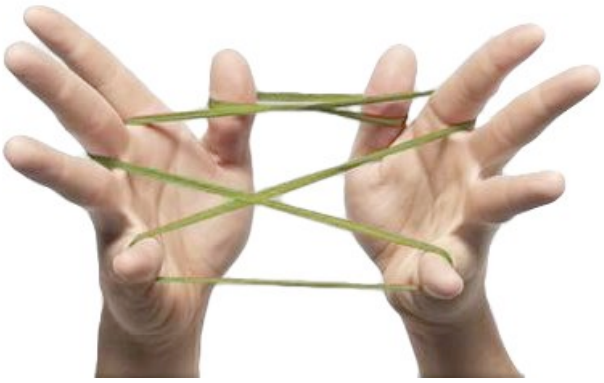
Reduce the Cost of Compliance

with SignaCert

Table of Contents

Introduction

Many organizations achieve compliance through costly, last-minute procedures. They don't have the proper visibility into their IT environment to truly know where they stand before racing to pass an audit. Compliance regulations are continuously evolving and organizations must find ways to maintain a state of compliance while keeping costs as low as possible. Providing auditors with the evidence they need to certify your IT infrastructure as quickly and as effectively as possible is of utmost importance.



SignaCert not only provides you with the proof you need to pass an audit, but also helps you streamline the entire compliance process. By automating the repetitive tasks and continuously monitoring your environment, you can more easily reach compliance and stay there. SignaCert's out-of-the-box compliance tests, next-generation file integrity monitoring (FIM), automated vulnerability assessment framework, and powerful reporting capabilities give you true visibility into your environment. In addition to these features, SignaCert also provides you access to their patented Global Trust Repository (GTR), which contains billions of software signatures for use when identifying software. With SignaCert, you can ensure that your IT environment stays compliant and secure at the lowest possible cost.

Compliance Automation

Demonstrating compliance for an ever-increasing number of regulatory standards is proving to be prohibitively expensive for IT organizations. SignaCert simplifies the process of establishing and maintaining compliance with the regulations and standards IT organizations face most.

Out-of-the-box Solutions

With out-of-the-box assessment and reporting capabilities, SignaCert solutions automatically generate the audit trail necessary to demonstrate compliance, providing significant cost savings over manual procedures. SignaCert provides solutions for NIST 800-53, HIPAA, SOX, PCI DSS, and other standards. These solutions contain tests for specific requirements, such as password complexity rules, as well as support for requirements bigger in scope, such as file integrity monitoring (FIM).

Validated SCAP Solution

Maintaining the security of enterprise systems is challenging due to the number and variety of systems to secure, the need to respond quickly to new threats, and the lack of interoperability among security management tools. In response, the National Institute of Standards and Technology (NIST) created the Security Content Automation Protocol (SCAP), which enables organizations to verify the presence of patches, check for proper system configuration settings, assess systems for vulnerabilities, and automatically generate reports. SignaCert provides a NIST-validated solution that enables customers to centrally manage, assess, and report on the compliance of your enterprise. SignaCert is a vulnerability and patch scanner, an authenticated configuration scanner, and a validated FDCC scanner. You can utilize security checklists and benchmarks such as USGCB (US Government Configuration Baseline), DISA STIGs (Security Technical Implementation Guides), Microsoft Security Compliance benchmarks, and any other checklists or

SignaCert provides out-of-the-box solutions for the following:

- NIST 800-53
- PCI DSS
- HIPAA
- COBIT
- SOX
- USGCB
- FDCC
- DISA STIGs
- Microsoft Security Compliance

Validated SCAP solution:

- Authenticated vulnerability and patch scanner
- Authenticated configuration scanner
- FDCC scanner

vulnerability definitions in SCAP-compliant formats.

Automated Validation, Continuous Compliance

SignaCert's automation capabilities enable you to continuously monitor your environment. This ensures that you not only meet compliance, but stay in compliance. It is far less costly and less resource-intensive to maintain a state of compliance with automation than to reassess your compliance posture every time you need to perform an audit.

