Whitepaper

Cloud + Data Center Transformation Support Services

Applications and security framework

Executive summary

For Insight Cloud + Data Center Transformation (CDCT), securing client environments and data are top priorities. As threats grow in number and complexity, we believe it has never been a better time to approach security as a pervasive component of every project, with every client. It is simply no longer appropriate to tack-on security as a single consideration or an afterthought.

In our pursuit to provide security leadership and proactive strategies, we share this framework to inform interested parties of our services and how they work. Primarily, we achieve our security objectives through applications and specific services like penetration testing and vulnerability scanning.

We are firm believers that digital transformation encompasses people, process, and technology — the same can be said for security. Through our numerous solutions, we aim to empower people, improve process, and strengthen and evolve technologies in order to build a security program that withstands immediate and unforeseen threats.

Table of contents

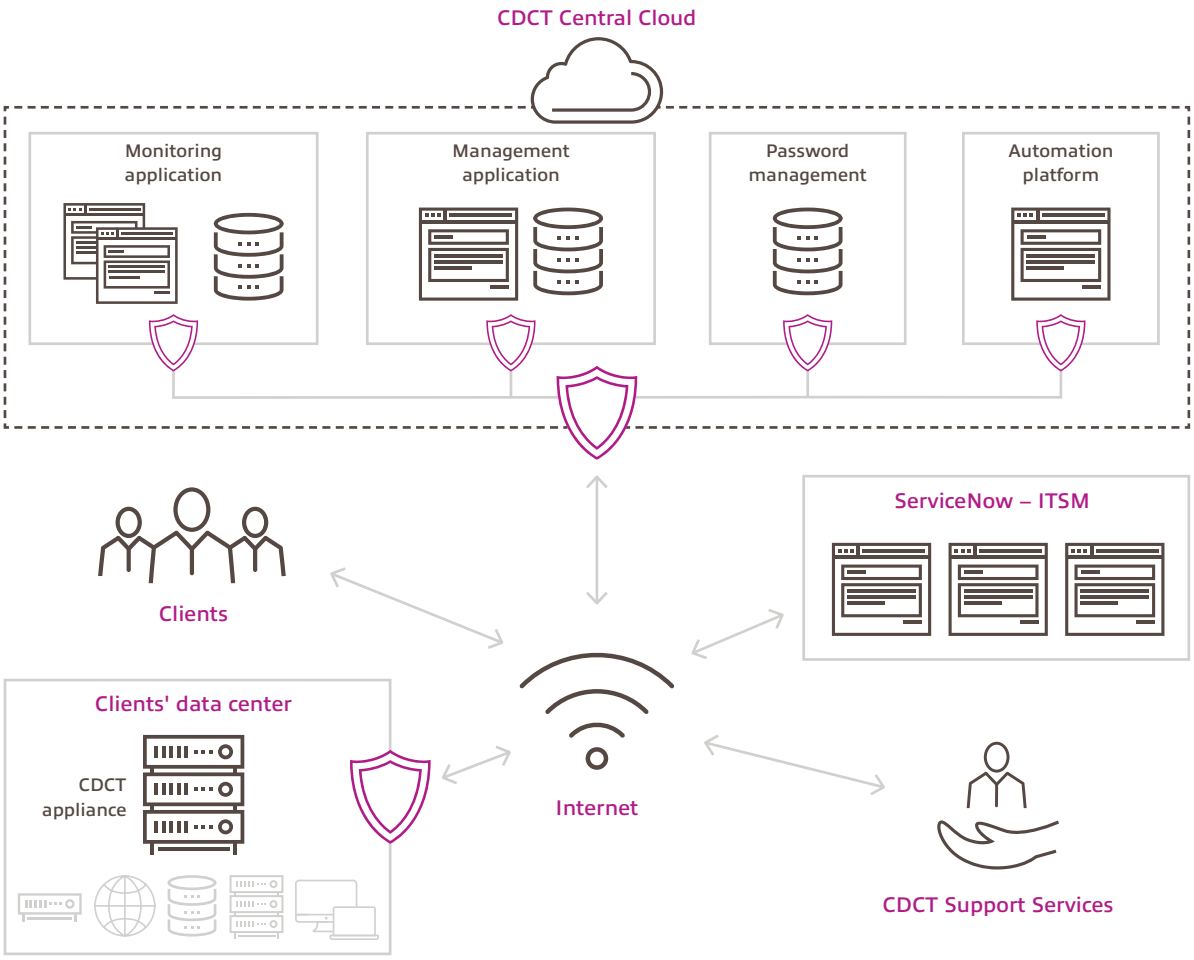
Introduction

CDCT Support Services are mainly comprised of applications and security solutions. Here, we will review four major applications — monitoring, management, password management, and automation. We then share details about our various security services.

Though our perspective here will be more narrowed than broad, we invite interested readers to explore our other materials that provide glimpses into the methods, strategies, and best practices we employ to support our clients in their transformation journeys.

CDCT applications

We run four primary applications to manage and monitor an environment. Each application has a different architecture, infrastructure, and set of requirements. We use a monitoring application, a management application, a password management application, and an automation platform. How each application performs within our services ecosystem is shown in the chart below. Specific capabilities are detailed in the following written sections.



Monitoring application

The monitoring application discovers and models resources in your environment, immediately creating an asset-service relationship context. Resource Manager, together with plugins, provides advanced performance and availability monitoring, event management, notification, and escalations in a single, intuitive, web-based interface.

The monitoring application is a fully agentless solution that provides unified monitoring without the deployment and maintenance overhead associated with agents. As a Manager of Managers (MOM), it can aggregate events from many different tools, allowing you to view events from throughout your entire environment on a single console.

Communication security

The monitoring application calls home via a secure, encrypted connection. This connection is used to send all monitoring data and events to the core monitoring servers for processing. It is important to note this connection is not used to manage client devices.

