Customer Success Story

The Company
Based in the Midwestern United States, this large personal and family health insurance provider offers programs across 40 U.S. states and the District of Columbia.

Founded in the late 1940s, the company counts more than half of all Fortune 100 companies among its customers via its parent company affiliation – accounting for more than 25 million individual consumers served by 560,000 physicians and care professionals, and 4,800 hospitals nationwide.

The company’s Senior Information Security Architect is responsible for leading operational IT security management including oversight of all server, endpoint and electronic data assets. He is also involved in preparing the company for its mandated external security audits, including those carried out under the Health Insurance Portability and Accountability Act (HIPPA) and Payment Card Industry Data Security Standard (PCI DSS).

Solution Summary

<table>
<thead>
<tr>
<th>CUSTOMER TYPE</th>
<th>National Health Insurance Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHALLENGE</td>
<td>Expanding vulnerability management and addressing compliance requirements</td>
</tr>
<tr>
<td>SOLUTION</td>
<td>CORE Impact® Pro, the first comprehensive penetration testing software solution for assessing organizations’ most significant IT vulnerabilities and information security threats.</td>
</tr>
</tbody>
</table>

“CORE Impact has helped us become a more secure and compliant company without taking up numerous hours and resources. Having an automated penetration testing system in-house is a huge time-saver. Assessments that previously would have taken weeks to perform can now be carried out over only a day or so.”

The Challenge
As a leading provider of health insurance services, the company maintains large volumes of sensitive electronic records. In addition to protecting those valuable assets from potential attacks while fostering close connectivity with its many business partners, the firm must also ensure that it remains compliant with a wide range of mandates aimed at assuring its vigilance in protecting confidential patient information.

“Being an individual health insurance company comes with more responsibility in regards to regulatory compliance than most group health insurance companies,” said the security architect. “Not only are we responsible for being compliant with SOX, HIPAA, and GLBA; we’re also responsible for PCI DSS because we allow our customers to pay their premiums using credit cards.”

While the healthcare provider has some penetration testing expertise on its IT staff, and has traditionally utilized external consulting services for conducting such assessments, the company sought a product that would allow it to perform internal tests more frequently without hiring additional staff or adding costly services engagements.

As the company has already adopted other elements of the vulnerability management lifecycle, including scanning, patch management, IPS/IDS and web applications firewalls, the insurance firm also sought an automated assessment system that would integrate with those tools and allow it to better filter and prioritize the data they produce.

Driven by all those factors, the organization required a penetration testing solution that could be used by its existing IT security staffers on a frequent basis to gauge their exposure to vulnerabilities, test the efficacy of its security management tools and demonstrate compliance with data security standards.

The Solution
To address its expanding security assessment and compliance management needs, the healthcare provider decided to license CORE Impact Pro based on the software’s ability to help the company perform more frequent internal penetration tests without requiring the hiring of additional staff. By bringing pen testing in-house and conducting tests on a far more aggressive (sometimes weekly) basis, the company is now able to isolate critical vulnerabilities faster and better manage its internal vulnerability scanning and patch management programs.
While the company used multiple scanners and an automated patch management system prior to expanding its penetration testing efforts, testing scan results and the efficacy of security remediation work using Impact Pro has allowed the organization to address its most pressing security issues in a far more direct manner.

In addition to its more traditional vulnerability management programs, the company has also made penetration testing of its web applications a more integral element of its overall development process, running the applications through assessments both before and after taking them into production.

“It’s pretty simple: things fall through the cracks and Impact Pro has done a tremendous job of picking up the pieces,” said the security architect. “We’ve used the product to find under-secured assets, support secure applications development, ensure the validity of anti-virus systems and further demonstrate to employees why they need to remain constantly aware of threats. One of the primary benefits of Impact Pro is its ability to address all of these challenges in one package.”

“The most utilized portion of Impact Pro currently is the Network Rapid Penetration Test. Being able to kick things off with a ‘set it and forget it’ mindset has made this tool invaluable. Once Impact Pro has taken a stab at the servers, I then have the ability to pick and choose other modules that I’d like to run, as well as to create my own modules, or even edit what’s already there to tailor it more to our needs.”

The Result

Optimizing Assessment Resources

Prior to buying CORE Impact Pro, the insurance company had relied on external vulnerability assessments performed on an annual basis to attempt to gauge its exposure to electronic attacks, attempted data theft and potential compliance violations. Using CORE Impact, the health insurance firm is now conducting proactive testing of its IT assets against real-world threat simulations to maintain a closer understanding of its overall IT security posture and benchmark changes over time to illustrate progress both internally and with third-party auditors.

“Before Impact, we hired consultants to perform an annual assessment, but after taking a hard look at what was being performed and the results that we were getting, the overall process seemed lacking and I felt that our return on investment wasn’t stellar,” said the security architect. “When you show people that internal penetration testing doesn’t have to be a completely manual process and that solutions have evolved to the extent that consultants use these same products, it’s easy to defend not only how Impact Pro can save the company money and provide more quantifiable results.”

Integrating with Vulnerability Assessment Tools

While the company had already employed vulnerability scanners made by GFI and nCircle to certify the security of its servers, identify potential weak points, and assess changes after significant network alterations, adding the ability to test the results of those systems using Impact Pro enabled the company to better prioritize its potential risks and inform its automated patching and remediation efforts. With fully supported product integrations with a wide array of scanner vendors including GFI and nCircle, and the ability to test the efficacy of its patch management system, the company is now engaging in a more robust overall vulnerability management process.

“Before Impact Pro, we already had a fairly good vulnerability management program in place, but now we have the ability to test how well the overall work is going on a frequent basis to understand where our strengths and challenges lie,” the security architect said. “Since we purchased Impact Pro earlier this year, it’s been used on almost a weekly basis!”

Expanding Web Applications Testing

As part of its internal security program and its efforts to remain compliant with regulations including PCI DSS, the firm was already engaging in efforts aimed at improving the security of its web applications both before and after they went into production. However, by adding CORE Impact to its overall secure applications development lifecycle (SDLC) process, the company is now able to save time and money that would have previously been spent on time-consuming remediation and re-coding, and ensure that its online systems are consistently aligned with its regulatory responsibilities, including the efficacy of its web applications firewalls.

“Today, as new pieces of our various web applications are developed and being made ready to go into production, we’re testing their resiliency with Impact Pro,” said the security architect. “Driving security into the development lifecycle can be challenging, but using the product we’ve been able to show people in our application development department exactly what needs to be remediated.”