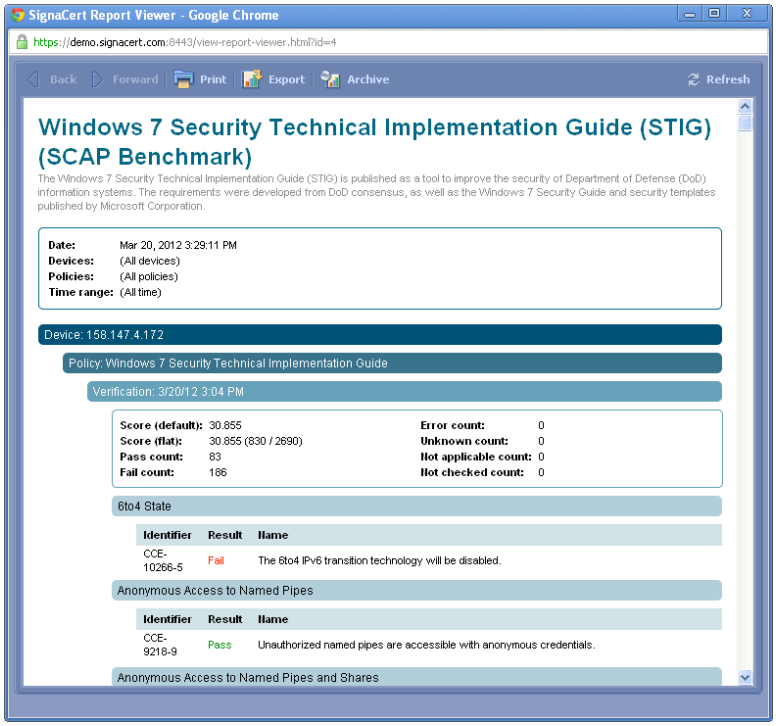


Figure 1: SignaCert SCAP-based STIG Report

In-depth Reporting

SignaCert's in-depth reporting capabilities enable you to view your compliance status in many different ways. Reports can be customized for auditors, executives, or IT administrators. SignaCert reports give you the necessary paper trail to comply with the auditing process.

Extensible Testing Framework

SignaCert offers an extensible testing framework that enables you to create your own tests using a simple-to-use standards-based scripting language. You can combine SignaCert's pre-built compliance solutions with your own custom tests to create a comprehensive set of tests best suited to the unique requirements of your enterprise.

File Integrity Monitoring (FIM)

No organization wants to contend with costly service outages or security breaches. But when devices are configured improperly, that is exactly what happens. In an attempt to alleviate these issues, organizations rely on file integrity monitoring. Not only is this an essential security practice, but it is also mandated by several compliance standards (e.g. NIST 800-53, PCI DSS, SOX, HIPAA).

Did it Change? vs. Is it Correct?

Up until now FIM solutions focused on the notion of whether systems changed. SignaCert is the first product to not only perform change detection, but tackle the idea of whether your systems are configured correctly.

The Flaw With First-Generation FIM

File integrity monitoring solutions take a baseline (or snapshot) of the data on each system (files, permissions settings, etc.) under the erroneous assumption that each system is in a known good state. Monitored systems are then evaluated, detecting and reporting deviations from the established baseline.

The fundamental problem with FIM solutions is that separate baselines are created for each monitored system. Not only is this a time-consuming and resource-intensive process, but it doesn't address the “integrity” aspect of file integrity monitoring. When a change is reported, all you know is that the system is different today than it was yesterday. What you need to know is whether systems have drifted from approved standards.

SignaCert’s Next-Generation FIM

SignaCert tackles this problem by giving you more flexibility in how you build baselines. As with traditional FIM tools, you can create a unique baseline per device (“snapshot per device”), but you can also create a “shared snapshot”, which is a single

SignaCert’s FIM solution addresses the following compliance requirements (among others):

NIST 800-53

- CP-9: “…protects the confidentiality and integrity of the backup information.”
- SI-4: “Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files…”
- SI-7: “The information system detects unauthorized changes to software and information…”

PCI DSS

- 10.5.5: “Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts…”
- 11.5: "Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files..."

COBIT

- DS 9.2: “IT management should be ensured that a baseline of configuration items is kept as a checkpoint to return to after changes.”
- DS 11.30: “Management should ensure that the integrity and correctness of the data kept on files and other media is checked periodically.”

HIPAA

- §164.312: “Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.”

baseline shared by multiple systems (see Figure 2). This goes beyond mere change detection to ensure that systems are aligned to your enterprise standards.

