

ei Ecom Infotech Inc

Governance Risk Compliance Solutions

Data Assurance
Governance Risk Compliance
COBIT , ISO 27001 , ITIL
IBM Tivoli
Identity and Access MGMNT
IT Infrastructure Managemant
Business Continuity and Resilience
Enterprise Security Managemant

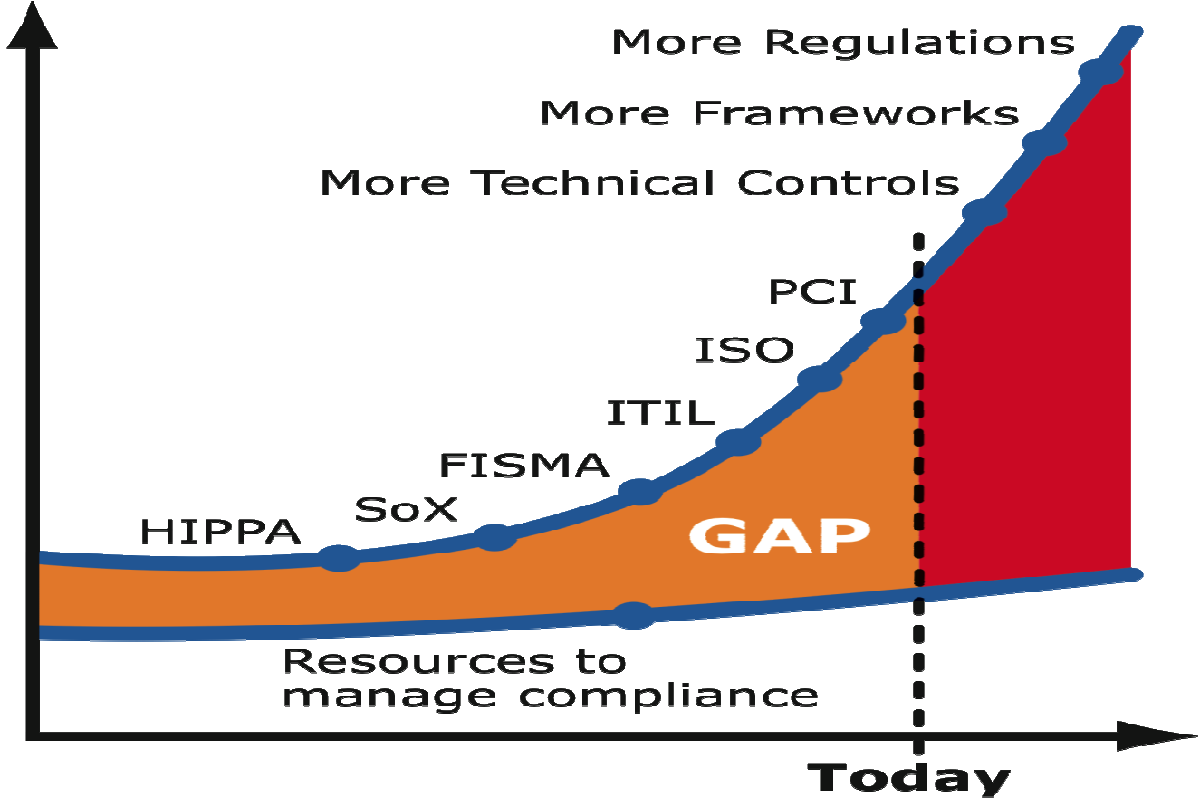
Information Security Governance Risk Compliance Solutions

[Click here for more details >>](#)

[Corporate Training](#)

