Product Spotlight

Ensure Business Continuity

Introduction

In today's digital world, laboratory-based businesses are required to provide correct results promptly and must be operational 24 hours a day, 7 days a week. This requires continuous, uninterrupted operation regardless of any internal (e.g. network outage, server failure) or external (e.g. power outage, construction, natural disaster) events. Unfortunately, it is becoming more prevalent for these companies to also undergo cyberattacks that can hack data and shut down the operations of a function or even an entire company.

A Business Continuity Plan (BCP) is a vital part of these business' strategy to ensure continuous, uninterrupted operation, regardless of any man-made or natural events, and with increasing reliance on digital data systems it has never been more important to ensure that your laboratory data systems are protected against the repercussions of a disaster.

Thermo Scientific™ Chromeleon™ 7 CDS delivers resilience to your business, ensuring compliance with zero-loss data security and continuous operation. Its resilient architecture provides flexibility, scalability, and robustness in relation to both data security and business continuity, giving protection from any unplanned downtime and safeguarding against ransomware attacks from hackers.

ThermoFisher SCIENTIFIC

Preventing unauthorized access

Unauthorized access to data and software, unintentionally or purposefully, can cause severe damage to the software installation, potentially resulting in inoperable software, data corruption or even data loss. To prevent this, controlled access to the software and data is key. Multiple security layers, in order of increasing security, prevent unauthorized access (Figure 1). These ensure that the security of raw data in the Data Vault is at the highest level possible while maintaining appropriate access to tools and data.

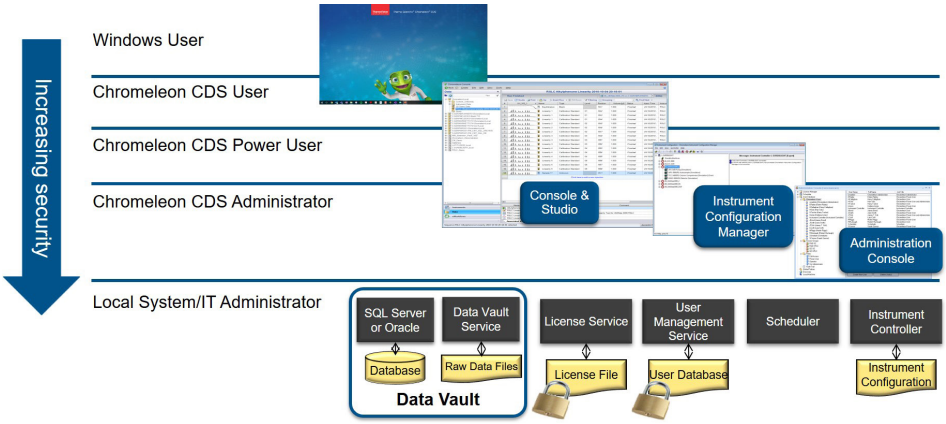

Figure 1. Security layers in the Chromeleon software installation.

- **Operating system:** Access to Chromeleon software starts with controlling access to the Operating System (OS), typically Microsoft® Windows®. User access can be limited to only running Chromeleon CDS without the ability to modify the operating system or computer where the CDS is installed.
- **Chromeleon user management:** Chromeleon CDS provides its own user management system beyond the Windows user management, that allows granular control over user access and privileges within the software. Typical examples of user types with an increasing level of privileges that would be created include:
  - **User:** Provides everyday access to the Chromeleon Console and Chromatography Studio in order to run, process and report data.
  - **Power user:** Higher level users who are more highly trained may be given more access with additional privileges, for example, to configure instruments or reports within the system.
  - **CDS administrators:** The highest level Chromeleon users, who can have access to some of the configuration tools in the Administration Console where they can setup and control the Chromeleon software. These users are typically based in IT rather than in the laboratory to ensure separation of roles.
- **Services:** With its modular architecture, all communication and processes of Chromeleon CDS are handled through Windows services, including deployment and updates. Only IT administrators can view these underlying services and components, ensuring users cannot access key system components of the CDS. These services use the local Windows account, eliminating the need for administrator-level ‘service accounts’ for databases, clients or file shares that must be registered with the Windows domain. This drastically reduces security risks due to malware attacks.

Network failure protection

Ensuring business continuity and preventing data loss or corruption during a network outage (e.g. server failure or network loss) is key to maintaining laboratory operations, data integrity and compliance. Chromeleon software provides unique, industry-leading Network Failure Protection (NFP) functionality to deliver 24/7 uptime in two key ways:

- Network-based resources required to properly operate the software — such as license information and user management data — are automatically cached on local instrument controllers and client computers ensuring software operation can be continued, as a 7 day recovery period is automatically enabled, allowing time for the issue to be resolved or for a longer-term solution to be implemented.