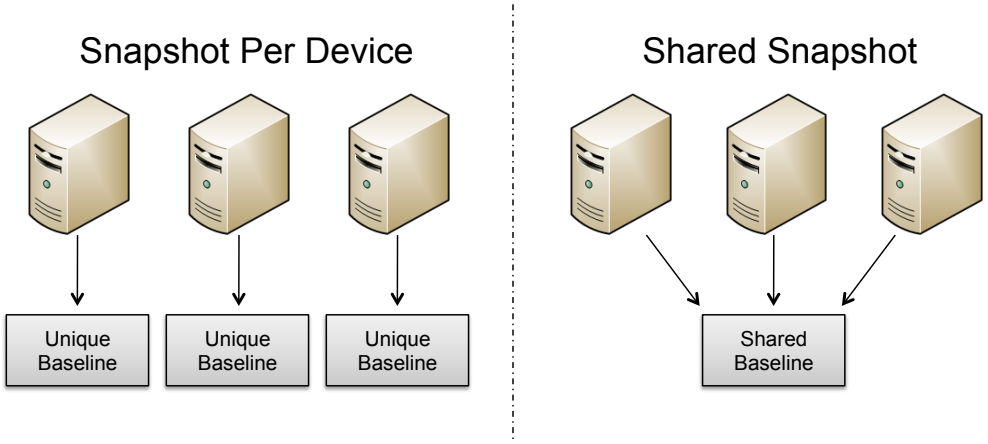


Figure 2: Snapshot Per Device vs. Shared Snapshot

Furthermore, unlike other FIM solutions that force you to create one baseline to encompass everything to be monitored on a particular system, SignaCert enables you to associate a system with multiple baselines for different aspects of the monitoring process. You can create a particular baseline for each facet of your FIM strategy (see Figure 3). This gives you flexibility in how you define and use baselines across your enterprise.

Not only does this make your job easier when assessing the state of your environment, this architecture far more scalable when dealing with tens, hundreds, or thousands of systems. You avoid the data duplication that makes other FIM solutions untenable (or even impossible) in large environments. And when your organization's policy changes, you only need to update the affected baseline(s), rather than creating new baselines for every system in your enterprise.

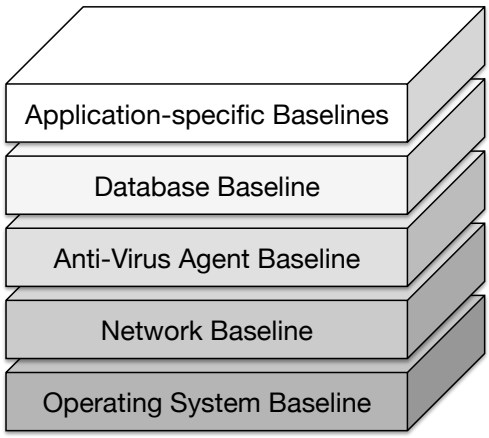


Figure 3: Sample Baselines for Device

With SignaCert's FIM solution you can easily determine whether critical applications are consistently deployed across a set of systems, and whether all of the critical components of an infrastructure service (web, service layer, database, etc.) are deployed consistently throughout a server farm. SignaCert is the only FIM-based solution on the market today capable of providing these answers.

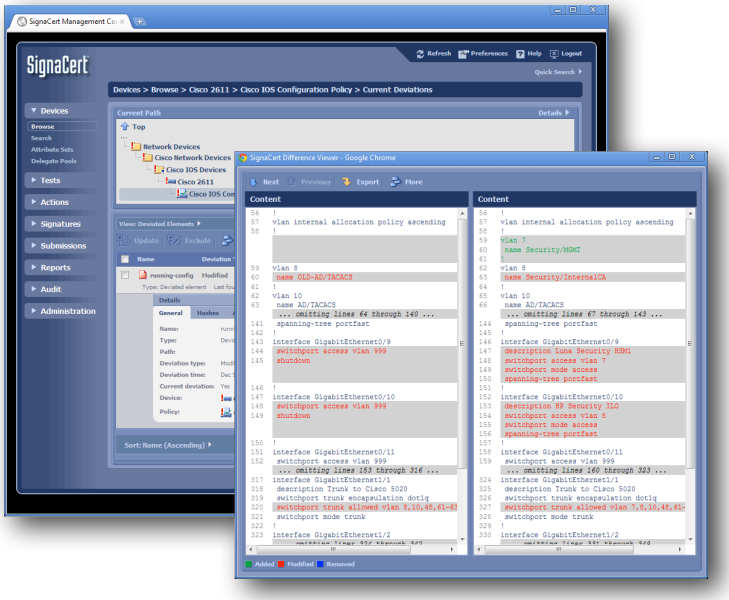


Figure 4: SignaCert Difference Viewer

Reporting Capabilities

SignaCert offers an extensive library of report templates. These reports provide a high-level view of your environment as well as detailed views designed for performing a comprehensive audit. You can also take advantage of SignaCert's dashboard feature, which displays thumbnails of multiple reports at once.

