A Locked Door Is No Longer Enough:

Protect Your Mainframe at the Console Level.

i/O CONCEPTS

SOLUTION DATASHEET

While the mainframe is typically considered an inherently secure environment, with limited access behind locked doors, mainframe system consoles are often overlooked when it comes to security.

Today, IT needs flexibility and the ability to access and manage their systems from anywhere, at anytime. This has resulted in greater exposure of the mainframe system consoles to the network and the security risks have multiplied. Yet, mainframe console security measures haven't increased as rapidly as the risks have—and confidence in console security is often misplaced—resulting in risk gaps that can threaten the security of your critical information assets.

Security gaps in console access could permit not only destructive actions against the hardware and operating systems, but also allow administrative access to all data on the mainframe. And it won't be long before auditors start paying more attention to these mainframe security and compliance issues.

ioEnterprise solutions can provide secure and auditable access—even remotely—to the mainframe console environment. This enables security departments to put the necessary controls on the mainframe consoles to meet the company's compliance requirements and avoid damage to, or exposure of, their mainframe systems.

DO YOU KNOW?

Are your mainframe system consoles:
1) secure,
2) remotely accessible, and
3) auditable?

I/O Concepts can help you answer these questions and find the right solution for your data centers.

Here's how ioEnterprise solutions close the risk gaps in mainframe system console security:

- **Secure remote and local access of consoles with *ioEnterprise CCS, CCS+* and *Automation***
- **Implement authentication control and command suppression**
- **Gain visibility into activity with complete audit trails**
- **Meet the security standards for regulatory compliance with *ioEnterprise Audit Manager***
- **Secure access and monitoring of the HMC with *ioEnterprise Secure HMC***

Completely Controlled Console Authentication

Access and share consoles both locally and remotely with multi-layered user authentication, with strengthened password rules

The mainstay tools of mainframe authentication, such as LDAP, RACF, ACF2 and Top Secret, manage access to mainframe-specific data and applications. Yet few organizations control console access with these tools because they are difficult to implement and have a negative impact (even when properly configured) to operator productivity. These tools also are limited to only prohibiting changes to the console; console messages are still visible without authentication. These conditions usually result in consoles that are exposed and vulnerable to threats.

The ioEnterprise Console Consolidation and Security (CCS) solution adds a layer of security to console access that mitigates these risks, yet does not interfere with the console itself. ioEnterprise CCS provides the ability to customize authorization and session access. The authentication can be made against an internal database of usernames and passwords or against a centralized authentication repository like LDAP, RACF, ACF2, Active Directory, RSA (Radius), and Top Secret.

Secure Remote Access

Secure console data with SSL encryption when connecting remotely over the internet

System console access is often extended to both public and private networks, as enterprises increasingly require access to these business-critical resources from anywhere, and at any time. This effectively removes the locked door and potentially exposes the mainframe to anyone who can access a network traversed by a remote console protocol.

Configured specifically for the purpose of secure mainframe console access, ioEnterprise CCS in effect acts as the mainframe console's firewall. These console connections across the internet are secured using SSL encryptions, allowing your staff to access host systems safely from networks inside and outside the enterprise. This optimizes workforce flexibility, increases your data center's workload potential, and maximizes the return on personnel investment. Combined with ioEnterprise's authentication and access controls, mainframe system consoles can be confidently protected against threats in a wide variety of networked environments.

Granular Control and Visibility

Customizable permissions for role-based user access and command suppression

Once connected to a console via ioEnterprise, console images are delivered based on security policies, such as read-only consoles that provide console visibility without the risk of unauthorized console access or use, command restriction, and customizable permissions. This allows proactive measures to be used to minimize and mitigate the danger of malicious or accidental access on production systems.

Customizable permissions limit access to sessions based on user name, user group, where the user is located, and/or any other system variables (like time of day). Role-based command suppression tools assure that users enter only authorized commands.