An SSL session is established with bidirectional authentication (i.e. each side of the connection must present its own certificate). If the SSL/TLS authentication succeeds, encryption/decryption and hash message authentication code (HMAC) key source material is then randomly generated and exchanged over the SSL/TLS connection from both sides of the connection. This mode never uses any key bidirectionally, so each peer has a distinct send HMAC, receive HMAC, packet encrypt, and packet decrypt key. The actual keys are generated from the random source material using the TLS pseudorandom function (PRF). During SSL/TLS rekeying, there is a transition-window parameter that permits overlap between old and new key usage, so there is no time pressure or latency bottleneck during SSL/TLS renegotiations.

We multiplex the SSL/TLS session used for authentication and key exchange with the actual, encrypted, tunnel data stream. This provides the SSL/TLS connection with a reliable transport layer, as it is designed to operate over. The actual IP packets, after being encrypted and signed with an HMAC, are tunneled over UDP without any reliability layer. No IP packets are tunneled over a reliable transport, eliminating the problem of reliability-layer collisions.

Docker containers

In recent years, evolving software development practices have fundamentally changed applications. These changes have impacted the underlying infrastructure, tools, and processes needed to properly manage applications throughout the lifecycle. Applications transformed from large monolithic code bases to collections of many small services, loosely assembled together into what is now called a microservices architecture.

These new applications not only behave differently, but their architecture consequently changes how they are built, deployed, managed, and secured over time. Instead of provisioning large servers to process a few large workloads in virtual machines (VM) or bare metal, collections of small applications are being run across a collection of commodity hardware. With applications sharing the same operating system (OS), containers have risen as the model for packaging these new applications. Fewer OS instances provide significant benefits to the application infrastructure with respect to host resources, costs, and ongoing maintenance. Application security best practices have long recommended layers in order to increase the overall resilience of a system.

Containers provide an additional layer of protection by:

- Isolating the applications and the host
- Working between the applications, themselves, without using incremental resources of the underlying infrastructure
- Reducing the surface area of the host

Containers and virtual machines (VMs) can be deployed together to provide additional layers of isolation and security for application services. Containers facilitate simple applications of patches and updates to the OS, application, and infrastructure layers, and help maintain security compliance.