Holistic Approach to Your Security

Enterprise Security Management



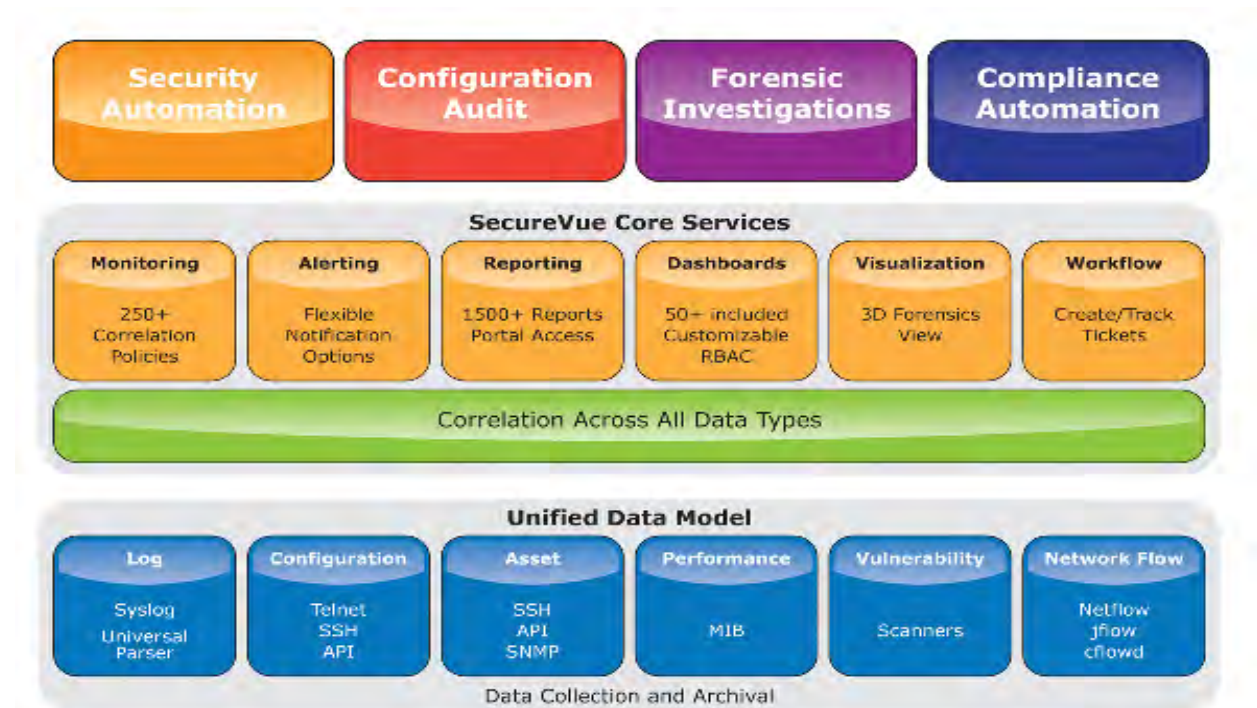
If you are an information security or IT audit professional, then you are in the business of securing your organization’s information assets and complying with regulations. Many organizations have historically adopted a “rifle-shot” approach to complying with regulations. As new regulations popped up on the radar, IT implemented a tactical program to comply with each specific regulation.

Given the number of regulations and the emerging threat environment, organizations must now take a much more strategic approach to compliance initiatives. Fortunately, in recent years information security and privacy compliance have made dramatic gains in becoming high-interest targets across Board Rooms –although for many organizations, “compliance” still equates to “regulations”. This regulatory-focused

approach is at odds with the reality that the scope of security and privacy compliance requirements that must be addressed and managed by organizations is increasing every day. No longer solely the domain of SOX, HIPAA, PCI DSS and other government-driven mandates, today's information security and privacy compliance programs must address a wide range of internal requirements dictated by business partnerships, established service level agreements (SLAs), known and emerging threats, and other factors driven by both business and technology. Addressing all of these requirements separately is an exercise in futility. The most effective method to manage compliance with so many different – and sometimes contradictory – compliance drivers is through a disciplined, holistic approach that addresses compliance not as a reactive or point-in-time event, but as a proactive, comprehensive program.

Convergence of Technologies

Our solutions bridge the gap between the stovepipe tool approaches that have evolved over the last 10 years. Our solution collects, manages, monitors and reports of Syslog Data, Asset Data, Scanner Data, Performance Data, Configuration Data, Network Flow Data etc.

