



XYGATE Access Control Identifies Illusive User Activity

Keystroke logging is more than PCI-DSS compliance - it saves time, money, and reputation



Company

Client is a credit card processor and issuer based in the United States. They provide payment processing services to many financial institutes, thousands of businesses, and millions of consumers in over eighty countries.

All over the world, millions of payments are accepted every hour of every day. Their vision is “to be the leading global payment solutions provider to those we serve – our clients, our shareholders and our team members.”

Background

Before this credit card processor began utilizing XYPRO software solutions and services, they had a manual checkout process for privileged account ids. In it a Tech Support Manager would manually process requests and release privileged account credentials for approved requests. This process was not only inefficient, but diluted accountability for the actions of those privileged IDs. Once the password was released, there was no way to track which commands were executed under that privileged ID. Additionally, if multiple people were using the privileged ID at the same time, there was no way to distinguish who executed each command. After implementing XYPRO’s XYGATE Access Control (XAC), not only was their process streamlined but it also increased security and accountability with capabilities like easily configurable access controls and keystroke logging, all while still providing their users with the privileged access needed to do their jobs.

Problem

In early 2018, the client encountered issues during a major system upgrade which impacted their business operations as well as those of several external customers. After they were unable to restore normal operations, the systems upgrade was stopped and reverted back to its previous state. Hours were spent attempting to resolve the issues and more time was spent attempting to identify the root cause. It wasn’t until the next day that the root cause was discovered.

Solution

An XAC keystroke log report determined that the problem was caused by human error. A technical team member had mistakenly executed an erroneous command, which impacted system communications. The client declared that “without the XAC keystroke log report, we may have never discovered the root cause.” Armed with the root cause, the company was able to inform impacted customers and reassure them that they had taken steps to make sure this type of outage unlikely to occur again. Additionally, the company created training to educate employees about proper privileged account id usage.

“THE XAC KEYSTROKE REPORT SAVED COUNTLESS HOURS OF RESEARCH TO DETERMINE THE ROOT CAUSE OF OUR ISSUE.”

- Spokesperson, Payments Processor

Product at a glance:

XYGATE Access Control (XAC)

- Enable Role Based Access Control (RBAC)
- Control the use of commands and subcommands
- Eliminate shared user IDs
- Keystroke logging for individual accountability
- Restrict Access by IP and Port
- Secure both Guardian and OSS operating systems
- Comply with PCI-DSS and other regulatory standards



Learn more at
www.XYPRO.com

XYPRO Headquarters, USA
4100 Guardian St., Suite 100
Simi Valley, California 93063 USA

USA/Canada: sales@xypro.com
Asia Pacific: apsales@xypro.com
EMEA: emeasales@xypro.com
Ibero America: iberosales@xypro.com
Japan: apsales@xypro.com



The Need for Keystroke Logging

Administrative users hold the keys to vital information on your systems. They have the power to take action with the highest privileges on the most sensitive areas of your HPE NonStop server. To ensure no damage has been inflicted either maliciously or inadvertently by user error, PCI DSS Requirement 10.2.2 and other compliance frameworks require that all actions taken by any user with administrative privileges must be tracked.

XYGATE Access Control comes packaged with keystroke logging functionality, ready to turn on, out of the box. The keystroke log report lists all the activities of each user making it easy to be in compliance. These data-rich logs can also be forwarded to an enterprise Security Event Incident Manager (SIEM) through XYGATE Merged Audit to for compliance with PCI DSS Requirement 10.2.2.

About XYPRO

XYPRO Technology Corporation is a leader in protecting mission-critical systems for the banking, financial services and payments processing industries. As specialists in the HPE NonStop server, XYPRO closely partners with HPE to enhance NonStop server security and compliance. XYPRO's XYGATE suite of security solutions provides Data Protection, PCI Compliance and Audit Reporting, Access Control, Database Management, and more.