How CDCT monitors devices

While not a complete list, here we share several ways that we monitor devices and environments.

+ WinRM – Windows®

  Microsoft's Windows Remote Management (WinRM) is used to monitor Windows devices. WinRM is the Microsoft implementation of WS-Management Protocol, a SOAP-based, firewall-friendly protocol that allows for interoperability of hardware and operating systems from different vendors. To allow for WinRM monitoring, a group policy needs to be pushed.

  Apart from WMI, WinRM uses the Intelligent Platform Management Interface (IPMI) driver for hardware management. The IPMI provider and driver enable a user to control and diagnose remote server hardware through Baseboard Management Controllers (BMCs), even when the OS is not running or deployed. Effectively, a BMC is a chip connected to the processor board of a server; it has its own network adapter and can monitor the server in situations even when the server is malfunctioning.

+ SNMP – (Network, Linux®, Unix®, etc)

  SNMP is an internet-standard protocol for collecting and organizing information about managed devices on IP networks. Devices that typically support SNMP include: routers, switches, servers, workstations, printers, and more.

  SNMP is used to monitor devices that support the protocol, by itself or in conjunction with other protocols like an application program interface (API). We may leverage SNMP v1, v2c, or v3, depending on the device support and needs.

  Two considerations to note: SNMPv1 does not support 64-bit SNMP MIBs; and SNMPv3 requires unique Engine IDs to function, which may present issues in some environments with older versions of software code or where cloning is used.

+ API – (VMware, Cisco, NetApp, etc)

  An API is a set of routines, protocols, and tools for building software applications. An API specifies how software components should interact, and is used when programming Graphical User Interface (GUI) components. A good API makes program developing easier by providing all the building blocks — a programmer simply needs to put the blocks together. We'll use the vendor's native APIs, at times, to monitor different systems.

+ SSH – (Linux, Unix)

  SSH is a cryptographic network protocol for operating network services securely over an unsecured network. SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server. This is used for some devices that do not support SNMP. These devices tend to be older versions of the server OS.

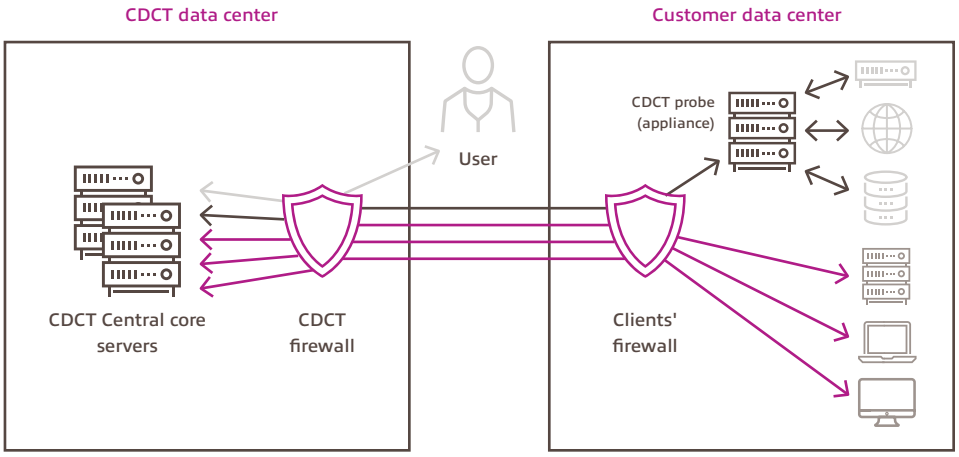
Management application

This application is used for:

+ Remote device management
+ Patch management
+ Asset reporting, including but not limited to:
  - Software inventory
  - Patch-level reporting
  - Hardware warranties

CDCT Central is a service provided by CDCT that is used to manage an environment. To understand what impacts it may have on the security of managed networks, it is helpful to learn the components and design of this service.

CDCT Central consists of three major components: probes, agents and CDCT Central core servers.