- Chromeleon software's unique XVault™ technology ensures continuous operation and data security. During data acquisition, sequences are always run in the XVault, present on each local instrument controller, and the acquired data is synchronized centrally. In case of network failure, NFP mode is automatically enabled and data acquisition continues, with the data stored on the local computer. While in NFP mode, the data interrupted during acquisition can be accessed via the XVault for processing, and reporting, and new sequences can be started — all in accordance with compliance and data integrity guidelines. After network recovery, the interrupted data (including full audit trails) is automatically uploaded and synchronized to the central server. Additionally, any new sequences initiated while in NFP mode can be uploaded within the Chromeleon Client, ensuring data integrity and compliance.

Built-in load balancing and failover protection

While load-balancing (sharing workload between two or more servers) and failover (automated switching between servers should one fail) is often handled by IT, Chromeleon CDS does provide its own load balancing and failover for the Data Vault Service, which handles the data exchange between the Data Vaults and the Chromeleon Client. Load balancing allows distribution of workloads across multiple computing resources, usually servers (Figure 2). In case a server fails or is taken offline for maintenance, the other server(s) simply take over, keeping the system online. This increases reliability through redundancy and, in addition, provides a capability for server maintenance.

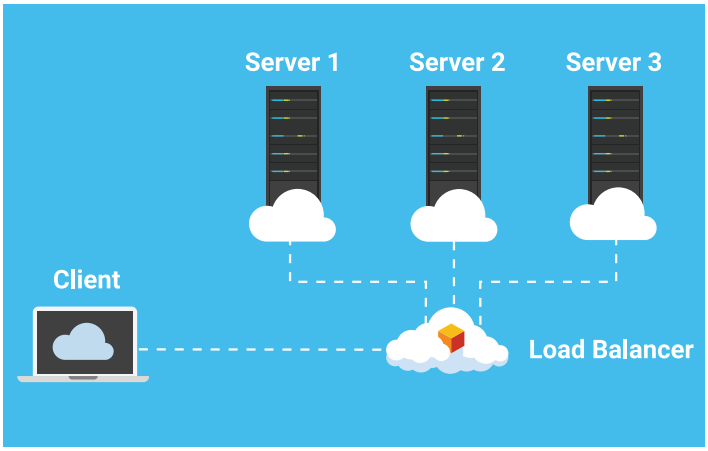

Figure 2. Load balancing setup to increase performance and reliability.

Secure instrument control

To control instruments and acquire data in an enterprise Chromeleon CDS environment, it is strongly recommended to attach them to an instrument controller device, rather than connecting them directly to the network for data security, NFP, and business continuity reasons. The Thermo Scientific™ 247 Instrument Controller (247 IC) is such a device, developed specifically for the security and uptime needs of chromatographic instruments in a Chromeleon CDS network (Figure 3).

The 247 IC uses an ultra-secure embedded Windows Long-Term Service Channel operating system with all external media and malicious or unsigned software blocked. It is designed specifically for connecting instruments to Chromeleon 7 CDS and does not require connection to the Windows domain, ensuring it is invisible to malicious software attacks and removing the need for virus protection or regular Windows security updates.

thermo scientific

Figure 3. 247 instrument controller.

As an ultra-low maintenance device, the 247 IC provides increased security, a lifetime of up to ten years, and reduction of maintenance costs by up to 90% compared to a standard Windows PC. Administration of the 247 Instrument Controller is straightforward and can be automated from any remote location.

Support and maintenance agreement

A support and maintenance agreement (SMA) or service level agreement (SLA) is an important part of a BCP. It will secure your Chromeleon CDS installation with several key benefits to maximize and future-proof your investment, increase productivity and minimize the risk of business interruption.

The SMA includes technical support provided by dedicated Thermo Fisher Scientific professionals, who offer professional investigation and issue resolution via follow-the-sun methodology and exclusive access to various resolution resources. In addition, product updates are included, both for Long Term Support releases — enabling utmost stability and robustness over an extended period with minimized validation efforts — and Feature releases — to stay up to date with the newest technologies and latest advancements.

Conclusion

With intelligent tools to prevent unauthorized access, ensure 24/7 uptime and built-in load balancing and failover protection, Chromeleon CDS provides confidence for the enterprise and ensures business continuity.

Find out more at **thermofisher.com/chromeleon**

ThermoFisher SCIENTIFIC