Dell goes beyond Internet security in its commitment to guard against physical breaches, malicious activity and other risks that may cause concern when you extend your network into an external facility. We share your desire for keeping sensitive content secure, and we share the responsibility for securing your information. You can rest assured knowing that the Dell Connected Configuration service is designed to keep your data protected.

The security of the Dell Connected Configuration service has been validated using the same intelligence-driven SecureWorks solutions we offer to customers as part of our enterprise security portfolio. A world leader in security solutions, SecureWorks has provided trusted managed security services to organizations of all sizes since 1999 – and today serves thousands of clients all over the world.
Isolating Customer Data in the Deployment Environment

The idea of extending your network into an external facility may lead to questions about how your data is protected in that environment. This is why the Dell Connected Configuration service incorporates security best practices and protocols designed to isolate your organization’s extended network and protect your data there. These practices and protocols include:

- Managing Hyper-V host access through Active Directory group policies, with regular reviews of access lists, and implementing stringent processes for access provisioning based on least-privilege, minimum-requirement standards.
- Assigning a virtual local area network (VLAN) for each organization that can be connected to only via secure tunnel, has no capability for intercommunication with other organizations and is controlled entirely at the hypervisor level.
- Rigorously segregating the specific preassigned deployment burn-in locations when connecting to the Dell Connected Configuration service appliance.
- Validating Hyper-V and VLAN security measures through SecureWorks Hyper-V assessment testing and network segmentation reporting.

“The Dell Connected Configuration service incorporates security best practices and protocols designed to isolate your organization’s extended network and protect your data there.”
Protection against Data Breaches

With new threats to the security and integrity of data emerging all the time, Dell is committed to maintaining constant vigilance and acting swiftly and effectively to detect and thwart these threats. Our commitment is backed by technology and expertise from SecureWorks, which offers unparalleled visibility to identify potential threats in critical areas of IT infrastructures, along with actionable, intelligence-driven insights powered by advanced analytics. Specific steps we take to defend against data breaches include:

- Incorporating enterprise-grade firewall hardware into each Dell Connected Configuration service appliance.
- Employing security experts who test the effectiveness of our security by making attempts to break into the secured environment.
- Automatically checking on a weekly basis for software patches from Microsoft and applying patches to protect against hacking through operating system (OS) or other software.
- Frequently and regularly conducting analytics of the environment to address new threats that may emerge.
- Validating the security of the service environment through SecureWorks.

“SecureWorks is a leading global provider of intelligence-driven information security solutions focused on protecting organizations from cyberattacks.”
Physical Barriers to Entering Service Facilities

Dell’s commitment to security includes measures to prevent improper physical access to any Dell Connected Configuration service facility and the hardware within it. These environments are operated as secure-access production environments and maintained accordingly. Our practices and protocols include:

- Maintaining an onsite staff of security personnel as well as 24x7 camera monitoring.
- Allowing access to the facility only via badge or access card, or in the company of an escort with a badge or access card, and forbidding anyone to leave the facility with hardware of any kind.
- Requiring all employees and visitors to go through a secured entry and/or exit equipped with a metal detector and staffed by security personnel.
- Vetting of all staff members by Dell Security or a contracted technical services provider.
- Employing a process to protect customers who provide content on physical media (rather than by file transfer) that includes retrieving the content from the drive, moving it to a secure server in a customer virtual domain, securing the physical media in a locked cabinet and returning the drive to the customer.
- Regularly carrying out audits on the physical security of facilities.

“Dell’s commitment to security includes a robust set of measures aimed at preventing improper physical access to any Dell Connected Configuration service facility.”

Doing Our Part to Keep Your Most Sensitive Data Secure

The lines between your company and providers like Dell are becoming less sharply drawn with the growing availability of offerings like the Dell Connected Configuration service that extend customer networks into Dell’s environment. Working together on security, your organization and Dell can do everything possible to make sure that as your organization enjoys the tremendous efficiencies afforded by this service, the data you share is fully protected. When your data is in our environment, you have the benefit of Dell’s security best practices – including SecureWorks testing and validation of the security measures guarding your data.

For more information about the Dell Connected Configuration service, please contact your Dell Representative.