Probes and agents

A probe is a software component that resides on a system within a client's network, behind their firewall, or within their private IP space. Probes provide monitoring and management services for devices on that private network by leveraging industry standard protocols such as Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), Open Database Connectivity (ODBC), and others.

An agent is an additional software component that may be installed on a Microsoft, Mac® OS X®, or Linux host device in order to gather data specific to that local device. Agents are typically installed on all Windows devices to provide full capabilities regardless of the logical placement of that device on the internet.

Probe and agent communications

Probes and agents communicate with the CDCT Central core server using similar architecture and methods. They leverage client-side, initiated communications, where all data communications begin with an outbound call from the agent or probe.

As a direct result of this architecture, no public IP address, nor port forwarding from the internet to the devices running the probes or agents, is required. Outbound communications from agents to the CDCT Central core server are based on Simple Object Access Protocol (SOAP) and Extensible Messaging and Presence Protocol (XMPP), and are transmitted using the HTTPS protocols on the standard web ports. The nature of these communications allows for the support of standard proxies on the local network.

After the outbound session is established, the agent receives an identifying session ID that is applicable until the session is closed. Agents and probes then open a second (asynchronous) signaling channel leveraging the XMPP protocol (on port 443) to allow the CDCT Central core server to signal agents and probes when actions are necessary (such as to initiate a remote control session). If the XMPP session is terminated abnormally, for example, by a firewall cleaning open sessions, the agent automatically re-creates the session. CDCT Central leverages the XMPP-based communications for control purposes only, not for the transmission of monitored data.

By default, the CDCT Central agent, probe, and XMPP-based communications use HTTPS, TLS-encrypted data, and the strongest cipher suite supported by both the client and the server.

Probe as a cache

The CDCT Central probe also acts as a cache location for software installation files such as the agent, AV Defender, and Windows patches. Agents communicate with the probe over TCP 10004 using the .NET remote communication protocol.

CDCT Central core servers

Our core servers are the "brains" of the system. As such, they contain a number of components, including: the web interface, the administrator console (AC), the data management system (DMS), the database, and other core system components. In addition to providing an interface for the agents and probes, the DMS is also the business logic layer of the application. All rules that govern how CDCT Central deals with data are executed at this level. All physical data — configuration or monitored — is stored within the relational PostgreSQL database.

CDCT Central core servers are designed and secured in a restricted internet zone, such as a DMZ, and include an integrated firewall to secure the system from unwanted network traffic.

The system is built using industry standard best practices including:

- One-way encryption of stored user passwords
- Input-type checking
- User access permissions
- Protective support for cross-site scripting (XSS) attacks

Remote control

One of the key features provided by CDCT Central is remote control of any managed device. Because remote control leverages the location of the CDCT Central server on the internet and the outbound communications model provided by agents and probes, it works regardless of the user's location on the internet.

CDCT Central uses several methods to establish encrypted connections from CDCT Central core servers to the remote control target device. DirectConnect and Attended Remote Control sessions use NTR Global, agentless cloud technology while other remote control types use connections established through one of the following protocols:

+ Secure Shell (SSH)
+ HTTPS
+ User Datagram Protocol (UDP)

The NTR Global cloud technology used by DirectConnect and Attended Remote Control sessions provides multilevel security to protect every point in the remote connection path. Data communication is maintained securely and privately using ISO 27001-certified data centers and a global network of relays that complies with regional Safe Harbor policies and strict international regulations including the Sarbanes-Oxley (SOX) Act, the Health Insurance Portability and Accountability Act (HIPAA), and others mandated for specific industries.

Note: The following ports must be accessible to use DirectConnect or Attended Remote Control for remote control connections:

	CDCT Central		Target Device	
	Inbound traffic	Outbound traffic	Inbound traffic	Outbound traffic
Port 443	✓	✓	✓	✓
Port 11438	✗	✗	✗	✓

For remote control types other than DirectConnect and Attended Remote Control, the first protocol attempted will be an SSH tunnel (TCP on port 22). Should the SSH connection attempt fail, the requesting user and the target system will again attempt to connect to each other through the CDCT Central server using HTTPS on port 443.

