tenable

A Government Health Agency Trusts Tenable to Protect Patient Data and Manage Expanding Attack Surface

> *"The level of visibility Tenable.io provides is phenomenal, something we just never had before... what we've been able to do with the data following that is just brilliant."*
>
> Cybersecurity Manager

ORGANIZATION SNAPSHOT

COMPANY
A Government Health Agency

NUMBER OF HOSPITALS
150+

NUMBER OF EMPLOYEES
125,000+

INDUSTRY
Healthcare, Government

CHALLENGES

- Reduce cyber risk across expansive network of hospitals
- Deliver sector-wide, advanced reporting on cyber risk to executives
- Easily roll out a comprehensive solution to 25 IT teams
- Simplify and streamline incident response process
- Provide non-intrusive monitoring of critical IoT assets

SOLUTION

tenable.io

Tenable.io with Nessus Network Monitor

RESULTS

- Peace of mind with improved visibility across an extended network
- A comprehensive, organization-wide view of cyber risk with actionable dashboards
- Increased efficiency, eliminated use of spreadsheets
- Helped deliver on organization's mission to improve patient care

A GOVERNMENT HEALTH AGENCY

As the government health agency digitally transforms healthcare – using data and technology to improve and streamline patient care – the number of cyber threats has increased exponentially. The cybersecurity team led by the manager of cybersecurity, must manage, measure and reduce risk across an expansive network of 150+ hospitals with 125,000+ staff and over 25 different IT teams.

Due to the personally identifiable information (PII) the hospitals manage, including patient data and sensitive health records, they are an attractive potential target for cyber criminals. With patient lives at stake, it is critical the hospitals quickly identify their exposures and meet the highest level of security standards.

.

CHALLENGES

The government health agency must monitor and measure cyber risk across a large network of hospital services, including both metro and rural hospitals. The cybersecurity teams require a leading-edge, organization-wide solution to address the following challenges:

- **Understand and reduce exposures in each of their hospitals**
  With several high-profile security incidents in the healthcare sector, along with increasing ransomware and phishing attacks, the agency requires a comprehensive solution to provide full visibility into their security posture across thousands of legacy and modern assets.

  The cybersecurity manager says, "We have a very large attack surface. The digitization of healthcare increases risk – as you collect, store and process more data, you must continue to raise the bar on security standards and performance to mitigate risk."

  As part of the organization's security strategy, the team has introduced a statewide framework requiring each of the hospital services to quickly identify and mitigate exposures to meet statewide KPIs.

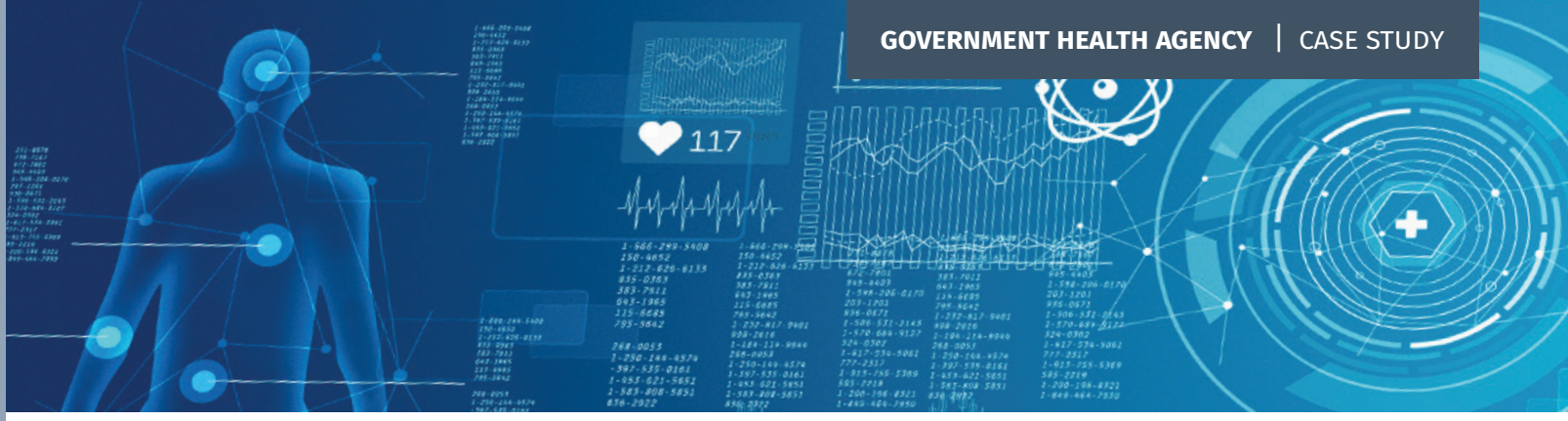
- **Deliver accurate numbers to their c-suite and executive team**
  The team needs ongoing visibility into the security posture of each hospital to ensure they are quickly mitigating risks as well as analyzing and benchmarking performance to share best practices across their network.