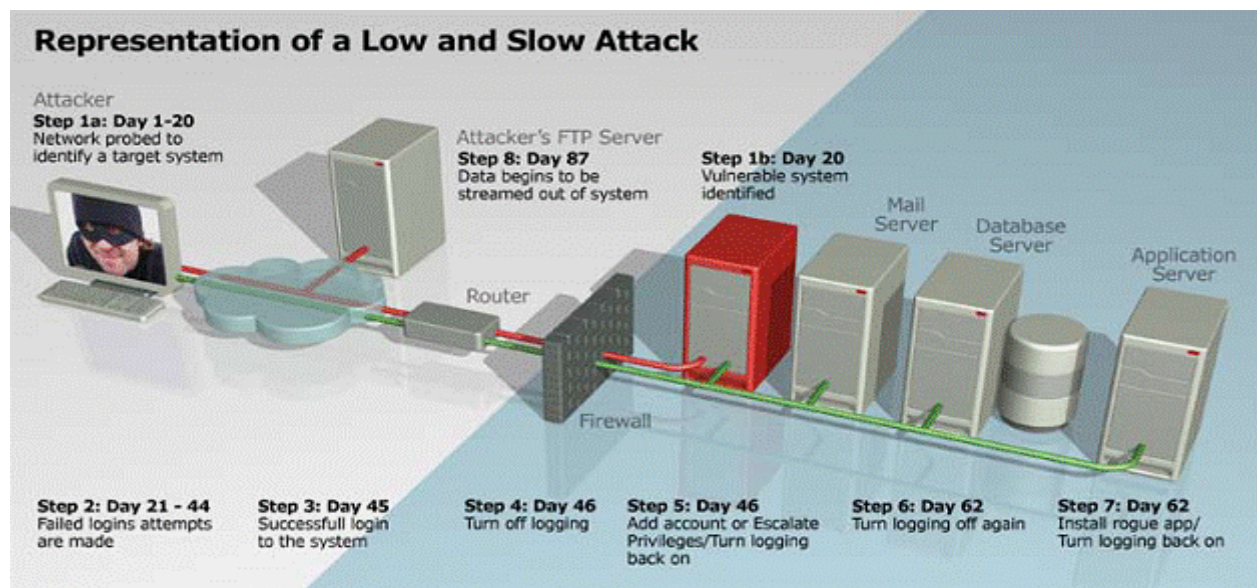


Our Solution collects this data from all devices and hosts on a network and brings it into one central, easily managed database. This approach equips with the unique capability and capacity to correlate all the different data types. This is important because:

- Role-based access control allows organizations to segregate and separate duties
- The NOSC can have a holistic view of the network and security posture
- Situational awareness can be gained from multiple viewpoints (Network, Security & Audit/Compliance)
- Dashboards, monitors and reports can be generated for the specific requirements of your initiatives
- End-to-end correlation is implemented between the different data silos
- The network risk posture can be visualized in its entirety
- Enterprise compliance requirements are met by built-in FISMA/SP800-53 compliance through Audit Center
- Additional mandated compliance requirements can be readily and easily customized for the organization
- A single pane of glass: The NOSC can drill down to identify the root cause with one tool.
- Both the Operations and Security teams can create workbenches and workflows to correctly identify a problem and correct it.

Analyze Log Data

Evasive attacks go undetected because you're looking backwards, after the attack happened. In order to detect a low and slow attack while it's in progress, you need to analyze more than just log data.

