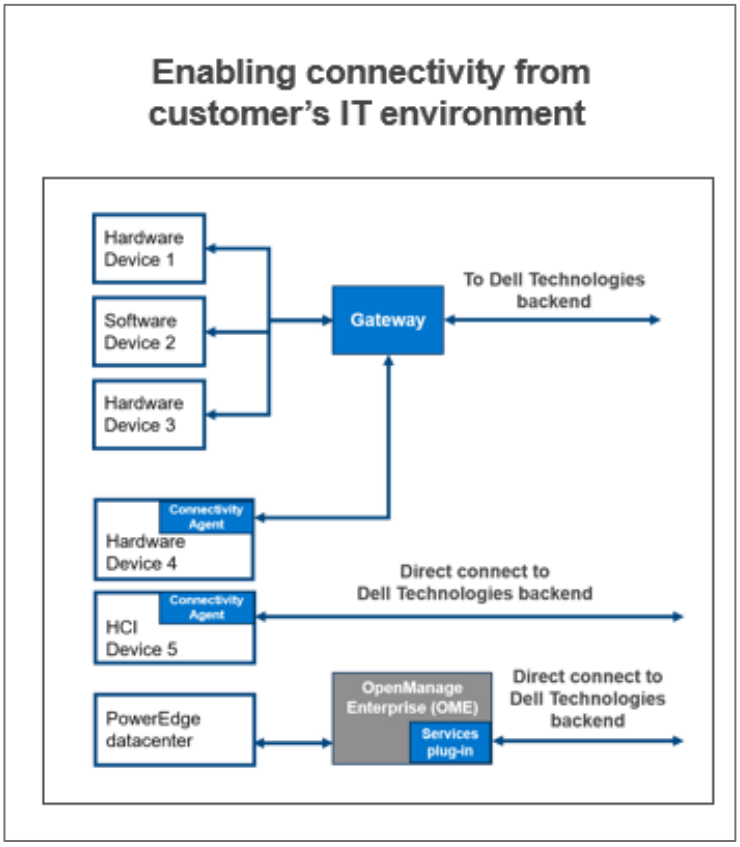
Considerations for deploying and configuring secure connect gateway technology

Technology overview

The secure connect gateway 5.x technology platform is the next-gen connectivity solution – also known as remote IT support and monitoring software – from Dell Technologies Services.

We provide **a single connectivity solution to manage your entire Dell infrastructure portfolio** i.e., servers, networking, data storage, data protection, hyper-converged, and converged (CI/HCI) solutions. Choose what's right for your environment from our flexible installation options – a gateway option, a direct connect option and a plugin option. All are customer installable and upgradeable.



The secure connect **gateway option** allows you to connect your Dell systems to the gateway to communicate back to Dell Technologies Services. This simplifies your firewall / networking set up so that the gateway is the only thing connecting outbound over the internet.

Dell provides a **virtual edition** for VMware and Hyper-V environments. We also have **container versions** for Docker, Podman and Kubernetes environments. For our smaller server customers, we provide a **Windows/Linux version.**

Customers looking for high availability and failover for their systems can set up multiple gateways, or a cluster that will provide redundancy in the event that one gateway is unavailable.

The **direct connect option** is for smaller customers and non-traditional customers who might not want to set up additional software.

Finally, for our compute centric customers, we have the **Services plugin for OpenManage Enterprise** for your PowerEdge server fleet.

For resources & details, get started at Dell.com or read our Customer FAQs.

Note: Connect your Dell systems with a contract for any level of ProSupport Infrastructure Suite services to enable intelligent automated support. By connecting, we can also provide analytics-based recommendations for support and services for many of these Dell systems.

Technology deployment and configuration considerations

The first items to consider are the **types of products – compute, storage, data protection and CI/HCI -** that you will be configuring for connectivity, and **your current environment** such as

- Are your datacenters networked together or not?
- Do you manage compute or storage (including data protection, CI/HCI products) *separately or together*?

You'll also want to consider the **security and networking policies** of the company. In addition, **whether your teams want to manage all products together or prefer to segment them by geo-location or product type.**

Essentially, you must think through how things are wired together, how teams work together and how to minimize network complexity. This will allow you to design the most effective architecture based on the varied deployment options.

