CASE STUDY

tenable

State Government Agency Turns to Tenable to Protect Valuable Taxpayer Data and Deliver on Compliance Requirements

> *"[Tenable.sc] has cut our team member's workload by approximately half – freeing up badly needed resources for other critical tasks."*
>
> **CISO**
> U.S. State Government Agency

ORGANIZATION SNAPSHOT

CHALLENGES

- Safeguard the personally identifiable information (PII) of millions of taxpayers
- Maintain compliance with increasingly stringent regulatory standards, including mandated security audits
- Must rely on resource intensive, manual processes for monitoring vulnerabilities
- Manage an increase in phishing attempts and other cyber attacks
- Increasingly distributed workforce across multiple states

SOLUTION

tenable.sc™
Continuous View

RESULTS

- Improved visibility and patch prioritization – reducing phishing attempts by 90% and doubling staff productivity
- Increase in business unit efficiency with reduction in downtime
- Peace of mind knowing all the assets are being scanned and monitored in real-time
- Saved IT staff time and improved decision making with turnkey reports
- Increased efficiency in meeting compliance mandates

A U.S. STATE GOVERNMENT AGENCY

A U.S. state government agency must safeguard the personal data of millions of taxpayers including a tremendous volume of motor vehicle records. The agency also enforces alcohol and tobacco regulations, and conducts IT forensics for the special investigations of the level agency. Given the valuable and sensitive information the agency stores, it's critical that they stay a step ahead of emerging threats to reduce their cyber risk, and at the same time, maintain compliance with the increasingly stringent regulatory standards including the IRS 1075 based on NIST 800-53.

INTRODUCTION

The InfoSec team is focused on providing end-to-end protection of customer data and confidential information. As new cyber risks emerge daily and regulatory pressures constantly evolve, the agency must work hard to ensure their network remains protected and compliant. Their CISO explains, "This is a 24X7 job, as cyber criminals innovate and persist." Taxpayers depend on the agency to keep their personal information safe. As the agency is an attractive target for cyberattackers, they must continuously monitor their assets and environment to protect their critical data and maintain public trust.

CHALLENGES

The agency needed a Vulnerability Management solution to address several challenges:

- **The agency was monitoring their networks for vulnerabilities and compliance manually.**
  This was a time consuming process for both the IRS Safeguard auditors and agency staff. The agency was only able to conduct scans periodically, leaving gaps in coverage of their attack surface.

- **Due to the confidential nature of their data, the agency had recently seen an increase in phishing attempts, complicated by a move to Office 365.**
  "It was not uncommon to see 10 to 15 attacks a day," says their CISO. "Every hit required that the impacted machine be removed from the network and remediated by the InfoSec team. This would tie up an IT resource for the day, and result in downtime for the impacted staff member who had to wait until the machine was cleaned."

- **The boundary of the organization's work environment had expanded.**
  The agency's workforce had become increasingly distributed with auditors working in multiple locations across the U.S. The growing use of laptops and mobile devices presented visibility and security challenges.

The agency needed a Vulnerability Management solution that provided continuous visibility into the security posture of their network, and delivered a turn-key compliance solution to meet critical regulatory requirements and reduce cyber risk.

SOLUTION

To improve their security posture and ensure regulatory compliance, the agency selected Tenable.sc Continuous View.

When looking at the solutions on the market, Tenable stood out for a variety of reasons. “When selecting a new solution, I value the feedback of my peers,” says the CISO. He indicates other CISO’s he’s talked with also use Tenable. “I don’t think you have any competition, to be honest with you,” he says.

Tenable.sc provides the agency with a Vulnerability Management platform that includes:

- **Better visibility into cyber risk and faster detection of threats, including phishing attempts.** The InfoSec team can now continuously monitor their network to get a real-time, holistic view of assets, network activity and events to expedite discovery and remediation of vulnerabilities.

  Using Tenable.sc , the agency’s security team discovered that many of the phishing attempts were originating from machines with unpatched McAfee Antivirus engines. The team can now immediately identify the machines that need patches and can work with their service provider to prioritize patching before an issue occurs.

- **Intuitive dashboards and reporting for communicating cyber risk and compliance.** The agency is able to leverage pre-built and customizable dashboards. The CISO says “It really is an easy tool to use. My staff has mentioned this, and from my perspective, the dashboards are easy to understand. I don’t need to take a lot of time explaining them, they just make sense.”

- **Turn-key workflows and process for NIST-800-53 and IRS 1075 compliance.** Tenable.sc’s predefined checks help the team ensure they’re aligned with the IRS SafeGuard requirements. Now the auditors simply plug into the network and a run a report from Tenable.sc to demonstrate compliance posture.

- **Coverage of a broad range of assets across an increasingly distributed enterprise.** Not only is the team able to get ahead of vulnerability threats across traditional assets such as desktops and servers – Tenable.sc Continuous View’s agent-based scanning also enables the agency to cover hard to scan assets like endpoints and other transient devices.

- **Proactive, continuous monitoring that simplifies patch management and prioritization.** The InfoSec team is alerted to machines to patch and has peace of mind knowing their assets are being scanned in real-time. If there’s a system that needs to be patched, they’re notified immediately.

- **Responsive customer support.** The team is happy with the support they have received. Their CISO mentions, “Customer support has been very, very good.”

RESULTS & ROI

- **Improved visibility and patch prioritization – reducing phishing attempts by 90% and doubling staff productivity**
  With Tenable.sc, visibility into vulnerabilities significantly increased and the team was able to prioritize patching. The CISO explains that with Tenable.sc, "the number of phishing attempts has dropped from 10 to 15 per day to 1 per day – or often times to zero a day. This has had a huge impact on the productivity and efficiency of our organization. It has cut our team member's workload by approximately half – freeing up badly needed resources for other critical tasks. It has greatly improved the productivity and efficiency of our department. It has also helped my business directors substantially by eliminating downtime and increasing the output of their staff."

- **Increased business unit productivity**
  The business directors are seeing fewer workers impacted by cyber attacks and less downtime. They appreciate the improved productivity and clearly see the ROI of Tenable.sc.

- **Peace of mind**
  The InfoSec team has increased confidence knowing all their assets are being scanned and monitored in real-time.

- **Time savings**
  Tenable.sc's turnkey reports have made decision making and internal updates significantly easier, saving IT staff time.

- **Efficiency in meeting compliance mandates**
  The team feels much more prepared for the IRS 1075 compliance process and audit meetings with a more automated approach. The reports and dashboards in Tenable.sc have made life much easier for both the auditors and their team.

This reduction in IT staff workload, improved business unit productivity and increase in efficiency in meeting compliance requirements has delivered tremendous ROI for the agency.

With Tenable as their strategic vulnerability management partner, the agency is able to monitor an ever-changing attack surface, identify new assets and vulnerabilities in real time and effectively manage compliance requirements while optimizing budget.

Interested in more information about how Tenable can help state and local government agencies meet IRS 1075 (FTI) and CJIS regulatory requirements?

Visit **tenable.com/cjis-fti** to download a complimentary white paper or contact **marketing@tenable.com**.