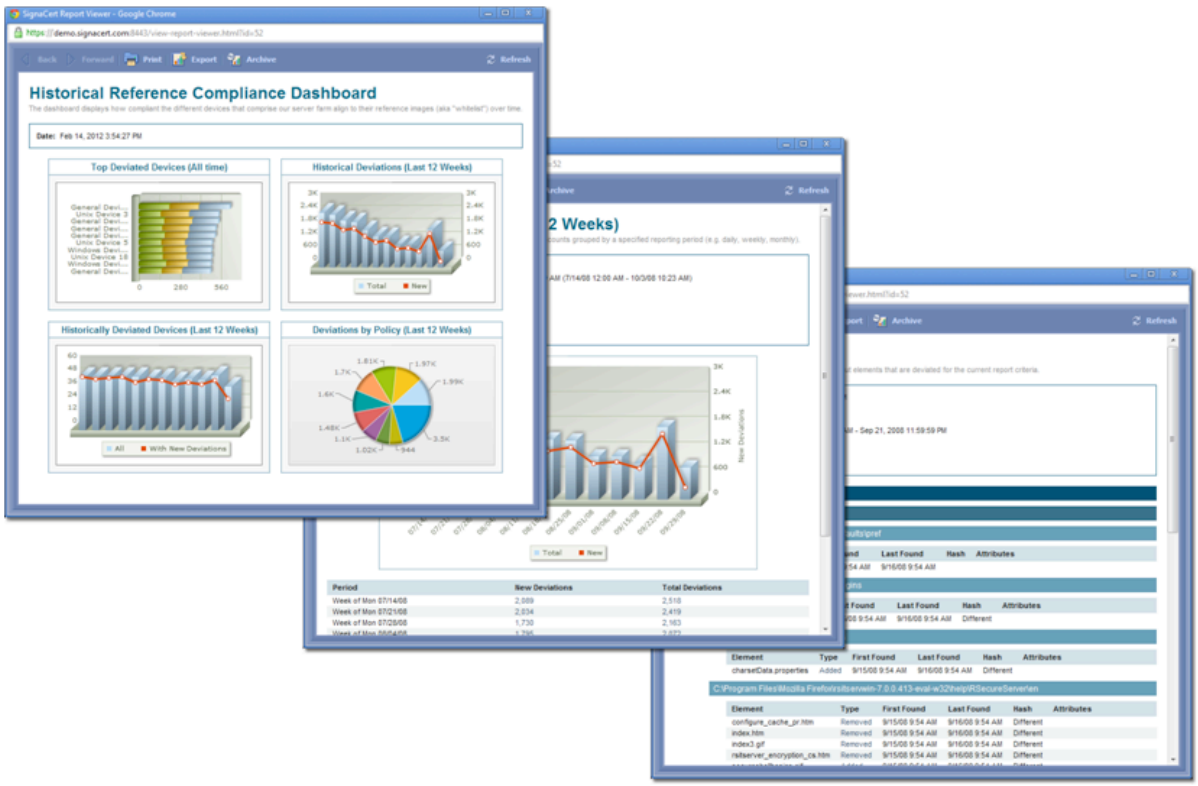


Figure 5: FIM-related SignaCert Reports

Vulnerability Assessment

Keeping up-to-date with a growing number of vulnerabilities and exploits is proving to be a never-ending process. Taking advantage of a well-known standard, OVAL, SignaCert simplifies the assessment process by leveraging vast repositories of frequently updated vulnerability definitions.

Open Vulnerability and Assessment Language

OVAL (Open Vulnerability and Assessment Language) is an international information security standard that establishes how to assess and report on the state of a machine. This provides a reliable way for organizations to automate the process of assessing systems for the latest vulnerabilities.

Automated Vulnerability Assessment

SignaCert allows you to subscribe to OVAL-compliant feeds and automatically incorporate new vulnerability definitions into your assessment policies. Vulnerable systems are immediately detected and reported, significantly minimizing the risk of an exploit.