After the requesting user and the target system are connected, the remote control tools can then communicate over this encrypted connection as if they were located on the same network subnet. Since the remote control session is outbound from both the user's system and from the device to be remotely controlled, no public IP address nor inbound port forward is required.

Remote control in CDCT Central uses several layers of security. The outbound request model ensures that no inbound ports are required.

Data passed through UDP connections is encrypted using an Advanced Encryption Standard (AES) symmetric algorithm (CDCT Central supports both 128-bit and 256-bit encryption). A new encryption key is generated for every remote control connection, and old encryption keys are never recycled. Both the target device and the CDCT Central core server have to authenticate with each other and exchange encryption keys using a secure channel before the remote control session can begin.

Data passed through SSH connections is encrypted using 128-bit AES-based encryption keys. Data passed through HTTPS connections uses HTTP in combination with Secure Socket Layer (SSL) and Transport Layer Security (TLS). SSL and TLS are cryptographic protocols that provide secure communications on the internet. HTTPS is designed for secure, encrypted communication between different devices as well as secure identification and authentication of the remote device.

No matter which of the three protocols is used, a user name and password are needed in order to access the remote device.

Remote control auditing
For each remote access, the requesting user, target device (managed or unmanaged), and session time are logged. Logs are reviewed by our practice manager and are shared with the client as requested. Clients may also initiate and run access reports at any time via the CDCT portal.

Secondary remote access
It's impossible to manage physical appliances using the primary remote access, as this action requires the appliance itself. In the event there is an issue with the appliance, we will require remote access to manage the appliance and as a backup connection.

Password management

Audit reports
Two types of audit reports are used: the user audit report and the secret audit report.

+ The user audit report

  The user audit report enables CDCT to easily assess vulnerability when someone exits the client company. This tool records all actions a user makes on what's called a secret. Actions include creating, updating, sharing, etc. We can obtain a relevant report of every secret a specific user accessed, simply by selecting a user and date range. Each secret can then be expired, instantly decreasing the likelihood of a security breach. The user audit report is also helpful in reviewing for appropriate secret use.

+ The secret audit report

  Whereas the user audit report focuses on the user, the secret audit report provides accurate details on the secrets themselves. Users can protect sensitive information by monitoring the level of activity on any of their accessible secrets.

Database encryption
We use AES 256-bit for encrypting data in the SQL database. AES-256 encryption — the Rijndael algorithm is approved by the U.S. Government and was declared for use by NIST after a 5-year standardization process. AES-256 is the strongest encryption available for password protection software.

Login protection
All connections to the password management tool are made via a SSL connection using TLSv1.1 or higher.

We hash and salt user login passwords using a randomly generated salt and the SHA-512 hashing algorithm. While SHA-1 is secure, given the compute power of modern technologies, it is not as secure as previously thought.

To further tighten security, a username and password is required with every login request, which incorporates authentication against Active Directory® and enforces two-factor authentication.

+ SHA-512 hashing algorithm

  User passwords are hashed in the database using the SHA-512 hashing function. A hash function differs from an encryption method in that a hash function, when used correctly, is computationally infeasible to reverse.

  Hashing algorithms are mathematical functions that convert inputted text values to a hash digest. Even the smallest change of the input text produces radically different hashed values. This guarantees that if two users choose the same password, their hash value in the database will not be the same.

  Hashing is an essential security requirement to ensure that authentication credentials are not exposed. We also use random salts and multiple hash iterations to prevent brute-forcing or the use of rainbow tables.

Password requirements

Our security policy and best practices dictate the password requirements for passwords entered into the database.

We have enabled the following password-related functions:

- Secure passwords can be automatically generated when creating a secret by using template settings.
- Templates can be configured to use specific characters and password length to create strong passwords.
- Password history can be enabled to keep a full history of all previous passwords.

The "copy to clipboard" and automatic, password-changing functions make it feasible to have 100-character, randomly generated passwords. This improves security, as long, complex passwords are tedious to write down or type.

