whiteside Jr. is responsible for overseeing all of the organization's IT security operations, including protection of the company's millions of electronic patient and employee records, and preparation for its mandated compliance audits under regulations such as the federal government's Health Insurance Portability and Accountability Act (HIPAA).

As part of his role, Whiteside is also responsible for selecting the many IT security solutions and services employed by VNSNY to help defend its critical data and operations from potential cyber-threats.

"Health care organizations are getting a lot more attention these days in light of all the ongoing federal activity and as a result have become an even larger focus of the underground. Testing using IMPACT Pro allows us to stay ahead of the curve and ensure we identify problems before anyone else can."

## THE CHALLENGE

With a massive database of sensitive electronic patient and employee information, VNSNY is constantly working to improve its IT security processes to ensure that it can continue to adapt its business to meet the needs of its clients while protecting their personal data and maintaining compliance with complex government and industry regulations including HIPAA.

Among the specific security challenges that the organization faces today is its effort to continue to adopt new technologies including web applications to support its customers and employees, and connect electronically with its many business partners, while preventing any of its critical assets to be compromised through the frequent and persistent cyber-attacks faced by such systems these days.

In addition to its applications security concerns, VNSNY is also focused on keeping its sizable network locked down despite the need to allow many different devices utilized by its diverse, widespread workforce and business partners to connect and gain access to sensitive customer records.

Driven by all of those factors, the organization sought an automated penetration testing solution that would allow it to emulate the same types of hacking and malware threats that its IT systems must withstand in order to identify and prioritize potential weak points, and inform its remediation efforts to best manage related risks.

"Our approach is based on the premise that penetration testing must be a fundamental piece of any mature IT security program, in terms of testing from both the internal and external perspectives," said Whiteside. "It's a critical element of what needs to be done to get to the heart of any vulnerabilities that you might have to eliminate them before they can be compromised."

## THE SOLUTION

To meet its multi-tiered security and compliance requirements and reduce its exposure to potential cyber-attacks, VNSNY opted to license CORE IMPACT Pro to perform regular penetration tests across much of its IT systems and applications. By making penetration testing a central element of its security strategy, including using the product to identify vulnerabilities in its web applications before

they go live, the organization is able to better prioritize its remediation efforts and manage its risk, as well as prepare for internal and external compliance audits.

VNSNY has experienced security staff in-house who previously performed penetration tests in a more manual fashion. By adopting IMPACT Pro, they added a significant level of automation to the process – making it possible to carry out many more tests on a much wider scale and at a faster pace. VNSNY is also using IMPACT Pro to filter through the data provided by its vulnerability scanners to help eliminate false positives and more comprehensively rank results to understand where its most critical points of risk reside.

And as its security programs continue to mature, VNSNY is driving penetration testing deeper into its applications development lifecycle to catch vulnerabilities earlier in the overall process.

"Penetration testing has traditionally been so specialized that if I didn't have someone available who knew how to manually write the scripts and do the command-line work it wasn't easy," said Whiteside. "Having a product like IMPACT Pro in-house allows people who aren't professional penetration testers, but who have an understanding of security, to get the job done and get us where we need to go."

"Much as vulnerability scanners have dramatically simplified that kind of security assessment by automating time consuming work like information gathering, IMPACT Pro is having the same effect on penetration testing. We don't need a genius to do it anymore."

## THE RESULT

### Advancing Web Applications Security

With the proliferation of sophisticated web-based attacks and the high cost of remediating vulnerabilities in customized web applications, eliminating potential security risks earlier in the development lifecycle has become a proven method for saving organizations considerable time and resources.

By incorporating penetration testing into its web applications development efforts using IMPACT Pro, VNSNY is finding that it is identifying and addressing potential problems that would have required attention after taking the systems into production – therein pushing its developers to focus more closely on security issues in general.

"It's a huge step. And while it's something new for a lot of developers to understand, showing them how much easier and cheaper it is to identify vulnerabilities before applications go live, is a pretty powerful message," said Whiteside. "It's also something we're working on with our outside developers and hosting companies. If something is going to maintain data, it absolutely needs to be tested."

### Maximizing Internal Resources

While VNSNY has penetration testing expertise in house, using IMPACT Pro has allowed it to perform far more assessments by arming those workers with the ability to automate many repetitive, time-consuming tasks and by empowering less experienced security staffers to conduct tests without requiring significant training.

By performing assessments across a larger share of its IT systems and applications, and by utilizing penetration testing in cooperation with its vulnerability scans, VNSNY has been able to significantly reduce its overall risk while optimizing internal resources.

### Supporting Internal and External Standards

While penetration testing helps support VNSNY's work to maintain compliance with elements of HIPAA and the PCI Data Security Standard, the company's primary focus in applying penetration testing to the arena of standards is based on its internal mandate to be as proactive as possible in protecting its assets, specifically its sensitive electronic data.

Some organizations may not be as aggressive in advancing their IT security and vulnerability management initiatives, and VNSNY may not yet be compelled to conduct penetration testing in as comprehensive a manner as it does, but Whiteside believes strongly that following the crowd in such matters is the wrong way to approach the issue.

"IMPACT Pro helps with compliance, but it's more about insuring that we are meeting our own requirements, which tend to be far more stringent than any external regulation including HIPAA," Whiteside said. "We certainly look at what others are doing, but when it comes to security architecture we don't want to follow, we want to develop our own mechanisms for evaluation, and lead."