

SPOCK REPORT HIGHLIGHTS



Prior to the full commercial release of the HYDRA network security platform, Sentinel Security Corporation successfully demonstrated their most audacious security claims to several commercial interests and government agencies through the DoD's Security Proof of Concept (SPOCK) program. These claims included:

- Resistance to all network-based attacks, including viruses and worms, penetration attacks, DoS attacks, and attempts at content modification.
- Secure content control through single sign-on and other user-to-user separation features.
- Simple configuration, requiring only minutes, is hardened out of the box.
- Simple administration, including automatic disaster recovery features.

The resulting report demonstrated NSA V2's cooperation with industry and government system integrators to jointly verify the security-related functions of HYDRA. This document includes a few key excerpts from the report that emphasize the success of the demonstration. The full report is available as a controlled document upon request from Sentinel Security Corporation.

“This product represents a true paradigm shift in Server technology. It is a ground up design using security as the paramount concern.”

“Our conclusion, based on comments made by the participants during this exercise, is a clear positive response.”

“This solution provides the capability to host complete Web Services and process transactions more securely than other Web Servers because it does not rely on a traditional OS/Applications architecture to execute it's responsibilities. It represents a new class of Hardware/Software that is especially designed to take maximum advantage of embedded technology.”

“The developer's design approach eliminates the need for periodic patching, security upgrades, etc.. Specifically, the solution has been designed from the 'Ground Up', including only features which support a heightened security environment. This translates to ease of configuration, reduced skill sets to administer, etc.”

“We found indications that the traditional patches required to 'beef up' Server Operating Systems to respond to vulnerabilities may never be necessary with this type of design.”

“The participants used vendor supplied test scripts to configure the HYDRA, recording the actual time to completion. The actual configuration took *two minutes*.”



4401 Ford Avenue
Suite 304
Alexandria, VA 22302-1473
<http://www.SentinelSecurity.us>