TECHNICAL INFORMATION

Cyber Security Features

ZELLA DC

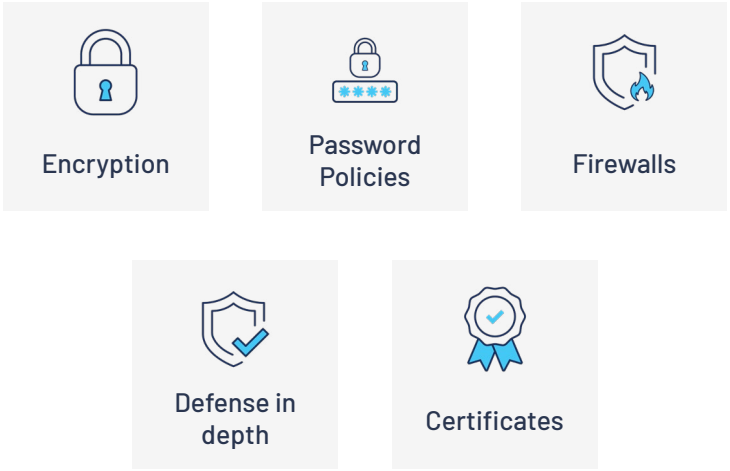
Cyber Security

The rapid growth of digital data has put immense pressure on data centers. That's why at Zella DC, security is top of mind.

Our intelligent micro data centres are equipped with latest cyber security protocols as well as advanced security features designed to keep your data and your assets protected by physical attacks.

Whether your micro data centre is located indoors (i.e. in an office) or outdoors (i.e. on a mine site or a farm), our security features have been designed to protect your uptime.

Get in touch if you have any further questions about our products or to find out about our products' cyber security features.



Encryption

As Zella DCs are connected to management networks and even to the production networks, it is critical that any and all data sent or received by the Zella DCs are encrypted. We only enable secure encrypted communication by default — HTTPS and SSH. We use the strongest encryption in the industry as in:

HTTPS connections use TLS 1.0/ 1.1/ 1.2 with AES 128/ 256-bit ciphers supporting the widest range of browsers.

SSH connections use public key authentication where password authentication is not adequate or feasible, like in scripts.

SNMP v3 connections are encrypted with MD5 or SHA authentication protocols and DES or AES privacy protocols.

StartTLS implementation ensures encrypted transport of user credentials from the PDU to the remote authentication server.

Besides being a secure server, the PDU is also secure client when dealing with remote authentication servers using TLS for OpenLDAP and active directory as well as CHAP for RADIUS communication.

Password Policies

With all the security measures available and implemented, passwords remain the most critical component of security. We provide several ways to ensure passwords are strong and current:

Strong passwords require a minimum of eight characters with lower case, upper case, numerals and special characters while forbidding the past three passwords.

Force password change ensures that the default password gets changed after the first-time login as default passwords are the easiest way hackers take control of connected devices.

Password expiration ensures passwords getting refreshed periodically, preventing hackers from accessing the Zella DCs from any known security breaches.

Firewall

Zella DCs are accessed over the network for various reasons ranging from simple data collection to critical alert notifications, and even power control. With systems and users needing access from various segments of the corporate network, it is critical to keep unauthorized access completely out through the following means:

IP-Based Access Control Lists (IP ACL) rules determine whether to accept or discard traffic to/from the PDUs, based on the IP address of the host sending or receiving the traffic.

Role-Based Access Control (RBAC) rules act similar to IP access control rules which allow access to PDUs based on the roles of individual users.

Defense in Depth

Zella DCs play a critical role in managing the power infrastructure and servers, using the PDU's remote power control functionality. Therefore, it is essential to protect against network breaches. We have implemented several security measures that keep the Zella DC PDUs one step ahead of these threats:

Blocking access after repeated failed login attempts to defend against potential Distributed Denial of Service (DDoS) attacks and logging the source of the attempts.

Timing out inactive sessions to prevent unauthorized access.

Limiting the use of the same login credential from multiple clients.

Enforcing restricted service agreement warnings and requiring that users accept them to login.

Certificates

X.509 digital certificates ensure that both parties in a secure connection (TLS) are authorized users. As Zella DCs are increasingly accessed over public networks, having valid certificates protect against man-in-the-middle attacks. In order to make this process as efficient as possible, Zella DC PDUs support two major types of certificates:

CA certificates that are issued and signed by public certificated signing authorities after thorough verification of the user's business; the PDU interface even generates the certificate signing request for submission to signing authorities such as Verisign, Digicert and more Self-signed certificates when a CA certificate is not deemed necessary; the PDU also provides an interface to generate a self-signed certificate.

ZELLA DC

Your data centre, your way

About Zella DC

Over a decade ago Zella DC pioneered the micro data centre. Since then, our next-generation server room in a box have been proven to work in the harshest environments on earth. The result is a vendor-agnostic approach to software, hardware manufactured to global standards, and partners across six continents.

Unit 17, 386 Scarborough Beach Road
Osborne Park, 6017
Western Australia

www.zelladc.com
Info@zelladc.com
+61 8 6311 2814