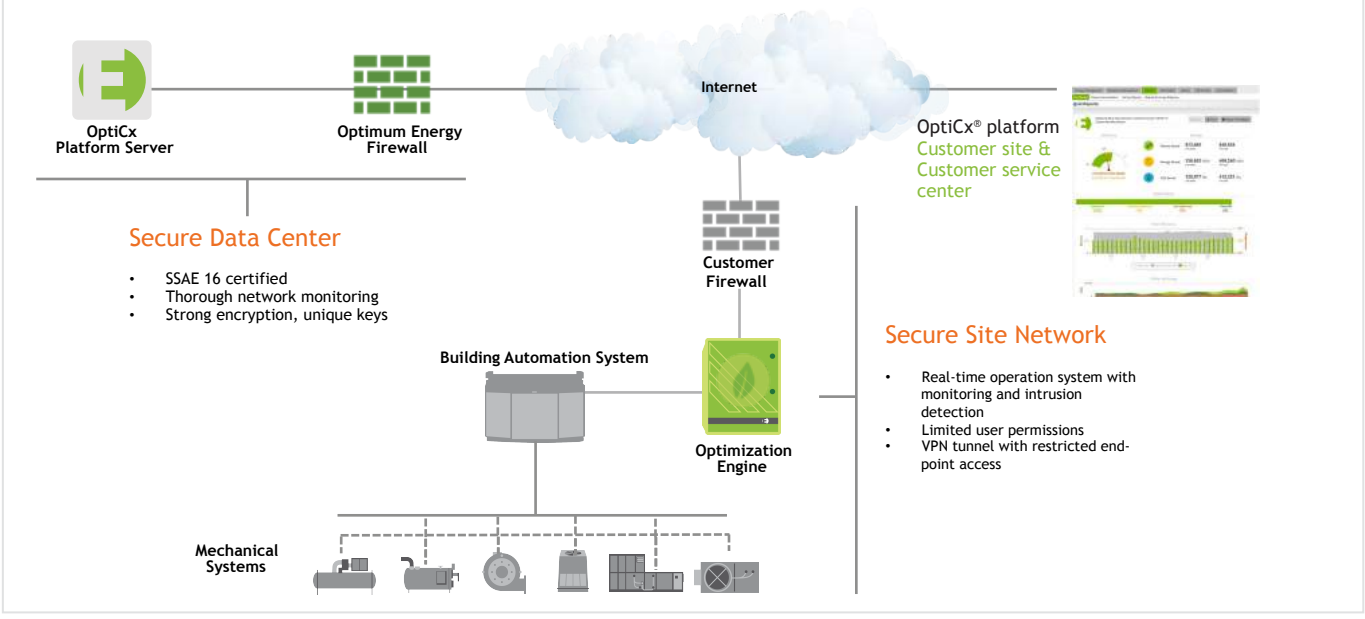
OptiCx® Platform Infrastructure Security Overview

As a leading provider of energy optimization solutions for facilities, security is paramount at Optimum Energy. Our data-driven solution, the OptiCx platform, safely and reliably delivers ongoing energy efficiency results for our customers. This document describes our network infrastructure and the security provisions that are at the core of our delivery model.

Our Commitment to Security

- The OptiCx platform uses strong encryption with unique keys. Our use of access controls ensures that we can access only the data needed to perform energy management and optimization services.
- We comply with customer security operating procedures and best practices.
- We strongly advocate that customers implement robust security separations between networks used for Building Automation System (BAS) sensors and monitoring, and those used to transact business and financial information
- The OptiCx platform is protected by anti-virus software.
- We follow industry best practices to secure our on-premise and cloud-based software and hardware.
- We earned SSAE-16 certification based on implementation of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

The OptiCx® platform: Rigorous end-to-end security



Server Physical Security

OptiCx® platform servers are hosted in a physically secure data center that has received the Statement on Standards for Attestation Engagements (SSAE) 16 certification. The data center is above-ground, preventing ground-level forced entry, and staffed 24x7, with card key access control and continuously monitored video camera feeds for all entry points and interior spaces. The data center has fully redundant UPS and power conditioning and full backup power generation capability. It includes automated fail-over HVAC systems and multi-zone fire suppression systems equipped with optical sensors, heat sensors, smoke detectors, automatic fire department notification, HVAC system controls and dry-pipe sprinklers.

Server Network Topology

Reliability is ensured through redundant systems for power and networking. Multiple tier-one fiber providers facilitate robust network access through diverse building entry points, with circuits terminating at four separate physical locations. Twin chassis are populated with multiple routers and switches in a fully meshed architecture. Each chassis has two power supplies, each connected to dedicated power circuits. The network is connected to multiple upstream providers.

Network security is maintained through close monitoring and best practices with packet and protocol filtering. Filters are maintained on the boundary routers to ensure basic network protection. Thorough monitoring of bandwidth and flow data — in both real-time and with historical data — is used to detect network anomalies.

Access to the server site is restricted to separate VPN tunnels for Optimum Energy operations personnel through firewalls using non-standard ports. Access is limited to designated operations personnel and authentication occurs via strong passwords that are frequently changed.

OptiCx platform security key points:

- Strong encryption with unique keys
- 100% compliance with customer security operating procedures
- Implementation of NIST Critical Infrastructure Cybersecurity Framework
- Secure data center for cloud operations

Building Site Network Access

Our on-site optimization engine uses the Tridium Niagara AX Platform, an industry standard in building system integration. The Niagara AX platform provides a secure networking environment for a wide range of building integration functions, in addition to scalability and cross-platform integration with the BAS. The optimization engine runs a real-time operating system that minimizes intrusion opportunities. The Niagara security model provides a layered set of functions for securing network connectivity, along with secure authentication classes and methods for communication between Niagara devices. These devices include the building appliance and the server to which it is networked. For a detailed discussion of the Niagara AX security model and the security functions it provides, see the Tridium Niagara AX Networking and IT Guide (2006). The OptiCx platform complies with all Niagara AX Security Best Practices including strong passwords, lockout features, and limited user permissions.

During our installation process, the building site is networked to the OptiCx platform server site described above, and monitoring with intrusion detection is included. The physical network connection may be via wireless broadband data, DSL, cable or other service. Static IP addresses are used for building site connections. When a physical connection is established, an IPSec Virtual Private Network (VPN) tunnel is configured between the OptiCx platform server site firewall and the firewall serving the building site. The VPN tunnel is configured to restrict end-point access to only the specific devices defined at either end. End-point access is restricted based on both IP address and port.