tripwire

SOLUTION BRIEF

Filling in the Gaps of HBSS with Tripwire Enterprise

HBSS originally focused on security for systems running Microsoft Windows. Significant scripting is required to manage UNIX systems even with a universal agent. Plus, there's no consistent platform support across HBSS products; each product in the suite supports different platforms.

The Host-based Security System (HBSS) is a suite of products that the Department of Defense (DoD) mandated for use within the DoD Enterprise Network in early 2007. The intent was that DoD organizations would use it to monitor, detect, and prevent successful attacks against the department's systems and networks. On the surface, the concept of HBSS is a solid one: a consistent, single IT security suite for a fixed price designed to protect all DoD systems and networks.

Since the time that HBSS use was mandated, the suite has undergone many changes. Products have been added, replaced and modified. The central management engine for the suite has remained consistent. But as DoD organizations have used and become accustomed to the suite, limitations and challenges have become apparent. The security configuration management solution Tripwire® Enterprise helps fill in those gaps.

Seen One HBSS Deployment, Seen One Deployment

It's a phrase often used throughout the public sector. Because each agency can select from among a list of vendor point products, no two HBSS implementations are the same. Further adding to the differences is the customization required to enable the DoD client to meet its needs. This customization stems from the fact that the vendor acquired most HBSS products from other companies, so they have little consistency in the underlying code.

In addition, because many of the vendor's premium security solutions aren't available with the HBSS suite, agencies frequently reach outside the master agreement to purchase solutions that do the job. So although HBSS offers all its products as part of a single site license, in reality, customization and the need to purchase non-HBSS solutions start increasing expenses.

HBSS Biased Toward Windows Systems

HBSS originally focused on security for systems running Microsoft Windows. Significant scripting is required to manage UNIX systems (such as AIX or HP-UX) even with a universal agent. Plus, there's no consistent platform support across HBSS products; each product in the suite supports different platforms.

ChangeIQ is change data Intelligence

Tripwire Enterprise automatically filters each change through ChangeIQ™ to let IT focus solely on changes of interest. These are changes that:

- Meet conditional actions that you specify
- Take a configuration out of compliance with policies like a DISA STIG or FISMA/NIST
- Indicate a problem, based on Tripwire's security expertise
- Tripwire Enterprise then alerts to these types of changes.

How Tripwire Enterprise Helps

Rather than replacing HBSS, Tripwire Enterprise complements it, filling in the gaps and smoothing coverage left open by the suite. By working alongside your HBSS implementation, Tripwire Enterprise improves your security posture with several key capabilities.

Baselines System State

Without knowing the original state of your server configurations, you can't tell what changed. Tripwire Enterprise baselines systems, helps you get them into a trusted and secure state, and detects any change from that state.

Enhances Change Audit Capabilities

Tripwire Enterprise adds more detail to change data. The kind of detail that shows exactly what changed, who made the change and when. Because the Tripwire agent doesn't require OS auditing to be turned on, it can capture "who" detail without causing a hit to system and network performance. That means you can tell who changed an IP address that caused a server to fail, or who changed an entry in an accounting file that modified annual bonuses. So whether it's a "fat-finger" mistake or an intentional unethical action, Tripwire Enterprise captures the detail to let you see exactly what happened.

ChangeIQ Adds Intelligence to Change Data

Tripwire Enterprise doesn't overload IT with all the change data that it captures. Instead, it automatically filters each change through ChangeIQ™ to remove extraneous data and let IT focus solely on changes of interest. These are changes that:

- Meet conditional actions that you specify
- Take a configuration out of compliance with policies like a DISA STIG or FISMA/NIST
- Indicate a problem, based on Tripwire's security expertise
- Tripwire Enterprise alerts to these types of changes. For example, a conditional action could specify to alert when the following three conditions occur: a specific person makes a change outside of a change window that causes a configuration to no longer match a golden build or DISA STIG compliant host. Any one of those changes alone might not indicate a security issue. But all of them together? Probably not a coincidence. Tripwire Enterprise even provides optional automated remediation to return non-compliant configurations to a compliant state.

Offers the Industry's Largest and Most Up-to-Date Policy Library

Regulations and standards change frequently—new requirements are added and existing requirements are made more prescriptive or stringent. If the policy you're using is two years old, can you be confident that you're compliant? Because Tripwire updates and publishes its policies frequently, you know that you're testing your configurations against the latest requirements. Plus, with over 400 policy/platform combinations for the most relevant regulations, standards, and security frameworks, you can be sure that Tripwire has the policy you need.

Complement Your HBSS Implementation with Tripwire Enterprise

Tripwire has a long history with the DoD, with over 700 deployments. Talk to your peers to learn how Tripwire Enterprise can help you get the most from your HBSS suite while adding greater coverage, better change audit capabilities, higher performance, and the most up-to-date and largest library of policies available today.

Tripwire Enterprise Product Complements to HBSS

- Provides DoD SHA-256 cryptographic and hash algorithm monitoring
- Tripwire Enterprise has an unlimited recurse capability, allowing for custom application or COTS rule building, as needed
- HBSS baselines are very limited compared to Tripwire Enterprise
- Reconciliation of file changes in HBSS is a lengthy process to get past Change Control Boards and into place
- HBSS does not scale well
- HBSS provides no "who" data
- HBSS cannot provide side-by-side content change comparison
- HBSS does not cover network or security devices, and is limited on *NIX
- A high number of discovered systems are considered "rogue" to HBSS (many false positives generated during asset discovery)
- Ticketing system integration is a huge challenge to HBSS
- Tripwire Enterprise monitors Active Directory and GPO. HBSS does not
- HBSS does not integrate well with log management solutions
- HBSS does not include an Event Generator agent like Tripwire Enterprise
- Compliance Checking with Tripwire Enterprise is thorough, complete and easy
- Correlation in Tripwire Log Center™ with direct integration to Tripwire Enterprise is a plus
- Automatically provide audit trails of changes with Tripwire Log Center integration (a must-have according to DISA)
- Dynamic Software Reconciliation (DSR) capability, which enables automatic change reconciliation of deployed patches, is lacking in HBSS

Schedule Your Demo Today

Let us take you through a demo of Tripwire security and compliance solutions and answer any of your questions. Visit **tripwire.com/contact/request-demo**

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

SBHBSS2j 1406