MICRO FOCUS

Case Study

Security

Datang Xianyi Technology

Because Datang Xianyi supports a wide range of systems, identifying issues in logs and troubleshooting their cause was very difficult. Micro Focus® helped Datang Xianyi create a central point of control for monitoring and resolving security issues, helped improve reporting, and increased employee productivity in security monitoring management by 60 percent.

Overview

Datang Xianyi is an IT service provider for the Chinese electric power industry. As a subsidiary of Datang Huayin—one of the largest power producers in Hunan Province—Datang Xianyi plays a vital role in the lives of millions of people.

Challenge

The Datang Xianyi Technology Co., Ltd (DTXY) System Maintenance Team manages its parent company's IT infrastructure, and maintains systems control and automation software in the group's power plants.

With numerous physical servers and network devices supporting a range of business systems, it was a challenge for DTXY to monitor and resolve security issues. The systems generated logs in a variety of formats scattered across the network, and IT didn't have a central point of control. This made identifying and defending against threats difficult and time-consuming.

Existing approaches to security were largely reactive, and DTXY could not always diagnose problems and determine improvements, even after significant effort.

DTXY manages some critical systems that support operations in its parent company's power plants. Proving network security was a top priority, and pressure was growing on DTXY to improve its security management.

Solution

After comparing and testing security management solutions from HP and IBM, DTXY selected NetIQ® Sentinel™ Enterprise for its internal network. The solution covers DTXY's principal systems, including Oracle databases, and provides an aggregated view of the security status in real time.

"We recognized that the growing maturity of information security management products made it the right time to find a third-party solution," said Qiang Zhang, IT Engineer at DTXY. Sentinel Enterprise was the best product DTXY tested in terms of data aggregation and

"...Sentinel had the right functionality for our requirements, and it was the best of the products we tested..."

QIANG ZHANG

IT Engineer, IT Operations and Data Center Maintenance
Datang Xianyi Technology Co., Ltd

At a Glance

- **Industry**
  Software & Technology
- **Location**
  China
- **Challenge**
  The systems generated logs in a variety of formats scattered across the network and IT didn't have a central point of control. This made identifying and defending against threats difficult and time consuming.
- **Products and Services**
  Sentinel Enterprise
- **Results**
  + Provided flexible reporting
  + Reduced operational costs by cutting workload
  + Improved employee productivity in security management by 60 percent

> **"We can then rapidly respond to the alerts it creates when it spots the targeted events—and we know precisely what action to take."**
>
> **QIANG ZHANG**
> IT Engineer, IT Operations and Data Center Maintenance
> Datang Xianyi Technology Co., Ltd

ease of use. "It was especially good for Oracle error log collection, for which the format is quite specialized."

Using Sentinel Enterprise, IT staff can easily check a variety of automatically generated reports daily and use them to analyze system security and error reports. With DTXY's previous approach to security management, there was simply no way to do all these tasks with the limited size of the team.

"In the past, we would have to search through a number of different logs to diagnose a problem," said Zhang. "Not only did this mean lots of manual work, but often we would not be able to identify the root cause or do anything to avoid it happening again." Sentinel Enterprise simplified security management so the IT team could improve the quality of its service to the business.

By aggregating logs from across the network and monitoring traffic, Sentinel Enterprise enables DTXY to focus on higher-level issues. The software uses a rules engine to generate alerts based on targeted issues or patterns of behavior, flagging potential risks for resolution. The automation offered by Sentinel Enterprise has enabled DTXY to shrink its security team to four people working in rotation.

Results

With Sentinel Enterprise, DTXY can now manage security threats rather than responding after the event.

According to Zhang, security reporting is nearly effortless, but still provides a more detailed and accurate picture than DTXY had before. DTXY no longer needs to keep a close eye on the logs; the team simply sets policies and controls in Sentinel Enterprise. "We can then rapidly respond to the alerts it creates when it spots the targeted events—and we know precisely what action to take."

By providing a central dashboard with automated alerts for pre-defined events, Sentinel Enterprise has enabled a small team at DTXY to be confident in its security measures. The solution provides flexibility in reporting, helping the team provide the necessary data and statistics for audit purposes. It also reduces operational costs by cutting workload.

DTXY estimates that Sentinel Enterprise has improved employee productivity in security management by 60 percent.

"Power generation for millions of people is dependent on the information systems we manage, so maintaining high levels of security is vital," said Zhang. Sentinel Enterprise enabled DTXY to identify and resolve threats in real time, and provide auditable reports to prove that the network is secure.