Secure Connect Gateway

Our technology integrates data protection and threat prevention into a secure, automated support experience

Up to

60%

of IT leaders surveyed by Forrester leverage connectivity technology to reduce risk[1]

It is also implemented as a direct connect version for select Dell EMC hardware and a Services plugin within OpenManage Enterprise for PowerEdge servers. Dell Technologies Services is committed to implementing security capabilities, based on markets, regulations and customer insights, that help our products meet our customers' security objectives and compliance requirements.

Content

1: Introduction:

In today's hyper-digital world, successful innovation leaders are turning to IT service providers to outsource IT support. According to a Forrester Consulting study commissioned by Dell Technologies Services[1], 59% of IT leaders say partnering with the right IT service provider enables them to shift their IT staff's time from day-to-day operations to innovation and strategic initiatives.

As a leading IT service provider, Dell Technologies Services is committed to ensuring that its IT support services and technologies are not potential sources of security threats. Every single day, we do everything we can to minimize risks to our customers from Dell EMC products deployed in their environment. This paper explores how security is built into the design, implementation and operation of the secure connect gateway to ensure a secure automated IT support experience for complex data center infrastructure.

Drawing on over 25 years of pioneering IT support technology, the secure connect gateway security architecture is engineered to head off threat incursions and protect data integrity. While our technology continuously monitors customers' devices for issues and initiates accelerated resolution:

- We only utilize telemetry and event data from active systems.
- We encrypt system state data for transport via the internet over HTTPS using the Transport Layer Security (TLS) protocol.
- Our authorized technical support engineers use multi-factor authentication to remotely access and resolve issues on connected systems.
- We process, store and use telemetry and event data at our locations using industry-leading security practices.

And, we rigorously vet the security measures integrated throughout the secure connect gateway architecture and processes with multiple best-in-class vendors, such as Secureworks, to assure you of a reliably private and safe experience.

Cyberattacks and data fraud or theft are among the top ten concerns for CEOs[2]

2: About Secure Connect Gateway

Dell Technologies provides secure connectivity technology that takes the guesswork out of issue prevention, providing you more time to focus on the projects that matter most. The virtual appliance and application editions provide a secure two-way connection between your environment and Dell Technologies Services ideal for monitoring Dell EMC devices across your data center, including data storage, servers, networking, CI/HCI and data protection, all in one place.

You can also flexibly deploy our technology as a direct connect version for select Dell EMC products and with a Services plugin within OpenManage Enterprise for PowerEdge servers. Visit Dell.com/Support to verify supported connectivity options for specific Dell EMC hardware and software.

Data is the lifeblood of secure connect gateway. We leverage system state data from customer environments. And correlate it with years of incident and engineering data from field and tech support teams as well as component manufacturers.

View Reportable Items for Secure Connect Gateway and the Services plugin for OpenManage Enterprise for details of the system state information collected.

Using sophisticated AI models, including machine learning, our connectivity technology can find and apply patterns to accurately detect the right issue to act on, the first time. It identifies hardware and software issues, creates a case and initiates contact from us to begin resolving an issue before it becomes a costly problem. It predicts failure on server hard drives and backplanes when connected via the secure connect gateway. Depending on the type of issue, the alert may also initiate an automatic parts dispatch.

In addition, the technology enables secure two-way communication for authorized technical support agents to remotely access managed devices to troubleshoot and resolve issues.

SECURITY FOR CONNECTIVITY

Third-party security assessments are conducted regularly against secure connect gateway and its supporting infrastructure.

Application assessments include data transport and API security, static and dynamic source code analysis, Common Vulnerabilities and Exposures (CVE) and Open Web Application Security Project (OWASP) cross-checks, and third-party libraries and products.

Infrastructure assessments include internal and external network devices, servers, and service providers.

