



The National Weather Service Southern Region Saves up to 60 Hours per Year on Compliance Audits



Customer

National Weather Service Southern Region, NOAA

Industry

Government

Website

www.weather.gov/SRH

Netwrix Auditor Applications
Netwrix Auditor for Active Directory and Windows File Servers

Customer Profile

The National Weather Service (NWS) provides a national infrastructure to gather and process weather-related data. With headquarters in Maryland and regional headquarters in Missouri, New York, Texas, Utah, Alaska and Hawaii, the agency has 5,000 employees in 122 weather forecast offices, 13 river forecast centers, 9 national centers and other support offices around the country. Each year, the NWS collects 76 billion observations and issues approximately 1.5 million forecasts and 50,000 warnings for the protection of life and property and enhancement of the national economy.

THE CHALLENGE

As a government agency, the National Weather Service Southern Region has to comply with a set of internal and external (NIST 800-series) security regulations. The main challenge for the NWS Southern Region was to establish centralized IT security control and monitoring across its most critical systems, including Active Directory and file servers, because its offices are located all over the United States and are supported by a distributed IT team of 24 local domain admins and 6 enterprise-level admins. The agency has to operate 24/7, so it was important to ensure ongoing IT system availability and security. A complex IT environment that includes two Active Directory systems (local domains and an enterprise domain) only added to the challenge. Lack of visibility under those circumstances can cause disruption of operations, security issues and failure to comply with regulatory requirements.

NETWRIX SOLUTION

Before deploying Netwrix Auditor, the IT team used a different software solution to monitor AD changes. While the tool was working fine for that purpose, it had a very limited functionality, which over time turned out to be insufficient to support the agency's complex IT infrastructure. Jeff Williams, Systems Integration Branch Chief in the National Weather Service Southern Region, explained the choice to switch to Netwrix Auditor: "The reason we chose Netwrix Auditor is that it is all in one. It monitors all the required systems and has extensive functionality for validation of all our security controls. It is very good in everything." With Netwrix Auditor in place, the NWS Southern Region has gained the following benefits:

Increased system uptime. Because of the widely distributed nature of the IT organization and the 24/7 uptime requirement, one of the top priorities for Jeff's team is to ensure ongoing system availability by monitoring system changes. Any change, such as the incorrect configuration or deletion of an OU, can affect system performance. Thanks to the detailed reports and alerts from Netwrix Auditor, the team has managed to reduce the number of IT incidents and troubleshoot the remaining issues faster, thus ensuring system uptime.

Centralized control over the entire IT environment. Because the agency has so many domain admins working in local offices, keeping up with all changes used to be a problem; it was easy to miss a potentially harmful action or an incorrect setting that could affect the entire domain. Now, Netwrix Auditor's alerts on critical changes enable the team to revert any unwanted change in a few minutes, before any damage is done. Jeff reviews summary reports of all changes daily to make sure that security policies are followed correctly and that nobody outside the domain admins group gets elevated privileges.

Continuous compliance and efficient audits. Netwrix Auditor's alerts and daily email notifications summarizing all changes make it easy to validate internal security controls and ensure continuous compliance with NIST. The IT team has regular data calls, both for spot checks and to respond to auditors' requests. In addition to automated reports, Netwrix Auditor includes an Interactive Search that enables the IT team to quickly find any requested information, such as changes to Group Policy, the domain administrator group or file servers, or details about a specific user action. And the solution's predefined reports mapped to the FISMA/NIST standard save the team a week or more of work preparing for the full annual audit.

KEY BENEFITS

- Centralized control over the IT environment
- Business continuity
- Control over privileged users
- Easy compliance with NIST and internal security requirements

[Learn more about Netwrix Auditor](#)

It is not an easy task to keep up with all the changes in an IT environment as distributed as ours. Yet Netwrix Auditor does the job in a very simple and efficient way. We use it for the most part to satisfy internal security controls and for audit purposes. Regardless of how complex the auditors' or security team's requests are, with Netwrix Auditor, we can just run a report and make it very simple. Netwrix Auditor saves us about 40-60 hours on preparation for each audit and even more in our daily work. But most importantly, we know that our environment is secure.

Jeff Williams,
Systems Integration Branch Chief,
National Weather Service Southern Region