

State Grid Shanghai Municipal Electrical Power Company

Sentinel Enterprise drastically strengthens security through tight integration with NetIQ Identity Manager, boosting productivity and saving costs.



Overview

State Grid Shanghai Municipal Electrical Power Company (SGCC) produces and distributes power from coal, gas, integrated gasification combined cycle (IGCC), wind, and solar. The company was founded in 1985 and is based in Shanghai, China. Shanghai Municipal Electric Power Co., Ltd. operates as a subsidiary of State Grid Corporation of China.

Challenge

SGCC has been a long-time user of [NetIQ Identity Manager](#) by OpenText and [NetIQ Access Manager](#) by OpenText to provide a unified identity solution for its 34,000 users. In recent years security has become

“With the introduction of [NetIQ] Sentinel Enterprise we were able to reduce our IT security staff from five to just two. Having the security data at our fingertips means we can respond 80 percent faster to any security breaches, and we have reduced our overall security incidents by 50 percent.”

Mr Lu Shida
Director
State Grid Shanghai Municipal Electrical Power Company

a more serious issue, with criminals actively harvesting information from data breaches, leading to revenue losses.

Although SGCC had a security system in place to protect its business systems and unified identity systems, the solution wasn't satisfactory, as Mr Lu Shida, Director at SGCC, explains: "We couldn't report on our data in a centralized manner, all the data was separated into different systems. That meant that when we found a security threat, our security administrators would need to examine the logs for each business system. This would take too much time; time in which a security breach could do untold damage to our business. This manual and time-consuming process meant we couldn't meet our compliance regulations and were being charged penalties."

SGCC needed a solution to help quickly identify data breaches and data theft. It also needed support in highlighting account password breaches and auditing so-called 'zombie' accounts; accounts which aren't in active use, but which could pose a security risk. As an existing NetIQ Identity Manager and NetIQ Access Manager customer, it was vital that the security solution integrates with the unified identity solution.



At a Glance

Industry

Energy and Utilities

Location

China

Challenge

Replace a manual and time-consuming security solution which left SGCC exposed to non-compliance and resulting penalties. The new solution needed to be tightly integrated with an existing Micro Focus unified identity system, managing 34,000 users, and provide sophisticated reporting and auditing capabilities.

Products and Services

NetIQ Sentinel Enterprise
NetIQ Identity Manager
NetIQ Access Manager

Success Highlights

- Reduced IT security personnel from five to two
- Improved security incident response time by 80 percent
- Reduced security incidents by 50 percent
- Reduced security-related revenue losses by 90 percent
- Enhanced compliance, monitoring, and auditing capabilities

“The native integration between [NetIQ] Sentinel Enterprise and our Micro Focus (now part of OpenText) unified identity system allowed us to introduce many more security features without having to change our system architecture.”

Mr Lu Shida
Director
State Grid Shanghai Municipal Electrical Power Company

Solution

SGCC investigated the market to look for an agile, scalable, and high performance security solution which could be integrated with the NetIQ Identity Manager and NetIQ Access Manager system. SGCC evaluated NetIQ Sentinel Enterprise, along with EMC eVision and IBM QRadar. EMC was discounted as the software is typically bundled in with EMC hardware; it doesn't contain an auditing and reporting module, which was important to SGCC; and proved an expensive option. Though the IBM solution was of interest, SGCC was concerned about the lack of IBM support services in China and its ability to help deliver the project.

Mr Lu Shida comments on the decision for NetIQ Sentinel Enterprise: “The native integration between [NetIQ] Sentinel and our Micro Focus (now part of OpenText) unified identity system allowed us to introduce many more security features without having to change our system architecture. The [NetIQ] Sentinel components are scalable and can easily be extended to meet any future needs we might have. The [NetIQ] Sentinel implementation was easy and we were quickly up and running.”

The solution creates daily reports for key application systems and it audits users who have bypassed the unified identity system

so that alerts are sent to the security team. Quarterly, the system generates a report to highlight accounts which haven't been used, so that these 'zombie' accounts can be closed down.

With 34,000 users to manage, understanding the “who, what, when, where, and how” of user system access is essential for controlling insider-based risks. NetIQ Sentinel Enterprise integrates security data with unique user identity information to help SGCC quickly identify risky access behaviors. To support SGCC's compliance position, NetIQ Sentinel Enterprise simplifies the collection of security events to automate compliance audit and reporting functions and significantly reduce the complexity, time, and costs of locating and preparing data required by auditors.

Results

Security has strengthened the entire SGCC infrastructure, while security management and labor costs are reduced, as explained by Mr Lu Shida: “With the introduction of [NetIQ] Sentinel we were able to reduce our IT security staff from five to just two. Having the security data at our fingertips means we can respond 80 percent faster to any security breaches, and we have reduced our overall security incidents by 50 percent. This has led to a 90 percent reduction in economic losses caused by security breaches.”

Connect with Us
www.opentext.com



He concludes: “With the [NetIQ] Sentinel implementation, ensuring we are always security-compliant is so much simpler. Through the clear and transparent system, we can quickly identify and respond to any security threats. Monitoring and auditing is easy and through the vital integration between the solutions we can manage our 'zombie' accounts and have a deep understanding of user access rights for every application we run. Micro Focus (now part of OpenText) has supported us throughout this process and we look forward to our continued partnership.”

About NetIQ

NetIQ provides security solutions that help organizations with workforce and consumer identity and access management at enterprise-scale. By providing secure access, effective governance, scalable automation, and actionable insight, NetIQ customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the NetIQ homepage at www.cyberres.com/netiq to learn more. Watch video demos on our NetIQ Unplugged YouTube channel at www.youtube.com/c/NetIQUnplugged.

NetIQ is part of Cybersecurity, an OpenText™ line of business.

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.