Vulnerability assessment features:

- SCAP-validated vulnerability and patch scanner
- Seamless, automated subscriptions to OVAL-compliant vulnerability feeds
- Automatically incorporates new vulnerability definitions into existing policies
- Access to authenticated OVAL vulnerability assessment feeds directly from the SignaCert Customer Cloud

Supported platforms for OVAL-based vulnerability assessment:

- Windows 2008 Server
- Windows 2003 Server
- Windows 7
- Windows XP
- Red Hat Enterprise Linux
- CentOS
- Ubuntu
- Solaris

OVAL-compliant repositories:

- OVAL (oval.mitre.org/repository)
- Red Hat (www.redhat.com/oval)
- SecPod (oval.secpod.com)
- Any other repositories containing OVAL-compliant content

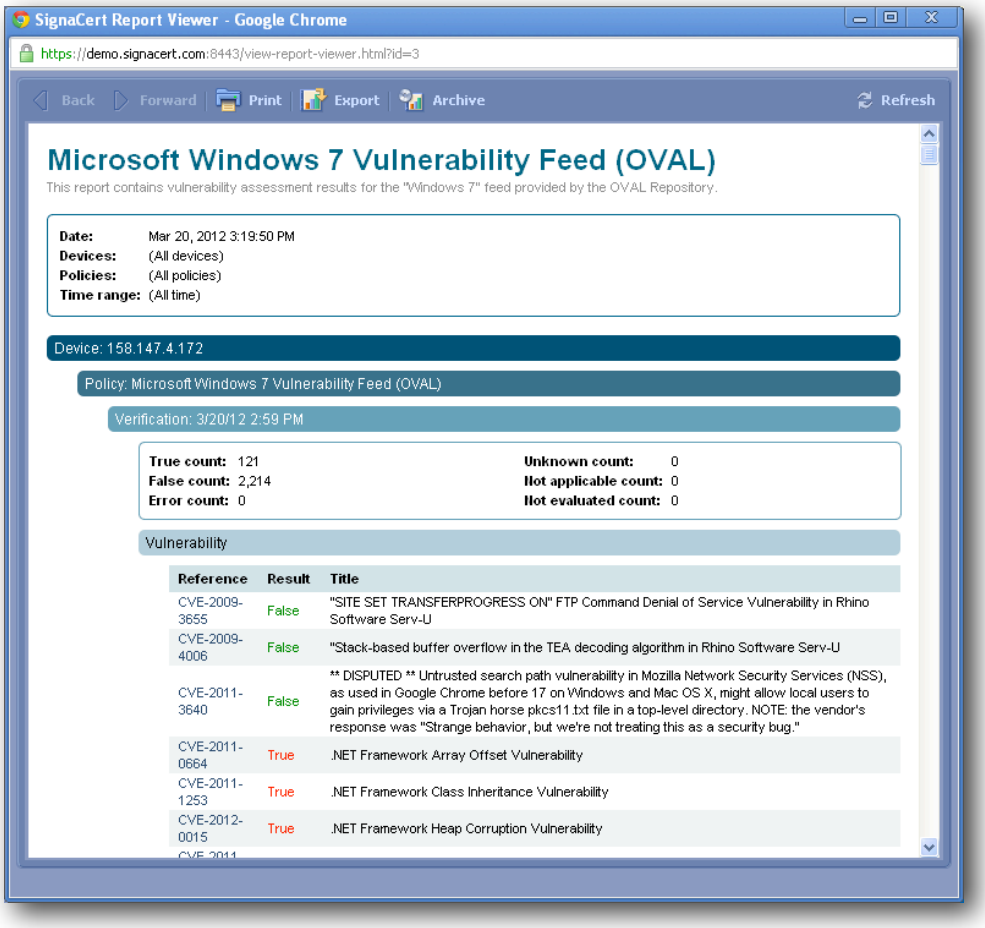


Figure 6: SignaCert Vulnerability Report

Global Trust Repository (GTR)

The SignaCert Global Trust Repository (GTR) is a patented cloud-based resource that contains over four billion signatures for commercial and open source products. These signatures are obtained through 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.

