CASE STUDY

tenable volpara health technologies

Tenable Helps Volpara Shift Left and Secure Its Azure DevOps Pipeline

> *“We selected Tenable for its ease of use, automation capabilities, expertise and brand recognition. The ability to automatically assess each new container image and to continuously protect the image as new vulnerabilities are discovered is invaluable. We now have unmatched visibility into the security of our CI/CD pipeline and running containers, allowing us to focus on what matters most: saving lives.”*
>
> **GARETH BEAUMONT**
> CIO & CISO

ORGANIZATION SNAPSHOT

COMPANY
Volpara Health Technologies

FOUNDED
2009

GLOBAL REACH
38 countries

NUMBER OF WOMEN SERVED
10 million in the U.S. alone

INDUSTRY
Medical Technology

CHALLENGES

- Protect a 100% cloud-native attack surface comprised of Azure services, Docker containers and IoT devices
- Identify a single platform for securing all assets
- Keep pace with the speed of change in DevOps
- Deliver on ISO13485 and ISO27001 compliance requirements

SOLUTION

tenable.io Container Security

RESULTS

- Unmatched visibility into the security of the CI/CD pipeline
- Increased efficiency and effectiveness with automated security monitoring
- Increased efficiency in reporting on Docker container assets with user-friendly, easy-to-consume reports
- Operate at the speed of DevOps by shifting left
- Effectively meet ISO13485 and ISO27001 compliance requirements

VOLPARA HEALTH TECHNOLOGIES

Volpara Health Technologies is a medical technology company dedicated to the early detection of breast cancer. It uses artificial intelligence (AI) to produce a complete set of digital health services that provide the accumulated data for predictive risk models ultimately aimed at prevention. The protection of this data is of paramount concern to Volpara.

CHALLENGES

Gareth Beaumont, Chief Information Officer and Chief Information Security Officer, and his team needed a single platform they could use to secure the organization's rapidly evolving and complex cloud-only infrastructure. Among the challenges they needed to address were:

- **Protect a 100% cloud-native attack surface comprised of Azure services, Docker containers and IoT devices**
  Volpara is operating 100 percent in the cloud. All of its information systems and data are running on Microsoft Azure, with no production systems on premises. "As such, our ability to demonstrate active and sound security measures in the cloud is paramount," says Beaumont.

  Volpara also recently launched an IoT product that includes a hardware appliance consisting of an Intel NUC, operating system, Docker containers and an application which sends data to be analyzed in the cloud. Given the sensitivity of the medical data being uploaded and analyzed, this IoT device requires an automated cyber risk solution to discover Docker container images and integrate security into the DevOps pipeline.

  Beaumont says, "Quantifying and regressively testing the web as well as IoT solutions was labor intensive and required an automated solution. With human involvement there is an increased chance of error and oversight."

- **Identify a single platform for securing all assets**
  As a strong advocate of standardization, Beaumont and his team were in need of a single platform to secure the entire attack surface, versus a plethora of separate tools for different assets.

  In the rapidly changing environment, Volpara requires a comprehensive unified view into the security of its containers and web applications across a very dynamic attack surface.

- **Keep pace with the speed of change in DevOps**
  The cybersecurity team at Volpara needs to keep pace with the rapid adoption of DevOps and new IoT solutions. The team needs to effectively monitor the frequent updates and constant revisions to the code as a way to do rapid automated development. Additionally, the team must ensure the security of Docker images as new vulnerabilities are discovered each week.

  To help secure containers and other short-lived assets, the team needed to shift vulnerability assessments to the left and into the development process.

- **Deliver on ISO13485 and ISO27001 compliance requirements**
  To ensure the highest level of security and increase customer confidence, Volpara is both ISO13485 (Quality Assurance) and ISO27001 (Information Security) certified. This requires continuous cyber risk management and turnkey reporting to help demonstrate compliance.

SOLUTION

After considering several solutions, Volpara Health Technologies selected Tenable as its vulnerability management partner for several reasons:

- **Expertise and brand reputation**
  Beaumont says he chose Tenable because of its brand reputation and expertise in vulnerability management. He is able to leverage Tenable's expertise in identifying ever-changing vulnerabilities and threats while its automation enables him to save on overhead and IT staff resources.

  The cybersecurity team ran three Proof of Concept (PoC) trials for its application testing functionality. Based on the results, and the ease with which Tenable.io Container Security integrated into the CI/CD pipeline, the team decided to invest in Tenable as its strategic vulnerability management partner.

