

SignaCert Enterprise Trust Solution

SignaCert's Enterprise Trust Server (ETS) combined with the Global Trust Repository (GTR) provides organizations with an unprecedented ability to control and identify changes in their IT infrastructure. SignaCert's configuration and change control solution captures, organizes, and compares the reality of what's running in your IT production environment against a set of trusted reference configurations and a whitelist application repository giving your IT staff not only data on change, but also the information they need in order to react appropriately.

Configuration and change control allows you to comply with regulations, increase the efficiency of your staff, and provide a more predictable environment through the deployment cycle. With the visibility that SignaCert brings, you'll:

- Comply with various industry and government regulations such as SOX and PCI which require change control processes exist and any changes made outside of the change control processes are identifiable
- Know when critical business systems have deviated from a known good state
- Get faster problem resolution and root cause analysis
- Know what files or configurations have changed, and which applications they correlate to
- Be able to conduct software inventories on systems off site
- Improve the predictability and reliability of your release process by ensuring that testing and production environments are exactly the same

The Challenges

What You don't Know Can Hurt You

One of the most daunting challenges an IT staff faces, is trying to keep all of their systems in a known good state. With many racks of servers in your data center, and increased use of virtualization, it is almost impossible to verify the integrity of systems, much less know if they match known good standard configurations. Unidentified changes and changes made outside of the change control process can have untold effects. Without a change detection system in place it is difficult to maintain high SLAs and just as importantly, it's difficult and time consuming to answer the question: "What happened?"

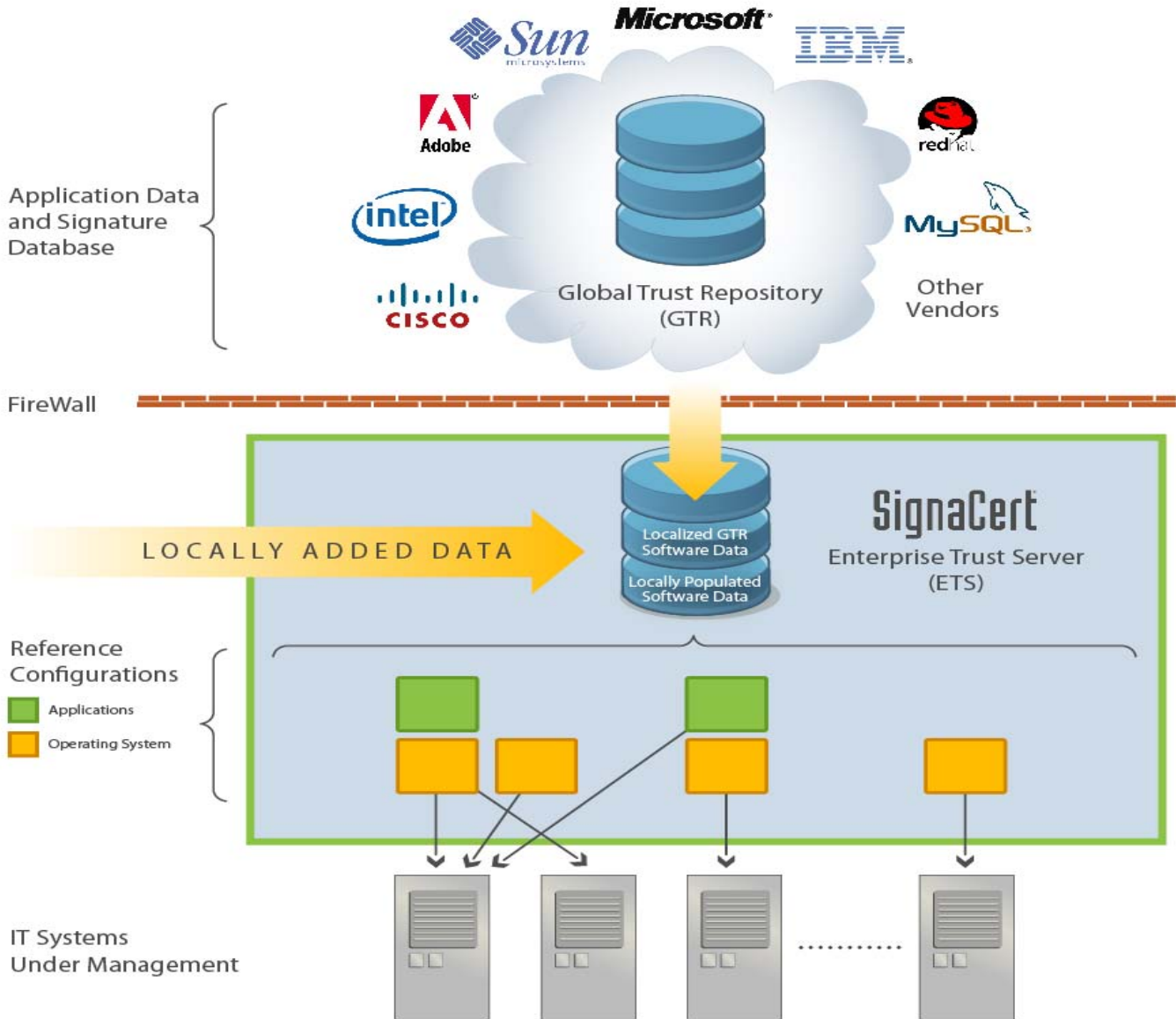
The Application Deployment Process

Business application development and management is a complex process that encompasses many systems, infrastructure types, business groups, and environments. The pressure to develop and deploy applications within aggressive timelines and strict budgets is commonplace. The goal is to create an environment in which the delivery of critical business applications is predictable and consistently successful. Unfortunately this is rarely the case. Staging environments don't match production systems, and configurations on production systems are inconsistent. This results in downtime and many non-productive hours trouble-shooting issues.

