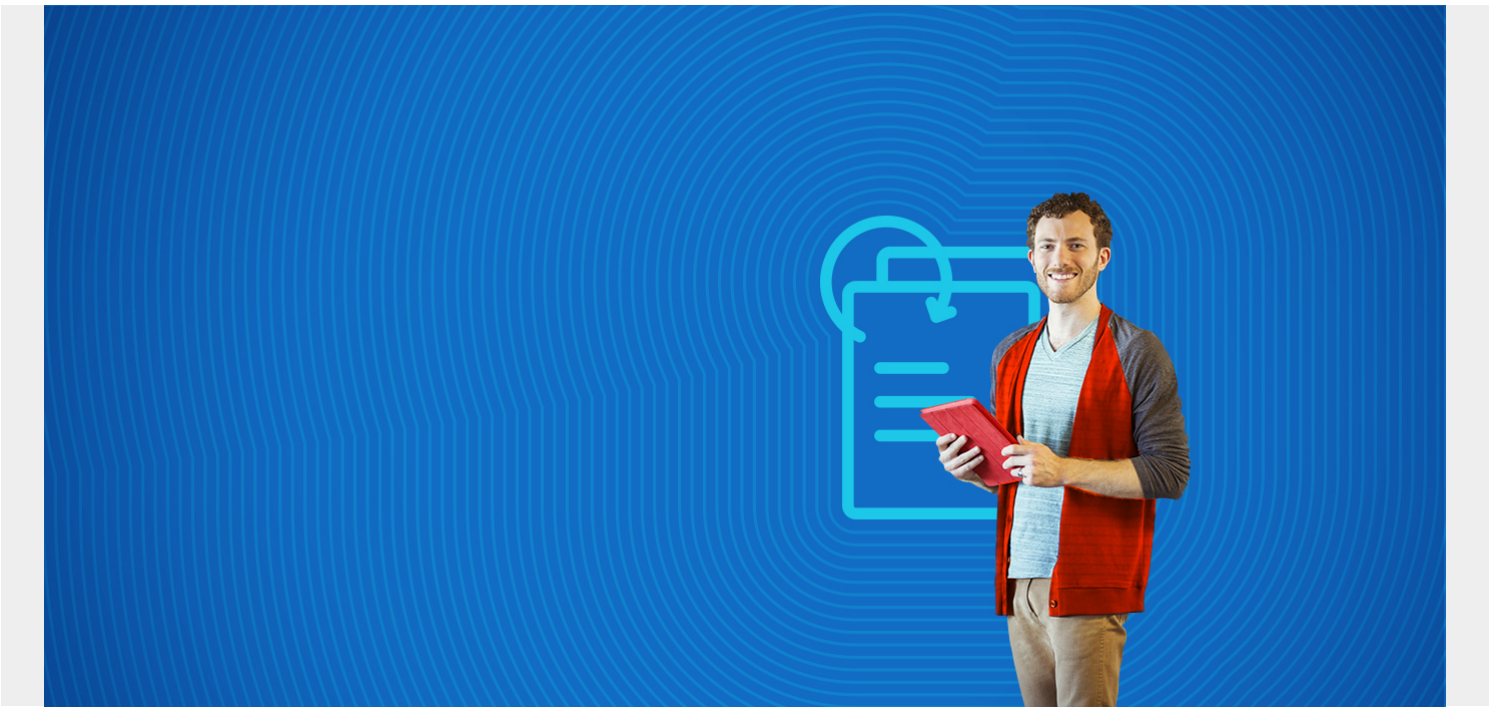
COMPLIANCE PROGRAMS: AN INTRODUCTION



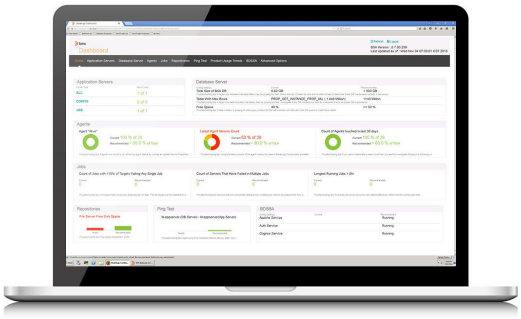
Managing OpEx with three IT compliance drivers

An effective compliance program helps you manage operational cost and risk in the data center and cloud environments in three major areas: security/regulatory, patch, and operational/build compliance.