Password requirements can be set for different variations of characters and symbols, for example: two uppercase letters, two lowercase letters, etc.

Password compliance reports help track and enforce requirements on passwords when they are generated, added, or edited.

+ Role based access control (RBAC)

  We use RBAC so that each role is designated an appropriate set of permissions. Every user and group is assigned to one or more roles within the password management tool. RBAC ensures strict, granular access to sensitive information.

Password Heartbeat

Password Heartbeat gives an effective, in-time way to monitor credentials across all of our clients. This helps to ensure we are able to respond to any event in a timely manner.

Heartbeat automatically tests a secret's credentials at set intervals and alerts administrators if credentials are changed outside of the password management tool. Heartbeat also signals when an administrator changes a privileged password.

Expire secrets

Any secret template can be set to expire within a fixed-time interval. For a secret to expire, a field must be selected as the target for interval changing. For example, a secret template for Active Directory accounts might require a change on the password field every 90 days. If the password remains unchanged past the length of time specified, that secret is considered expired and will appear on the expired secrets dialogue on the home page.

Secret expiration provides additional security by reminding users when sensitive data requires review. This can also be useful for meeting compliance requirements that mandate certain passwords be changed on a regular basis. When expiration is combined with remote password changing, we can completely automate the process of regularly changing entire sets of passwords to meet security needs.

Request access

Access to sensitive secrets are managed with request access. When this feature is applied, users must request access to a secret, from a predetermined approval list of groups/users. An email is sent to everyone on the list notifying them of the request, which can then be approved or denied by any of the members. Access will be granted for a set time period as determined by the approver.

All requests, approvals, and denials are fully audited. The user can enter a reason with their request to explain the need for the password. The reason field can also be used to enter a tracking number from a change control or task management system.

CDCT appliance

Physical appliance

The CDCT appliance requires a 1U section of a server rack. The appliance has dual hot-plug 350W power supplies capable of handling a 120V – 240V power source. The appliance uses two network connections; one will be used to monitor the environment and the second connection is for management. Both connections are set up to fail over to the other Network Interface Controller (NIC) in the event of a failure. The appliance builds a secure tunnel back to CDCT to send metadata for analytics and alerting. It is expected that this tunnel will use between 0.063KB/s – 0.126KB/s for outbound traffic and between 0.001KB/s – 0.002KB/s for inbound traffic per device being monitored.

What runs on the appliance?

The CDCT appliance runs ESXi and hosts virtual appliances (standard is four virtual appliances). These virtual appliances have the capabilities of monitoring and managing an environment. Each virtual appliance runs a hardened version of either CentOS® or Windows Server®.

Appliance security

We use two principal methods for securing the appliance. The first approach is prevention; by hardening the appliance, the risk of the appliance becoming compromised is reduced. The second method is detection; by employing a host-based intrusion detection system, we can be alerted to changes being made to the appliance.

Device hardening

The hardening process guidelines are:

- Disable unnecessary service
- Enforce a strong password policy
- Limit access to privileged accounts
- Restrict root access to the console (CentOS) only
- Allow remote access only via secure connections

Host-based intrusion detection system (HIDS)

In the case where an intrusion has been detected, CDCT is immediately alerted and will investigate the alert. HIDS offers: a powerful correlation and analysis engine, log analysis integration, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting, and active response.

CDCT security

Security is an ever-changing and always critical component of an IT organization. We consistently adapt existing security services, add new ones, and stay current on ways to be proactive in this field. Below are a number of our specific security offerings that bring our clients peace of mind.

Security incident response

A security incident response team responds to client security concerns. Calls are received 24/7/365 on the Support Services Security main phone line at 952.260.5715.

Role based access control (RBAC)

CDCT Support Services ensures role based access control (RBAC). This means that users are assigned privileges based on job classification or function, not per specific employee demand, request, or preference.

SIEM

Our security solution offers around-the-clock protection. Through manual and automated daily log analysis, our security team proactively detects suspicious activity in the environment and coordinates course-corrections. The team is also ready 24/7/365 to field client security calls.