  They need an actionable, comprehensive dashboard that delivers accurate numbers to their c-suite and executive team.

- **Ensure adoption with a solution that is easy to use and implement**
  The agency requires an easy-to-use platform that is simple to implement and roll out to each hospital. With over 25 teams using it across the sector, the system must be intuitive and provide immediate value.

- **Simplify incident response process**
  The agency also requires a more streamlined incident management process to efficiently reach across all their hospitals. If an exploit occurs, they do not want to rely on sending out an agency-wide email and pulling together responses into a spreadsheet.

- **A non-intrusive way to monitor IoT biomedical devices**
  The adoption of IoT biomedical devices — from infusion pumps to cardiac pacemakers to robotic carts — has increased hospital efficiency and improved patient care. But, device vendors do not always allow patching or enable organizations to scan or put an agent on them. The agency needed a non-intrusive approach to safely monitor these devices and quickly identify vulnerabilities.



SOLUTION

After evaluating several vulnerability management vendors including Rapid7 and Qualys, they chose the cloud-based Tenable.io due to the following reasons:

- **Continuous, accurate visibility with comprehensive assessment**
  Utilizing Nessus® scanners for vulnerability assessment, combined with the centralized management capabilities of Tenable.io, the agency gained unparalleled visibility into its IT infrastructure, including legacy and modern assets that were once blind spots.

- **Actionable dashboards to identify, prioritize and manage risks**
  Tenable.io's actionable dashboards give the agency the data they need to identify and prioritize risks. Additionally, the cybersecurity manager can now benchmark remediation of vulnerabilities between IT teams. The cybersecurity team is able to analyze the data and lessons learned, and share best practices across their network of hospitals.

  "With Tenable.io, we're able to confidently analyze, report and reduce our level of exposure across the hundreds of thousands of assets we manage every day. This ensures we can properly brief leadership with actionable insight and recommendations on how best to reduce our cyber risk and protect our patients," says the cybersecurity manager.

- **Turn-key implementation**
  Due to the cloud-based design and ease-of-implementation of Tenable.io, the agency was able to successfully deploy a statewide solution across over 150 hospitals in two months. The cybersecurity manager mentions, "I don't think this broad implementation has been done in the government before. The team at Tenable and the professional services group were very flexible and the training for our hospitals was simple."

- **Continuous monitoring of critical IoT assets with passive network monitoring**
  The agency can now continuously monitor IoT assets and systems with Nessus Network Monitor in Tenable.io. This enables the critical devices to be available 24/7 and not be taken offline when lives are on the line. The hospitals can safely monitor these devices and quickly identify vulnerabilities and implement controls where needed.

IMPACT

- **Peace of mind with improved visibility and significant risk reduction**
  With Tenable.io as their enterprise Cyber Exposure platform, the agency is assured they have eliminated blind spots and have continuous visibility across all their assets.

  Comprehensive coverage of both traditional and IoT assets significantly reduces their cyber risk and enables the team to continually understand their exposure. They can also establish best practices to mitigate future cyber risks.

- **A consolidated view of risks**
  The security team now has a centralized view of their overall risk and Cyber Exposure. Their manager says, "We have never had this level of data before. In the past, we would rely on phone calls to over 25 different organizations to provide us with the information we need and assemble this together. Now, we have access to actionable, consolidated data to provide to our leadership team, so it's been fantastic."

- **Improved efficiency**
  Actionable dashboards provide the team the consolidated view of risk they require. They no longer need to manually collect data across their network or use spreadsheets to summarize their efforts. In addition, the team saves time with a streamlined incident management process. In short, Tenable.io significantly improves the team's efficiency.

- **Help the organization deliver on business goals**
  By reducing cyber risk, the security team actively participates in the organization's mission of improving healthcare outcomes.

CONCLUSION

With Tenable as their strategic partner, the government health agency is able to accurately identify and manage risks across their expansive network, have a consolidated view of their program to share with leadership, and help the organization deliver on business goals. They have a comprehensive vulnerability management solution in place which they can build on as their IT infrastructure and attack surface evolves.

The cybersecurity manager concludes, "The level of visibility Tenable.io has provided has just been phenomenal, something we just never had before...what we've been able to do with the data following that, is just brilliant."

The agency is enthusiastic about Tenable's vision for the future and its road map. Advanced benchmarking and predictive prioritization capabilities will offer new benefits to the organization's security strategy.

To learn more visit tenable.com | Contact Us: marketing@tenable.com

tenable®

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 25 percent of the Global 2000 and large government agencies. Learn more at **www.tenable.com**.