State Health Department Minimizes Ransomware Risk with Server Workload Hardening

The State of Hawaii is ranked 40th in population, but due to its geographic location, it attracts an extremely high number of tourists from the rest of the US and around the globe. In 2023 alone, US tourist visits were up 29%. These numbers mean that the Hawaii Department of Health serves over 1.4 million residents and 6 million visitors each year.

As a state agency and health-related services organization, the Hawaii Department of Health is one of thousands of similar agencies whose operating systems and applications run on legacy IT Windows servers. This leaves the department vulnerable to ransomware and other cyber attacks from bad actors, including nation-state threats. The department maintains a small core IT team, making it challenging to stay on top of alerts and effectively stop attacks.

The U.S. Department of Health and Human Services (HHS) referred Virsec in 2020, and the Hawaii Department of Health has been a loyal customer, renewing several times since.

The Virsec Security Platform (VSP) provides Zero Trust Runtime Defense with a 'default-deny, allow-on-trust' approach, which instantly stops any deviations from trusted processes, files, and scripts. This means that the Hawaii Department of Health servers are protected against ransomware and other known and unknown cyber attacks, even those EDRs miss. The platform provides the strongest legacy IT protection possible, as demonstrated by AttackIQ testing prior to deployment.

> *"The Virsec team has been so flexible working with our IT staff, helping us analyze threats with alert snapshots. The Virsec Security Platform's UI is extremely user-friendly. A lot of stress has been taken off my shoulders because Virsec was there to protect our servers. This has given me peace of mind and allowed me and our staff to focus on other priorities."*

~ Lyle Maesaka, System Analyst | Disease Outbreak Control Division
Hawaii State Department of Health | Ka 'Oihana Olakino

virsec™ Visibility and Runtime Protection for Cloud and Legacy Server Workloads

To learn more about the Virsec Security Platform and to find out how to start protecting your mission-critical server workloads, visit us at **www.virsec.com**

Virsec Customer Success Profile

Industry
State and Local Government

Key Challenges

- Small IT team with limited resources to manage alerts and constantly patch vulnerabilities.
- Installed EDR didn't effectively protect against memory attacks and signaled a high rate of false positives.
- Existing security tools on the servers didn't catch critical vulnerabilities, leaving them vulnerable to exploits.
- Increased risk of ransomware, with more than three-quarters of attacks targeting state and local government, and most of those stemming from exploited vulnerabilities.

Business Outcomes

- Closed the EDR vulnerability gap, with minimal CPU usage.
- Strengthened security posture by implementing a defense-in-depth strategy.
- Team morale improved, knowing they can sleep at night, and worry less about their server security.
- Drastically reduced the number of false positives, allowing them to prioritize other IT initiatives without the distraction of constantly panic patching, even with a small team.
- Positive business outcomes mean that the Virsec contract was renewed through 2026 for seamless protection over the next 2 budget years.