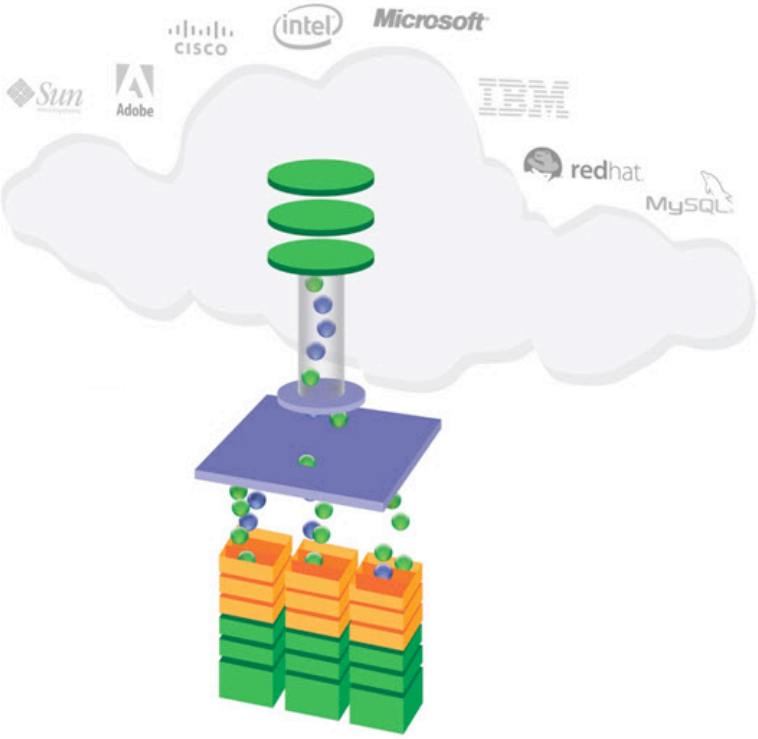


Figure 7: Global Trust Repository

Global Trust Repository Statistics

- Over 4 billion unique signatures
- Growing at 10 million signatures/day
- Millions of unique products
- More than 2000 vendors
- Patented technology that is unmatched by any other repository

GTR Patents:

- 7,272,719
- 7,487,358
- 7,733,804
- 7,904,727
- 8,139,588

SignaCert solutions can seamlessly communicate with the GTR to provide the following features:

- **Noise Reduction**
  Correlating the information presented in compliance reports by the applications and software with which they are associated
- **Infrastructure Software Inventories**
  Creating software inventories for physical and virtual IT infrastructure
- **Forensics Analysis**
  Quickly determining suspect software installed on physical and virtual systems for forensics-based analysis
- **Software Authenticity Validation**
  Validating that physical and virtual IT configurations are comprised of authentic software from the original vendors

With SignaCert, you have instant access to the world's largest repository of known provenance software signatures.

Device Support

SignaCert supports integrated monitoring of a wide range of devices. All Windows operating systems since Windows 2000 are supported. SignaCert monitors Linux distributions including RHEL, CentOS, Ubuntu, and SUSE. Additionally, Unix platforms such as Solaris and AIX are supported. A vast number of network infrastructure devices are monitored, including devices from HP, Cisco, Brocade, Palo Alto, F5 Networks, and Juniper. SignaCert supports storage systems by EMC, IBM, HP, and others. A variety of mobile devices are supported. SignaCert also monitors virtual infrastructures by VMware, Citrix, Microsoft, and others.

Ready to Use

The SignaCert Enterprise Trust Server (ETS) enables the solutions covered in this document. Available as a hardened physical or virtualized appliance, SignaCert's Enterprise Trust Server is ready to use out-of-the-box. A single ETS can support up to 10,000 monitored devices.

Figure 8: Enterprise Trust Server

SignaCert supports a wide range of devices including popular operating systems, switches, routers, firewalls, fiber optic interconnects, storage devices, and virtual infrastructures.

Microsoft
redhat
ORACLE
IBM
cisco
EMC²
vmware
hp
CentOS
JUNIPER NETWORKS
solaris
FireEye
Remedy Corporation
f5
bmcsoftware
ubuntu
FOUNDRY NETWORKS
BlackBerry
paloalto NETWORKS
BROCADE

Contact us to find out more about SignaCert.

Website: www.signacert.com
Email: sales@signacert.com
Phone: 888-711-7633

Summary

Compliance costs money. It is just a matter of how much money and how many resources you want to use for your compliance posture. You can panic at the last minute and deal with a tedious audit process that derails the real work you need to accomplish. Or you can take a proactive stance to your compliance status and use a product that keeps you in a continuous state of compliance with minimal resources, lower costs, and increased reliability.

Learn more at www.signacert.com or contact us directly.

Email: sales@signacert.com

Phone: 888-711-7633