

Why Choose eConnect® Electronic Access Control (EAC) from Chatsworth Products?

Traditional cabinet-based networked locking solutions are expensive and can be challenging to deploy and use. Chatsworth Products' (CPI) eConnect® Electronic Access Control (EAC) solution is an economical, effective and easy-to-use networked locking solution for data center cabinets that works with CPI's eConnect Power Distribution Units (PDUs). This integrated solution enables remote programming, monitoring and control of every cabinet—limiting physical access to information systems and equipment—and preventing data and identity theft.

Benefits of eConnect EAC:

- Provides a completely integrated, easy-to-use and deploy networked solution at a savings of 50% or higher over traditional solutions
- Integrates cabinet- and device-level power management, environmental monitoring and access control, removing the need to power and network the locks separately
- Works with most employee badges to easily manage access rights
- Extends monitoring to the cabinet- and device-level for more granular reporting and better decision making
- A built-in audit trail helps ensure regulatory compliance and meets requirements, such as PCI DSS, HIPAA and FIMSA.
- Compatible with Power IQ® for eConnect (DCIM)

Additional Savings from eConnect Secure Array® IP Consolidation

CPI's eConnect EAC works with eConnect PDUs to provide integrated power management and cabinet access control using a single network connection, one user interface and one user database, which provides additional deployment savings. You can link up to 32 PDUs, 32 locks and 64 environmental monitoring sensors using one IP address!

For more information on eConnect EAC, visit

www.chatsworth.com/econnect-electronic-access-control.



CHATSWORTH PRODUCTS

Prevent Data Breaches and Ensure Regulatory Compliance

More stringent cybersecurity frameworks are requiring closely controlled access to personal data.

CPI eConnect EAC is the first line of defense for data centers' data protection and security policies, providing audit capabilities and detailed reports of who and when the cabinet is accessed. For enhanced security, add dual-factor authentication with Zwiipe® biometric cards.

Prominent Regulations

✓ **FISMA - Federal Information Security Modernization Act**

- Physical access must be managed and protected.
- Remote access and access permissions are managed.

✓ **HIPAA - Health Insurance Portability and Accountability Act**

- Physical access to electronic information systems and the facility or facilities in which they are housed is limited.
- Access attempts, dates and reason for access must be documented.

✓ **PCI DSS - Payment Card Industry Data Security Standard**

- Use appropriate facility-entry controls to limit and monitor physical access to systems where data is stored.
- Use a visitor log to maintain a physical audit trail of visitor information and activity.

✓ **GDPR - General Data Protection Regulation**

- Demonstrate examples of preventing unauthorized access to electronic communications networks.

✓ **SaaS SOC 2® - System and Organization Control (SOC)**

- User identification, authentication, authorization and credentials management must be documented.
- Operating location and data center physical security and environmental safeguards must be in place.



CHATSWORTH PRODUCTS

US & Canada

+1-800-834-4969
Toronto, Ontario, Canada
+905-850-7770
chatsworth.com

Latin America

+52-55-5203-7525
Toll Free within Mexico
01-800-01-7592
chatsworth.com.co

Europe

+44-1628-524-834
chatsworth.com

Middle East & Africa

Dubai, UAE
+971-4-2602125
chatsworth.ae

Asia Pacific

+86 21 6880-0266
chatsworth.com.cn