CASE STUDY (DIGITAL DEFENSE)

Healthcare Case Study: Austin Travis County Integral Care

Digital Defense Helps Reduce Risk of Data Breach and Realize Cost Savings

DD Service: Vulnerability Lifecycle Management – Pro (VLM-Pro)

Situation Analysis

Austin Travis County Integral Care (ATCIC), like all healthcare organizations, faced a finite budget and needed to protect information with efficiency and best-in-class technology, expertise, and customer support. Any investment it made needed to have a proven track record of return-on-investment and demonstrate cost effectiveness over time.

Challenges

- **Secure Protected Healthcare Information (PHI) as required by HIPAA and HITECH**
  Cyber-attacks are inevitable in all industries but can be incredibly damaging when they impact a healthcare provider. Every organization knows that an information security breach which results in the disclosure of electronic or hard copy PHI will likely lead to both the loss of patient trust and potential fines from federal agencies charged with oversight in the healthcare vertical.
- **Austin Travis County Integral Care Needed a Total Solution**
  Faced with mounting regulatory requirements to protect sensitive and protected information and the fact that a finite number of IT personnel were available to apply towards information security-related activities, ATCIC recognized that licensing a vulnerability scanning tool that they would need to manage and update was not the answer. In evaluating the organization's options, management quickly realized that what was truly needed was a holistic solution that came complete with highly skilled security resources that could ensure that the organization's networks were protected.

AT-A-GLANCE

Austin Travis County Integral Care
This health care provider in Travis County, Texas, serves the citizens of the county with community-based behavioral health and developmental disabilities services.

Austin Travis County Integral Care administers an annual budget of

$57 million of local, state, and federal funding through services at 44 physical facilities. In the last year, it served more than 22,000 individuals and families, offering numerous services and programs year-round.

Services include psychiatric evaluations, 24-hour crisis interventions, medication treatment, inpatient treatment, employment and vocational services, service coordination, family support and respite care, housing, information and referral, supported living and residential services. Integral Care also provides community services in homes, on the streets or at other sites as needed.

Solution

The organization selected managed vulnerability scanning from Digital Defense. The solution, Vulnerability Lifecycle Management – Professional (VLM-Pro), is used to conduct host discovery and vulnerability scans on external (internet facing) and internal IP-based systems and networks. DD employs a variety of proprietary scanning techniques to survey the security posture of the target IP-based systems and networks. These scans proactively test for known vulnerabilities and the existence of mainstream industry best-practice security configurations.

The VLM-Pro service also provides workflow management, host-based risk assignments, and remediation progress reporting. In addition, VLM-Pro includes professional, dedicated assistance with configuring and maintaining scan profiles as well as project management of the client's remediation efforts (regardless of whether they are handled by the client's IT staff or a 3rd party provider).

Further, DD assigns each VLM-Pro client a Personal Security Analyst (PSA) who serves as the client's primary point of contact for more involved, technical questions. The PSA provides the client clear, consistent security consulting advice on their vulnerability lifecycle management program.

Results

ATCIC now experiences assurance and peace of mind, knowing that DD's managed VLM-Pro is reducing the risk of cyber-attack in a cost efficient manner. VLM-Pro has given ATCIC freedom from the day-to-day oversight of its security program and benefits from:

- **Reduced Risk Through Improved Security GPA** – In only four months, ATCIC's enterprise Security GPA, which is a combination of their internal and external hosts, has improved 33%from 2.57 (C+) to 3.41 (B+). It's important to note that companies often neglect the importance of their internal devices, which pose a significant risk. The best approach for a higher total GPA is enterprise-wide scanning as opposed to ad hoc scanning of a subset of devices. Security GPA, developed by DD, is a rating of security posture that reflects business risk and improvements made to the security of clients' networks over time. ATCIC can compare its Security GPA rating to its peer organizations.
- **Improved Return on Investments and Reduced Total Cost of Ownership** – With no hardware or software to purchase and maintain, nor license fees to pay, ATCIC requires significantly fewer trained and dedicated IT resources compared to traditional premise-based tool deployments. Not only is the cloud-based service more cost effective, it helps reduce the carbon footprint of their data center.

  ATCIC's savings can be demon-strated in terms of total cost of ownership (TCO) and return on investment (ROI). Its network is represented by the calculations for a typical network with up to 250 IP devices.

> *"The DD VLM-Pro solution has made a real difference for us at Austin Travis County Integral Care. The assistance provided by our DD PSA ensures that our IT teams can focus on those vulnerabilities that present the most threat to our critical IT assets. Additionally, Security GPA® makes it easy to report on the progress we continue to make in securing our networks and protecting our patient's healthcare information."*
>
> – David Evans, Chief Executive Officer

Total Cost of Ownership – Premise vs. Cloud-based

TCO takes into account computer and hardware programs and operational expenses and compares them for both cloud-based and premise-based systems. ATCIC's network is in the <250 IP device size. Clearly, the cloud-based service is less than half the cost of a premise system.

Up to 250 IP Device Network	Year 1	Year 2	Year 3	3-Year Total
Premise-based Service	$26,465	$25,592	$26,938	$78,995
DD Cloud-based Service	$13,495	$12,480	$12,711	$38,686
3-Year Savings				**$40,309**
3-Year Savings as Percentage				**51%**

Return on Investment

The ROI of an information and network security program designed to identify and mitigate risk is measured in reducing its risk of a data breach. The value of DD's cloud-based service is a very small expense when compared to the potential cost of a breach. The ROI for ATCIC is based on the following assumptions:

- ATCIC serves approximately 22,000 patients each year, whose records are potentially at risk
- Cost of a data breach is $194 per capita[1]
- One data breach could potentially compromise the personal and protected information of their 22,000 patients
- ATCIC's annual budget is $57 million

The table below shows a potential cost of a data breach of all their patient records if one should occur.

Client Records Potentially at Risk	Breach Average Cost One Year	Potential Cost of Breach as Portion of Total Operating Budget
22,000	**$4,268,000**	**7.5%**

[1] 2011 Cost of Data Breach Study: United States, Ponemon Institute, March 2012, sponsored by Symantec.

- **24 x 7 Customer Support and Workflow Management** – ATCIC's PSA manages the end-to-end service delivery that includes customized reporting of assessment and remediation efforts. In addition, ATCIC can view its progress through an intuitive online dashboard, Frontline™ Solutions Platform. The PSA can respond quickly to any enterprise-wide issue that ATCIC may encounter.

- **Best-in-Class Expertise** – DD's Vulnerability Research Team proactively mines our Frontline Solutions Platform database to accelerate the discovery of instances of flaws then analyzes these flaws for rapid identification of Zero Day vulnerabilities, further bolstering security.

- **Reduced Scan Times** – DD's patent-pending NIRV Scanning Engine has reduced the organization's scan times by almost 80%. This allows DD to respond quickly to any enterprise-wide security threat

At the time of this case study, Fortra VM and its corresponding security solutions were referred to under the Frontline brand.

FORTRA®

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.