VERTIV.

Solution guide

Vertiv™ Next Connect Security

Product security is integrated

Product Security is integral to Vertiv's product development process.

- Product Security is integrated into Vertiv's overall New Product Development and Introduction (NPDI) process to assist all new products are developed with security in mind.
- All new products are expected to meet Vertiv's SECURE requirements. These requirements have been derived from multiple industry security certifications as well as industry best practices.
- At different phases of new product development, security related risks are evaluated against Vertiv's SECURE requirements, and changes are suggested or mandated depending on the level of risk. This process includes static and dynamic testing of code and binaries.

Cloud native architecture

Vertiv™ Next Connect is a cloud-native platform designed for managing and monitoring IT physical infrastructure.

- In the cloud-enabled approach, you're able to apply cloud-based security capabilities for more effectiveness and use cloud intelligence to improve your threat detection and response time.
- Connect benefits from Microsoft's security leadership and expertise through partnerships on architecture and design review, as well as benefiting from the hardened architecture of Azure PaaS to get the latest fixes as soon as Microsoft publishes them.
- This approach helps that customers consistently operate on the latest version of the Vertiv Next Connect software, equipped with Vertiv's most recent security patches.
- By staying up-to-date, organizations can proactively mitigate vulnerability risks to their critical infrastructure.

Built on Microsoft Azure

Vertiv™ Next Connect is built on the Microsoft Azure Cloud Platform. The Azure Cloud platform is used Globally in a wide range of industries and applications such as Energy, Finance and Banking, Healthcare, and Government applications.

- Built using the Microsoft Azure IoT Edge suite.
- Microsoft's cloud features continuous monitoring, making it harder for attackers to breach security. This proactive approach helps identify and tackle threats in real-time, assisting a safer environment for users and their data.
- Azure adheres to security controls for ISO 27001, ISO 27018, SOC 1, SOC 2, SOC 3, FedRAMP, HITRUST, MTCS, IRAP and ENS. Azure compliance available at Azure Compliance.

> "Microsoft runs on trust, and our success depends on earning and maintaining it. We have a unique opportunity and responsibility to build the most secure and trusted platform that the world innovates upon."
>
> **— Satya Nedella,**
> *Chairman and CEO of Microsoft*

Utilizes end to end data encryption

With Vertiv™ Next Connect your Data is encrypted while at rest, in transit, and during use. This end-to-end encryption protects data from unauthorized use and provide data integrity and confidentiality.

- While in transit data is encrypted using Transport Layer Security (TLS) protocol to protect your data.
- Authorization and authentication are done using x.509 CA Certificates. Each agent holds a unique secret as the basis for trust.
- While at rest TDE is used to encrypt data files in real time, using a Database Encryption Key (DEK). TDE protects data and log files, using AES and Triple Data Encryption Standard (3DES) encryption algorithms.

Identity management and authorization

Vertiv™ Next Connect follows industry standards for managing user registration, authentication, and authorization.

- To provide the validity of the user, each user is registered by invite using a registration email.
- Vertiv Next Connect has implemented password complexity and user lockout guidelines to prevent brute force attacks.
- User capabilities are managed individually and are limited to their specific tenant and can be further restricted to specific entities within the platform.

Key takeaways

1. Product security is a crucial part of Vertiv's development process, ensuring that all new products meet strict SECURE requirements based on industry certifications and best practices.
2. Vertiv Next Connect features a cloud-native architecture that enhances security through the use of cloud-based capabilities and intelligence, which improve threat detection and response times.
3. Built on Microsoft Azure, Vertiv Next Connect benefits from continuous monitoring, providing ongoing protection against potential security breaches.
4. Your data is encrypted using Transport Layer Security (TLS) during transmission and Transparent Data Encryption (TDE) when at rest, provide strong protection through real-time encryption. This guarantees the security of your information both while it is being transmitted and when it is stored.
5. Vertiv Next Connect also provides secure user management through industry-standard registration, authentication, and authorization processes. This is further strengthened by password complexity requirements, user lockout policies, and Multi-Factor Authentication (MFA).