IBM Security Harness Service Asset

Delivering a secure enclave in which unaccredited mission applications can be deployed

Highlights:

- Evaluate the functionality of the latest mission applications without the time and expense of accreditation
- Evaluate and operate multiple mission applications at once
- Easily expand virtualized environment to support changing system loads
- Help ensure network integrity and isolation with proven IBM BladeCenter® technology

Defense forces are under pressure from constrained budgets, even as they contend with the increasing speed of enemy threats. In response to these challenges—and to enable rapid deployment of mission capabilities—the *IBM Defense Operations Platform* environment offers transparency and flexibility, boosting mission effectiveness while controlling costs. The platform is designed to increase coordination and information sharing between military services and across a wide network of coalition partners, suppliers and external agencies.

When applied to the Defense Operations Platform, the *IBM Cyber Hygiene Service* Asset offers users the ability to harden the platform so that they can develop service oriented architecture (SOA)-based solutions on cleansed servers that are free of known vulnerabilities. The *IBM Security Harness Service Asset* is built on the *Cyber Hygiene Service Asset*.

Hosting unaccredited applications without introducing security risks

Traditionally, before any solution could be deployed on an enterprise network, it had to be certified. This was an expensive and time consuming process that delayed getting the answer to the key question that was being asked: Will this new application help our war fighters?

The IBM Security Harness Service Asset is a virtualized, pre-integrated SOA platform. It provides one or more protected enclaves for hosting un-accredited applications and allowing them to interact with users and other systems without introducing additional security risks to the larger enterprise. The Security Harness Service Asset is particularly valuable to government secure defense networks where new technology must be accredited before it can be tested on the networks. Time and money spent on complex, traditional accreditation processes reduces the ability of the Department of Defense to rapidly take advantage of new technology.

Providing access to new software in a controlled and managed framework

The Security Harness Service Asset can host one or more third-party mission applications. Each of these mission applications is in turn isolated from other hosted tenants. The Security Harness provides the necessary supervised network routing to enable the hosted mission applications to continue to provide their capabilities to the enterprise. In addition to the network infrastructure, the Security Harness provides a series of services that can be used by the mission applications to enable them to operate within the Security Harness Service Asset in a manner that is consistent with the enterprise's security policies.

Preventing unauthorized information exchange in both directions

The Security Harness controls all IP traffic using a software firewall. It directs browser based traffic to an IBM Tivoli® WebSEAL server that enforces authentication and authorization, while web service based traffic is sent to an IBM DataPower® appliance that will validate and proxy all web service providers residing in the Security Harness. The firewall translates network addresses for all traffic (both from the network and from the untrusted applications) so that the untrusted applications have no information about enterprise network addresses, and enterprise applications have no information about untrusted application network addresses. This prevents unauthorized use in either direction, thereby protecting the enterprise from potential risks being introduced by the untrusted application.

IBM BladeCenter technology—providing ease-of-use with a high degree of flexibility

The recommended hardware deployment configuration for the Security Harness Service Asset is an IBM BladeCenter® solution (with a minimum of four or five blades). The Security Harness Service Asset is designed to leverage the internal networking capabilities of the BladeCenter servers to ensure network isolation. For each mission application to be hosted in the Security Harness Service Asset, a virtual local area network (VLAN) is created and the mission application is deployed to this network. From the private VLAN, an untrusted application can be integrated with the Security Harness Service Asset and only specified, permitted traffic will flow between the enterprise network and the untrusted application.

Virtualized environment—offering connectivity in a manner consistent with enterprise security policies

The Security Harness Service Asset is delivered as a set of 15 VMware virtual machines, configured as a group that can be deployed and connected to enterprise services, such as:

- User authentication using either lightweight directory access protocol (LDAP) or public key infrastructure (PKI) certificates (hard [CAC] or soft)
- User authorization using role-based or attribute-based access control through a policy decision point/policy enforcement point (PDP/PEP) architecture
- The Online Certificate Status Protocol (OSCP) responder used to ensure point- in-time valid certificates
- Support for web service providers and web service consumers
- Application-to-application messaging controlled through a software firewall and optionally mediated by the Security Harness Service Asset framework
- Support for Extensible Messaging and Presence Protocol (XMPP)

Using the Security Harness Service Asset can help to significantly reduce the cost to implement and time to deploy new applications. Key benefits of the Security Harness include:

- Security-rich, rapid deployment of mission applications
- Enhanced speed to market, with reduced costs and minimized risks
- Integrated and harvested U.S. Federal Certification and Accreditation Processes
- Support for mission operational requirements with optimized operational efficiencies
- Automated install scripts for rapid infrastructure deployment
- Optimized hardware virtualization
- Security hardened environment
- Pre-integrated software stack
- Pre-integrated software calibration test harnesses

When and where it's needed most—security and interoperability function for promising capability

The Security Harness Service Asset is helping organizations adapt to increasingly complex and time consuming security certification and accreditation processes to deploy third-party applications. The Security Harness Service Asset for the Defense Operations Platform enables mission application capabilities to be made available on a security-rich network even though the mission application itself has not been certified a clear cost- and time-saving advantage.

For more information

To learn more about the IBM Defense Operations Platform and the IBM Security Harness Service Asset Service Asset, visit **ibm.com**/software/industry/defense-operations-platform/

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
September 2011

GVS03028-USEN-00