Vulnerability scanning

Regular vulnerability scans are performed — internally and externally — on the operating system, web application, and databases in the environment using a variety of tools. Also, our security teams subscribe to newsfeeds, monitor vendor websites, and review other relevant sources to stay constantly abreast of potential vendor flaws and new patches.

Penetration testing

Penetration tests conducted by carefully selected industry experts are performed on the environment on a regular basis. In fact, such testing is part of our security risk assessment review that begins during the design phase.

Network security

Our network provides significant protection against traditional network security issues such as:

+ Edge firewalls

  Edge firewalls protect from Denial of Service (DoS) attacks, including distributed, flooding, and software/logic attacks. The networks are multi-homed across a number of providers to achieve internet-access diversity. When unauthorized port scanning is detected, it is stopped and blocked from reoccurring.

+ Advance threat protection

  Advance threat protection (ATP) combines multiple technologies to identify and block outgoing traffic to command-and-control hosts. Clients have the option to conjoin ATP with web protection to improve protection through cloud-based, selective sandboxing.

+ Web application firewalls

  Web application firewalls protect our web servers and apps. Reverse proxy authentication provides an added layer of security for enterprise applications. This helps to prevent hacking from Structured Query Language (SQL) injection, cross-site scripting, directory traversal, cookie tampering, and much more.

+ Firewalls

  In addition to outside-facing firewalls, every server is equipped with a firewall with dedicated rule sets. Rules only allow necessary, internal and external, traffic to a server. Rule sets are regularly reviewed to ensure only required firewall rules are in place. When a change is needed, it must go through a formal change management review process.

+ Web protection

  The latest web threats are blocked using advanced techniques like JavaScrip® emulation and Live Protection cloud lookups, which detect malicious web code before it even reaches the browser. Web protection also prevents infected systems from calling home with sensitive data. Our engine inspects all Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol, Secure (HTTPS), and File Transfer Protocol (FTP) traffic, including active content like Active X, Flash®, cookies, VBScript, Java®, and JavaScript.

Physical security

CDCT's state-of-the-art data centers use innovative architectural and engineering approaches developed from many years of experience designing, constructing, and operating large-scale infrastructure. Our data centers are housed in nondescript facilities where physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff, video surveillance, intrusion detection systems, and other electronic means.

Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Access to the data center and the information is only provided to employees and contractors who have a legitimate business need for such privileges. All visitors and contractors are required to present identification and are signed in and escorted by authorized staff. When an employee no longer has a business need for access privileges, such privileges are immediately revoked. All physical access to data centers by employees is logged and routinely audited.

Storage devices
When a storage device has reached the end of its useful life, we follow techniques detailed in NIST 800-88 *Guidelines for Media Sanitization* to properly decommission the device and prevent client data from exposure and unauthorized usage.

Security awareness training
All CDCT Support Services engineers and contractors go through security awareness training upon hire and annually thereafter to provide a deepening, foundational platform of knowledge. Training is a series of modules — each module covers a specific human risk or compliance requirement and concludes with a quiz to measure learner comprehension.

CDCT availability
Our infrastructure is designed to tolerate system or hardware failures with minimal client impact, through a high level of availability and resilient IT architectures.

Data centers are built in clusters and are online — no data center is "cold." In the case of failure, automated processes move client data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

In the case of a regional event, we can fail all operations to geographically separated data centers, each located more than 2,000 miles apart in order to extensively safeguard operations.

Each data center uses state-of-the-art technology to ensure ultimate availability. This includes, but is not limited to:

+ Fire detection and suppression
  Automatic fire detection and suppression equipment is installed to reduce risk.
+ Power
  Data center electrical power systems are designed to be fully redundant and can undergo maintenance without impact to operations. Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility. Generators offer backup power for the entire facility.
+ Climate and temperature
  In order to avoid overheating and possible service outages, data centers are climate-controlled. Atmospheric conditions are kept at optimal levels for server and hardware performance.

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at:
insightCDCT.com | insight.com