Security and regulatory: any organization operating in a regulated environment, and those for whom security of information and systems is important, must comply with one or more policies. Sometimes these are explicitly provided by a regulating agency, in the case of the Defense Information Security Agency or the Payment Card Industry's policies, other times the organization is left to define their own policy that satisfies higher goals, or where guidance is less explicit. Either way, having a set of out-of-the-box compliance policies to start with makes it easier to either define from scratch, or refine a custom hardening policy from existing standards.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

Fast track security with TrueSight Vulnerability Management for Third-Party Applications



[Explore TrueSight Vulnerability Management for Third-Party Applications ›]

See how you can accelerate vulnerability resolution, lower costs of remediation and avoid major security incidents.

- Prioritize and remediate vulnerabilities with TrueSight Vulnerability Management for Third-Party Applications
- Reduce time spent logging changes in CM system
- Improve systems stability through granular, role-based access
- Explore the security view to see predictive SLAs and burndown with TrueSight Vulnerability Management for Third-Party Applications

While there are many platforms and tools that provide some form of security policies to evaluate servers against, we don't tend to see real or consistent improvement on compliance to those policies without a number of key ingredients.

Regular scanning is key to achieving consistent compliance over time. Those organizations that scan daily or weekly have much better visibility into their current state than those that scan only monthly or quarterly. These regular scans help keep the state of compliance at front of mind, and reward those organizations that make efforts towards improving the state of compliance. This regular feedback, and visibility into the trend-lines helps support the ongoing compliance effort.

Integrated remediation practice and content is how organizations achieve ongoing, affordable compliance. There have been scripts and systems to identify where the compliance gaps are in environments for almost as long as there have been configurable systems, but real compliance improvement is rarely achieved until it becomes cheap and easy to enforce and remediate compliance gaps. Tools like BladeLogic Server and Network Automation that ship with out of the box remediation instructions mean that teams using these products are able to quickly get to work bringing systems up to the compliance standard, rather than having to stand up multi-person projects just to build these initial remediations.

Exceptions or rule changes are the fine polish of compliance: there's always an application that needs an exception, or a server that has a configuration needed for a special case, or a rule that needs to leverage an environment variable, like different domain names in different production environments, or a local administrator account that includes the name of the server in it. The ability to parameterize rules, or add the occasional rule exception makes it much easier to hit 100% compliance, rather than having to "accept and wonder about" a 97-98% compliance figure.

Integrated change is key for modern, mature production environments. Our customers in highly regulated environments often tell us that more than half of the effort of any type of compliance remediation is in documenting and gaining approval for the change. A solid integration with the change system (often implemented via orchestration or direct integration) is key to making this easy. Otherwise your teams can easily spend half their time "swivel-chairing" the paper process between automation and change, driving up operational cost, and opening a gap for the last 3-5% of compliance to fall through.

Closed loop compliance and change is the process of identifying compliance gaps and creating both incident (because something's not the way it's supposed to be) and change (because we want to fix it) tickets, automatically. This is easy to execute in an automated environment, because we know the policy, we know the CI (the server or network device), and we know what's out of compliance. Automation removes any potential for manual entry error at this point. In environments that have implemented closed loop, tickets are created automatically, many of the types of incidents have standard approvals, and are often cleared and closed automatically, without human intervention. The potential and real savings of OpEx are significant.

Build or operational compliance is the second major type of compliance we see in production environments, and this should be the most important to drive down day to day operational cost. In environments when systems were built by hand, it was usually easy to identify who had built a particular server by the "fingerprint" that person had left on a server, perhaps a commonly missed configuration item, or a particularly well-executed build. Unfortunately, variety in server or application builds increases costs of support, and decreases system reliability over time. Even implementing as few as 5 rules around basic agent versions and simple configurations can have a significant impact on the reliability and cost to support a production environment. Typical build policies usually have 20-25+ checks in them, and deliver the greatest part of their value when they are used consistently across the environment.

Lastly, Patching, which we discuss elsewhere, is the fastest route to closing the bulk of known vulnerabilities. A policy-based approach drives down cost in a function that rarely delivers new value to the business, but instead helps manage risk, ideally executed at a minimum operational expense to the business. A consistent, smoothly orchestrated and automated process is key to satisfying application and business process owners.

We cannot consider compliance in a vacuum, it must come from all three of these major pillars.