The SignaCert Configuration & Change Control Solution

The founders of SignaCert have many years of experience in building and deploying complex enterprise-grade IT change detection systems. Armed with visibility into the challenges faced by thousands of first generation product users, we embarked on a mission to dramatically improve change control through the introduction of a more scalable, manageable, and informative change detection solution. After over four years of development SignaCert created the following next-generation change detection innovations:

SignaCert Architecture



Many-To-One System to Reference Configurations

Unlike existing change detection solutions, SignaCert is fundamentally unique by providing a solution that centrally manages multiple reference configurations and images and compares deployed systems to those reference configurations. Using this approach, IT organizations enjoy a much more scalable solution that adheres to best practices IT management processes such as ITIL and COBIT.

The Enterprise Trust Server enables customers to create their own localized whitelist and reference configuration repository. As the reference image is actually decoupled from the IT device that is being monitored, *many* devices may be monitored with *one* reference configuration. In addition to this, several reference configurations or images can be

associated with the same device. This allows you to separate standard images as individual application stacks or operating systems, providing more flexibility in the assignment of monitoring responsibilities and improving scalability.

Hierarchical Reference Configurations

Reference Configurations are more than just flat files of the load-time and run-time data elements. Parent-child relationships are automatically retained, and relationships of packages to the application stack itself can be easily established. Through correlation of individual file and configuration changes to the higher level applications, the amount of noise is reduced, and your administrators can make more informed decisions regarding the nature of the change.

Whitelisting for Application Identification

SignaCert leverages whitelisting in a unique and revolutionary way. Employing a tiered architecture consisting of a cloud-based Global Trust Repository (GTR) and a local Enterprise Trust Server (ETS) SignaCert has created a way to leverage known provenance software from third party ISV's. The repository is a cloud service providing known-provenance whitelist measurements of commercially available and open source software. The measurements are obtained via direct partnerships with many software vendors covering a broad range of operating systems, device drivers, third-party applications, and many other types of data representing the desired state of systems comprising IT business services.

The Global Trust Repository is essential for achieving the following:

- Correlating the information presented in change reports to the applications and software to which they are associated
- Creating software inventories for physical and virtual IT infrastructure
- Quickly determining suspect software installed on physical and virtual systems for forensics-based analysis

How it Works

Harvest & Organize: In the harvesting step, a single reference provides software signatures to the SignaCert ETS. Initial collection and subsequent updates are as simple as adding a single line to your release process scripts. This information is stored on the SignaCert ETS so it becomes independent of your production environment.

Verify: SignaCert ETS gives you an easy-to-use console in which to select how you want to run the verification process. For example, you may want to look at the entire enterprise for a patch or just the web servers. The ETS compares your actual production environment against the trusted reference configurations you identified and shows you the deviations. The ETS also keeps historical data so you can generate reports on historical or real-time data.

Notify & Report: SignaCert notifies you of deviations through alerts and many reports. Links in the notifications let you quickly access the dashboards in the ETS console. There, you can drill down and learn more, or customize reports to your specific needs. When changes have been made that are unidentifiable by the ETS, you can manually or automatically synchronize with the Global Trust Repository to leverage its information and identify the applications with which the changes are associated. The ETS integrates with your current enterprise management system through a syslog, an event log, and SNMP.

Agent & Data Types Measured

Agent: SignaCert's Solution has a non-persistent java client (SignaClient) that performs the scans. It is scheduled or manually launched via SSH, WMI, Task Scheduler, or your own scheduling tool. Since SignaCert does not run a persistent agent, there is no idle memory or CPU footprint. During scans, CPU usage runs from 2 to 10% CPU depending

on the hash used, and disc I/O overhead. All transactions during a scan can have their priority levels lowered, to ensure other applications are not impacted during the scan.

Types of Data Measured: Depending on your use case, the data type may vary. Below is a list of data types, and the recommended data element to measure:

- Software Installations – Binary/Library
 - Hash based Policy utilizing 1 of our 4 supported hash types, MD5, SHA1, SHA256, SHA512
 - Attributes of the files: Permissions, Ownership, SACL/DACL(windows only), etc....
- Software Installations – Configuration/Registry
 - Attribute based configfile parsing
 - Attribute based registry measurements
- Offline virtual machine images from industry leading vendors, VMware®, Microsoft®, and Citrix®, as well as databases and the Windows® registry.

About SignaCert

SignaCert is the leading provider of next-generation IT compliance solutions allowing organizations to rapidly achieve and prove continuous compliance for the systems that deliver critical business services. SignaCert's patented technology can be quickly deployed and provides immediate visibility into the actual state of IT infrastructure. The SignaCert architecture is designed to seamlessly integrate with existing change processes and continuously monitor critical business services without disruption.

Founded in 2004 by 34-year IT security and compliance industry veteran Wyatt Starnes, SignaCert has assembled a world class team of industry leaders with hands-on IT experience for its executive team, board of directors, and advisory board. SignaCert's customers span a wide variety of industries, including financial services, government, and healthcare.

For more information visit: www.signacert.com.