



A United States Government Case Study

Mission:

In 2007 the United States embarked on a Comprehensive National Cyber Initiative (CNCI). One major component of this program is the Trusted Internet Connection (TIC), dictated in OMB memorandum M-08-05 of November of 2007, specifically designed to improve the security of Federal agency networks.

TIC reduces the risk to government data by consolidating the number of internet connection points, establishing common security controls across the agency and departmental levels, and providing adequate monitoring capabilities into traffic – thus improving incident response capabilities.

An aggressive implementation timeline for TIC put pressure on executive branch agencies to move quickly. Our client, a large department, was given only three months to complete the tasks of documenting existing network connections across all offices, assessing technical architecture plans and security policies and creating a plan of action with milestones for TIC implementation by the June 2008 deadline. The department also used the TIC consolidation project to develop a centralized Security Operations Center (SOC) to deliver a consistent level and quality of security monitoring across the components.

“We had to look seriously at our security strategy and find the best combination of next generation monitoring technologies that would enable us to implement an efficient TIC architecture, but longer term also address advanced threats and implement better processes to make our operations staff more efficient,” said the agency-level deputy CISO.



Evaluating NetWitness

Due to its critical role in the national security infrastructure, the department was under constant attack from a wide variety of threats ranging from script kiddies to state-sponsored entities, criminal organizations and political activists. Thanks to years of hardening by the dedicated staff and a wide variety of technologies, the agency was effectively fending off most intrusion attempts. The detection and mitigation of advanced persistent threats remained a serious challenge. The department had to address this gap through increased network visibility and improved threat intelligence simultaneous with the consolidation into a TIC architecture. Integrating a network security monitoring and analysis solution to compliment existing IDS and security event and information management (SEIM) technologies was considered critical to provide a much deeper level of analysis and incident response capabilities. The security and architecture teams collaborated with peers across other government agencies. The CISO of an intelligence agency recommended NetWitness NextGen, a technology used successfully for similar problems for a number of years.

“My peer was raving about NextGen and of the breadth and depth of full visibility into network, application and user context and content,” said the department’s CISO. “Given the complexity of our environment, we were somewhat skeptical going into the evaluation process, but a brief evaluation of the solution quickly made it compelling.”

NetWitness NextGen is a network security monitoring solution that was explicitly designed to help combat advanced cyber security threats. The solution is based on full packet capture and session analysis. It utilizes the most comprehensive and advanced network session modeling techniques to provide very specific and granular security analytics into terabytes of data. Using SIEMLink, the department leveraged NextGen’s application layer insights and intelligence to augment existing security countermeasures and accelerate operational security processes. The resulting workflow acted as a force multiplier to improve the security team’s efficiency and effectiveness.

Instant Success

The initial NetWitness deployment began with a two week proof of concept. The department deployed NetWitness NextGen appliances on their production network, emulating where these appliances would reside in their TIC configuration, with full access to production data. Both government and contractor support teams worked closely with NetWitness engineers, comprised of cleared professionals that have spent decades working at the forefront of IT security. Within just two weeks of active testing, the agency was able to uncover both a potentially serious external data breach and an employee created data leakage incident. Both of these incidents were overlooked by the agency’s existing security technologies and were deemed critical incidents by the department’s leadership.

An Evolutionary Engagement

The initial purchase and phase I deployment went very well. A close working relationship between NetWitness staff and the TIC project team resulted in a virtually error free implementation, and significant operational improvements within the department’s security operations and threat analysis teams. Based on the early success of the project, the client has officially launched its centralized SOC strategy – delivering centralized event analysis, incident coordination, response and reporting for its components. According to one of the government senior engineers, “On a consistent basis over 60% of our confirmed kills are now attributed to data we obtain from our NextGen infrastructure versus the combination of other technologies we have deployed and use.”

Get in the Know.

NetWitness NextGen is not for everyone. The threats facing our customers are advanced and our customers are very demanding. They are security experts with years of experience and a refined sense for the challenges facing their organization. NetWitness excels at working with this savvy base of users, whose workload and requirements push the limits of any platform. Our discerning customers are provided unprecedented access to technical support, our product and development staff and our executive leadership. Our fanatical focus on this advanced user based, coupled with our extensive knowledge of advanced threats resulted in the department taking full advantage of the power of our solution from day one. Since our initial success together, their appetite for visibility has only expanded, with additional deployments into the corporate environment

NetWitness helps clients combat advanced cyber-security threats by giving them an unprecedented level of knowledge into what is happening across their networks, and providing them the insight needed to take definitive action. The NetWitness NextGen security monitoring solution has received numerous awards for its innovation and has become a critically important part of our clients’ day to day operations. It is this intersection of rich application data and context that differentiates the patented NetWitness® products from any other solution available in the market.