- **A single platform for securing cloud services, web applications, and Docker containers**
  Tenable's industry-leading Cyber Exposure platform provides Beaumont and his team a complete picture of its cyber risk. They have a unified view of their Cyber Exposure, not siloed visibility caused by using separate tools for different assets.

- **Seamless integration into the CI/CD pipeline**
  Tenable.io Container Security seamlessly integrates security testing into Volpara's DevOps pipeline without sacrificing velocity. The product easily integrates with the company's CI/CD tools, like Microsoft DevOps services and Octopus Deploy so that as new container image builds are created they are assessed for vulnerability risks and malware.

- **Complete visibility into the security of Docker containers from development through operations**
  Beaumont needed assurance that the company's containers were secure before and after release into production. With Tenable.io Container Security, security became a crucial quality-control test in the development process, and the security posture of running containers could be monitored to detect issues in operations.

RESULTS

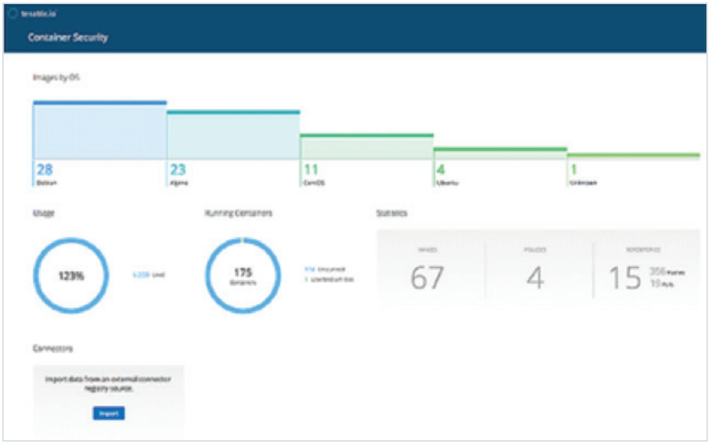
- **Unmatched visibility into the security posture of the CI/CD pipeline**
  Tenable products provide Beaumont and his team complete visibility across the entire attack surface, with security effectively integrated into the CI/CD pipeline to prevent vulnerabilities and malware from being exploited in production.

  Beaumont says, "Tenable was PoC tested, purchased and integrated into our existing systems and processes. Success doesn't get easier."

  Additionally, Tenable's solutions give the organization the ability to internally test its LAN, which has proven invaluable, as it revealed several vulnerabilities related to old desktop PCs and personal usage devices. While plans were already in place to mitigate these devices on the network, vulnerability testing results provided quantifiable evidence to speed up this process.

- **Increased efficiency and effectiveness with automated security monitoring**
  The ability to automate its vulnerability management has allowed Volpara to perform weekly tests versus quarterly tests. This significantly increases the efficiency of staff resources and provides the security team peace of mind knowing they are effectively monitoring all their assets and systems.

- **Increased efficiency in reporting on Docker container assets with user-friendly, easy to consume reports**
  The security team now has complete visibility into the container environment —including images, policies and repositories — with easy-to-consume reports in a variety of formats, including json and html. In addition to helping monitor assets, the reports are used by Beaumont to update leadership in executive meetings.



Illustrative Data:
Tenable.io Container Security provides "at-a-glance" visibility into the container environment, including images, policies, repositories and key operational information.

- **Operate at the speed of DevOps by shifting left**
  Volpara is now able to reduce its Cyber Exposure gap by integrating security into the software development lifecycle (SDLC). By shifting left, the security team is operating at the speed of DevOps and ensuring end-to-end protection of its entire attack surface.

- **Effectively meet ISO13485 and ISO27001 compliance requirements**
  Beaumont and his team are now able to effectively deliver on compliance initiatives using Tenable's solutions. They are able to assure their customers they are meeting the highest level of security standards and effectively managing their cyber risk.

CONCLUSION

With Tenable as its strategic vulnerability management partner, Volpara Health Technologies has complete visibility across its entire threat landscape, including cloud services, web applications and Docker containers.

The innovative cybersecurity team has shifted left, integrating security into the CI/CD pipeline, and is operating at the speed of DevOps.

“We selected Tenable for its ease of use, automation capabilities, expertise and brand reputation,” says Beaumont. “The ability to automatically assess each new container image once it’s created and continuously protect the image as new vulnerabilities are discovered is invaluable. We now have unmatched visibility into the security posture of our CI/CD pipeline and running containers, allowing us to focus on what matters most: saving lives.”

To learn more visit tenable.com/products/tenable-io/container-security | Contact Us: marketing@tenable.com