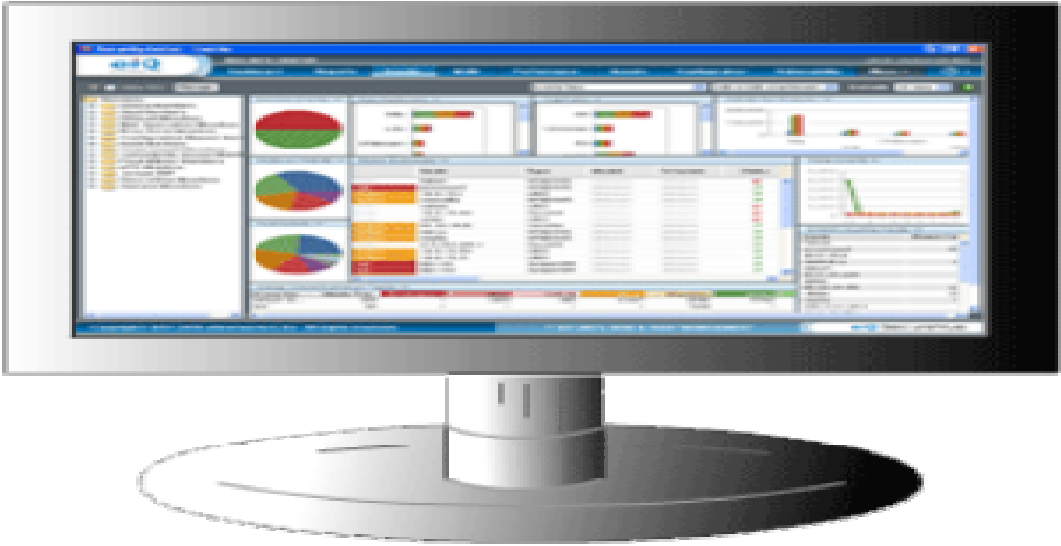


An integrated platform that collects, correlates, and analyzes log data plus configuration, system, asset, and flow data can help reduce the millions of events into single-digit real incidents, and also provide complete context around any event. As a result, end-to-end correlation reduces false positives and optimizes the system's ability to detect breaches while reducing cost and management complexity. A single unified console eliminates multiple data silos and enables efficient root-cause analysis. Because everything is interlinked, you can get to the bottom of an issue in minutes or seconds. Your existing SIEM just relies on log data, doesn't it?

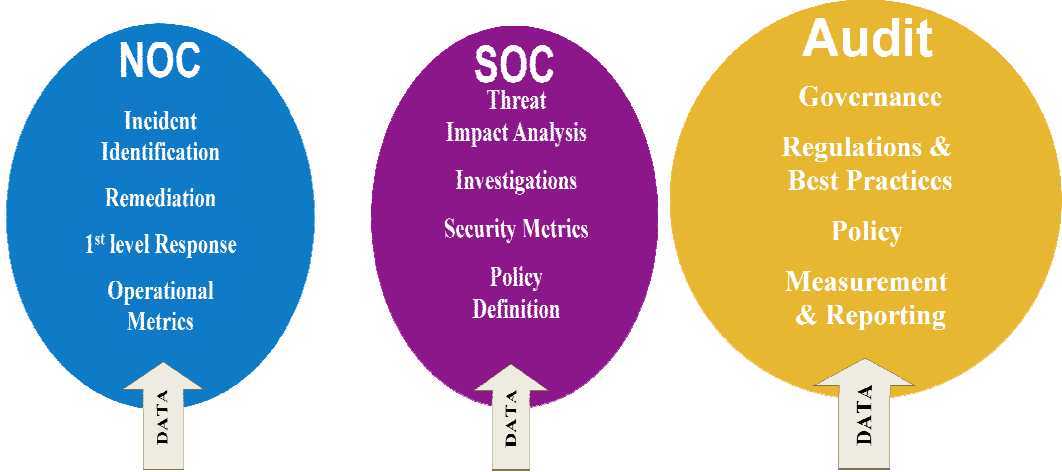
What to do when "Logging is turned off"

The first thing an attacker does is turn off logging to remove evidence of his tracks. What will you do when logging is turned off on your SIEM? How soon will you know? This is an inherent limitation to today's SIEMs, which are driven by log data. If the log data isn't there, you're blind. This is not a good way to manage a security environment. However, if your SIEM is also looking at configuration data, you'll know that logging has been turned off because it's a configuration change. You'd also see different performance metrics from the device, since it's doing the attacker's evil tidings. The attackers leave a trail; the problem is that it's usually not in the logs. Do you see that log data is not enough?

The network never lies. Attackers always leave a network trail, and flow data (if your system is collecting it!) can provide you with another clue that an attack is happening. By analyzing flow data you can develop a baseline for network traffic with which you can compare suspect behavior. Unfortunately, most of today's SIEMs don't pay attention to network flows.



Integrated Security and Compliance Management Platform



Analyze configuration changes

Any attack includes configuration changes, including turning on or off services, installing malware, and initiating connections. All of these provide more clues to help you effectively corroborate the data you already have. No product will be able to tell you, “Hey, you’ve got an issue here!” These tools are not built to replace you. But they should make you more efficient and help make your job a little easier. Configuration data does that. It gives you more corroborating evidence when you’re investigating suspect network activity. Monitoring device configurations is also critical to ensure adherence to corporate policies. Many organizations have adopted secure configuration policies from organizations like the Center for Internet Security, and having the security management tool monitor adherence to these policies and pinpoint when a device is no longer configured correctly can alleviate many security issues.

Contact us for more details

Ecom Infotech Inc

Call India +91 9869436685 US 1-312-224-1657

www.ecominfotech.biz <mailto:ac@ecominfotech.biz>