Hear from our experts:

- **Listen to podcast:** Maximizing datacenter uptime with intelligent support
- **Listen to podcast:** Maximize PowerEdge uptime with proactive, predictive support
- **Read:** Security white paper

Watch short videos:

- Connectivity features and benefits
- Security architecture and features
- Security configuration for large and small scale environments
- Security features for financial sector
- What is connectable
- Services plugin for OpenManage Enterprise

Read on for real-world scenarios:

1. **What's the recommended configuration for a larger security-conscious company?**
2. **What are the configuration and deployment options for a mid-sized to small organization?**
3. **What if I'm a large to mid-sized company with a compute centric environment? How do I decide which tool to use?**
4. **What if I have ~ 1 – 50 PowerEdge servers and I don't have a virtualized environment. What are my gateway options?**
5. **What if I have Dell products with direct connect availability? What are some typical use cases?**

1: What's the recommended configuration for a larger security-conscious company?

This really depends on the security and networking policies the customer has or sometimes the policies of the datacenter hosting their equipment. Thus, even two large companies that are security-conscious may look completely different in how they configure their environment. It also tends to be industry specific and depends on whether the Dell products in use have remote support capabilities. For example, banking, healthcare, and other critical service companies may require additional security considerations due to policies or regulations.

Configuration scenario 1	Configuration scenario 2
A configuration example for a larger company would consist of multiple gateway clusters placed in each of their datacenters. These are controlled by a policy manager which allows the customer to approve or deny remote support actions before they occur, in addition to logging any transactions that occur.	Another example is more of a distributed model where a company may be putting a hyper-converged (HCI) product like Dell VxRail in each of their retail stores and configuring them to connect directly back to Dell Technologies Services – which uses the same technology – versus connecting them via a gateway. Today, some large retailers use this model for hundreds of stores.

2. What are the configuration and deployment options for a mid-sized to small organization?

The difference between a large organization and a mid to small sized organization usually comes down to resources but the security concerns are often no different.

Configuration scenario 1	Configuration scenario 2
While a large company may have 5 – 6 gateway clusters in different locations, a smaller company may have one gateway or a cluster spread across a couple of locations. Clusters do not need to be in the same location, nor do they need to communicate with each other directly. The key is network connectivity between the Dell devices and the gateways.	Some smaller customers may even have a handful of Dell devices in their datacenter that are configured to directly connect, or they may even have just a single Dell device deployed to a single gateway.

The reasons for different configurations may be the additional features of a centralized gateway solution such as deploying a policy manager to control access and auditing capabilities. Or the company simply wants to be ready for future growth.

For smaller customers that only have PowerEdge servers, we also offer an application version. For customers who may not have a virtualized environment, we also have a containerized version of the gateway that supports all the same devices as the full virtualized versions.

3. What if I'm a large to mid-sized company with a compute centric environment? How do I decide which tool to use?

The secure connect gateway technology is also implemented as the Services plugin within OpenManage Enterprise for PowerEdge servers.

Typically, the Services plugin for OpenManage Enterprise is good for companies with PowerEdge servers while the secure connect gateway solution is the way to go for companies managing a variety of Dell infrastructure products. Both solutions include our alerting, auto-case creation, auto-dispatch and telemetry collection capabilities.

Configuration scenario 1	Configuration scenario 2
If you are only setting up a compute centric environment - and you already have or are thinking of setting up OpenManage Enterprise, the Services plugin is right for you. As a reminder, OpenManage Enterprise is Dell's infrastructure solution that facilitates lifecycle management of thousands of PowerEdge servers from a single console. The Services plugin provides a single, secure direct connection to the Dell Technologies Services backend.	For customers with a mix of Dell infrastructure products such as Powerstore, PowerMax, PowerScale, Data Domain, and VxRail, running alongside PowerEdge servers, we recommend setting up our secure connect gateway solution to manage those systems from a single user interface. Here you connect the devices to the gateway and the gateway connects back to Dell, minimizing the connectivity points outbound for security and ease of use. If you're looking for high availability and failover for your systems, you can set up multiple gateways or a cluster to provide redundancy if a gateway is unavailable.

4. What if I have ~ 1 – 50 PowerEdge servers and I don't have a virtualized environment. What are my gateway options?

You should consider the Application edition of the gateway which is available for Linux and Windows distributions.

5. What if I have Dell products with direct connect availability? What are some typical use cases?

In some instances, our connectivity technology is integrated into the Dell product's operating environment and allows for direct connection to our Services backend. This is what is meant by 'direct connect'. For product details, read our Customer FAQs.

For larger, non-traditional environments e.g., Retail, companies may prefer a direct connection back to Dell Technologies for a Dell system e.g., VxRail in a store location, rather than to set up a single gateway and then connect a single device.

Alternatively, some smaller customers with a handful of Dell storage, data protection or CI/HCI devices in their datacenter may configure them to connect directly to Dell because they do not want the overhead costs and maintenance of a gateway solution.