All user interactions with host systems are tracked by the ioEnterprise Audit Manager and managed in a data store. This provides a complete record of who does what, when, and from where, what commands individuals are entering, and more. Internally, audit information helps troubleshoot the root causes of inadvertent errors. It can also act as forensic evidence of malicious activity in the event of a security breach, and protects the integrity of trustworthy professionals by documenting responsible actions.

Audit trails for addressing compliance regulations—every message that the systems generate and a complete record of user activities and commands issued

Remove Regulatory Compliance Gaps with Audit Trails and Reporting

Failure to address the security risk gaps in the mainframe environment can expose the enterprise to regulatory penalties. Considering the mainframe's critical role in managing sensitive information, auditors and security officers are becoming more aware of the issues that threaten the mainframe.

PCI, SOX, Cobit, and HIPAA rules require accurate details of user interactions with host systems. ioEnterprise CCS implements the required security measures needed to meet these regulations, and ioEnterprise Audit Manager maintains audit trails for all activities to provide the necessary reporting for these regulations.

Secure remote and local access to the HMC with ioEnterprise authentication and encryption

Secure Access and Monitoring of the HMC

ioEnterprise Secure HMC provides secure local and remote access to the HMC. Since the HMC is the command entry point from some of the most basic commands to boot, IML/IPL, and configure the mainframe, access to the HMC is critical. Yet, keeping staff on-site near the HMC can be problematic in lights-out or remote data center operations. Also, since some very important information is generated by the HMC, having that information integrated into the overall mainframe operations is desirable for security purposes. Securing the access to the HMC from malicious or even accidental access is critical and ioEnterprise Secure HMC provides for this by requiring unique login IDs, auditing user access, and encrypting data across networks.

So, Are Your Mainframe System Consoles Secure, Remotely Accessible, and Auditable?

If you have a mainframe, the risk gaps in console security outlined above likely mean that your data centers aren't as secure as they should be. And most executives and risk managers aren't aware that these risks even exist. The ioEnterprise solution offers a proactive set of tools for addressing these issues, behind the locked door as well as in any network, public or private—before they become the subject of opportunistic attack, unintentional operator error, or a compliance defect report. In addition, these solutions are designed to dramatically enhance efficiency, accountability, and workload potential of data center operations staff while they are protecting your mainframe at the console level.

Manframe console security, consolidation, and event management solutions for enterprise data centers.

i/O CONCEPTS

About I/O Concepts

I/O Concepts helps today's networked enterprise implement expert management and security solutions for their mainframe and midrange systems in order to facilitate more efficient, responsive, accessible and protected data center operations.

Since 1989, I/O Concepts has been providing expert solutions to help IT operations consolidate, secure and remotely access and monitor their mainframe and midrange data centers. The ioEnterprise solutions from I/O Concepts allows companies to protect their mainframe environment at the console level, consolidate data centers across the world, and more effectively monitor the mainframe/midrange environment with integrated event management, secure remote access and automation tools.

I/O Concepts is headquartered in Bellevue, WA and supports IT operations for some of the largest companies in the world. ioEnterprise solutions can be implemented quickly and I/O Concepts consistently provides its customers immediate and identifiable cost savings and productivity enhancements. Learn more at www.ioconcepts.com.

To learn more about I/O Concepts ioEnterprise solutions for the mainframe, contact an I/O Concepts representative at info@ioconcepts.com or visit www.ioconcepts.com to download a free whitepaper, "Closing The Four Security Risk Gaps of Mainframe Console Access."

ioEnterprise products from I/O Concepts include a complete suite of tools to help manage and secure the mainframe/midrange data center environment: ioEnterprise Console Consolidation and Security (CCS), ioEnterprise CCS+, ioEnterprise Automation, ioEnterprise Event Manager, ioEnterprise Audit Manager, ioEnterprise Secure HMC.

2125 112th Avenue NE, Suite 201
Bellevue, Washington 98004

TEL (425) 450-0650

FAX (425) 450-0614

info@ioconcepts.com

www.ioconcepts.com