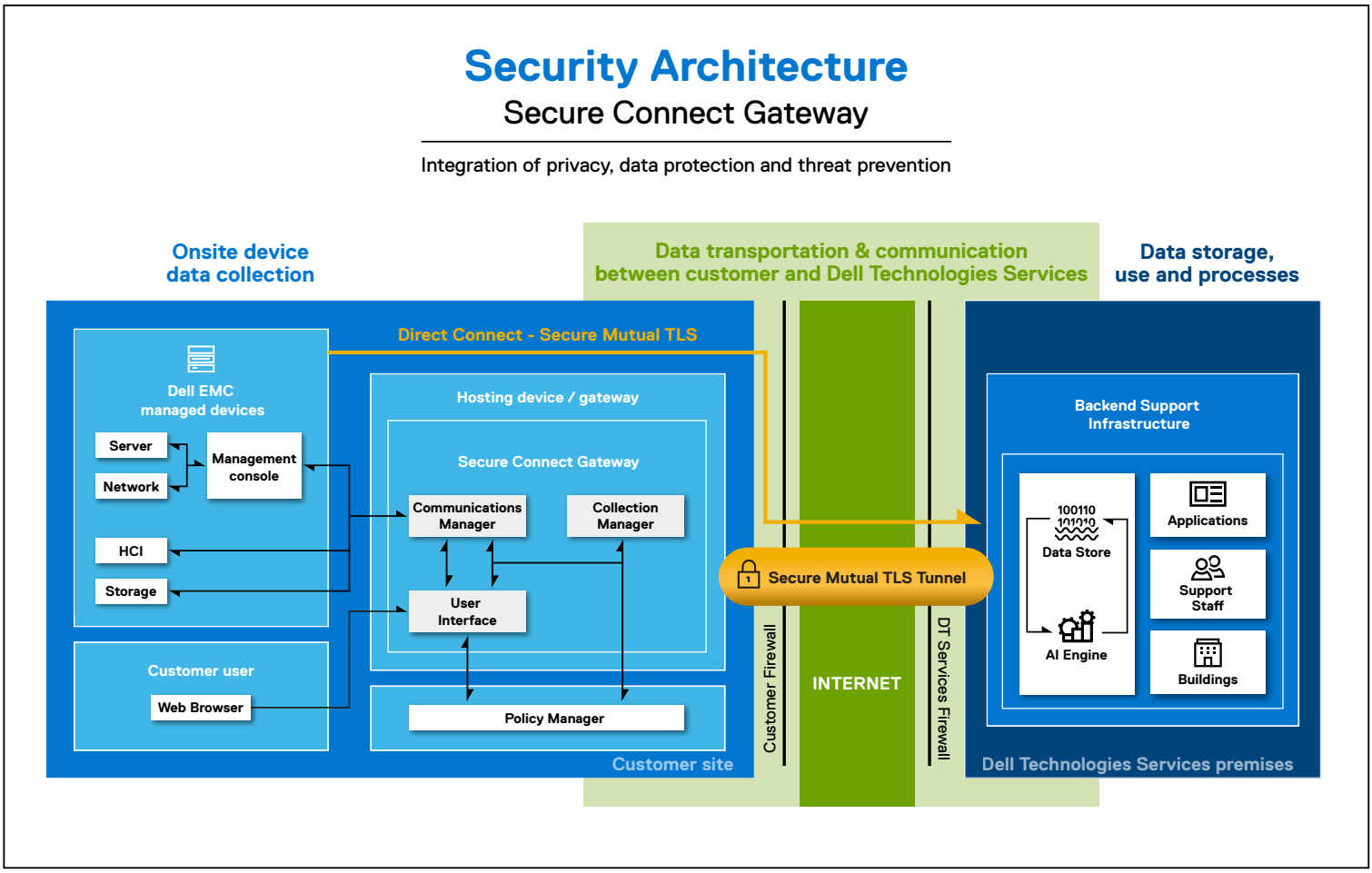
3: Security Architecture Overview

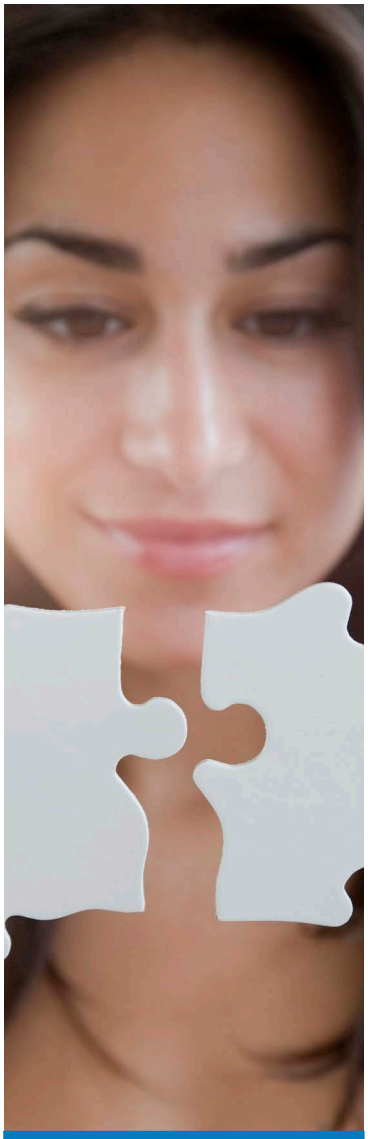
Dell Technologies Services is committed to minimizing the risk of security threats in our automated, proactive and predictive connectivity technology. Our security architecture is built to rigorous industry standards and adheres to measurable and repeatable security practices at every step of product development and deployment. See section 4 for more information.

Diagram A below provides an overview of the secure connect gateway security architecture. In the following sections, we will deconstruct how our technology only collects the system data from Dell EMC managed devices needed to diagnose and fix issues and, then handles that data with maximum security and privacy across:

- Onsite device data collection
- Data transportation and communication
- Data storage, use and processes at Dell Technologies Services

Diagram A:





Customers gain an added layer of security for onsite data collection via the audit capabilities of the policy manager in the secure connect gateway

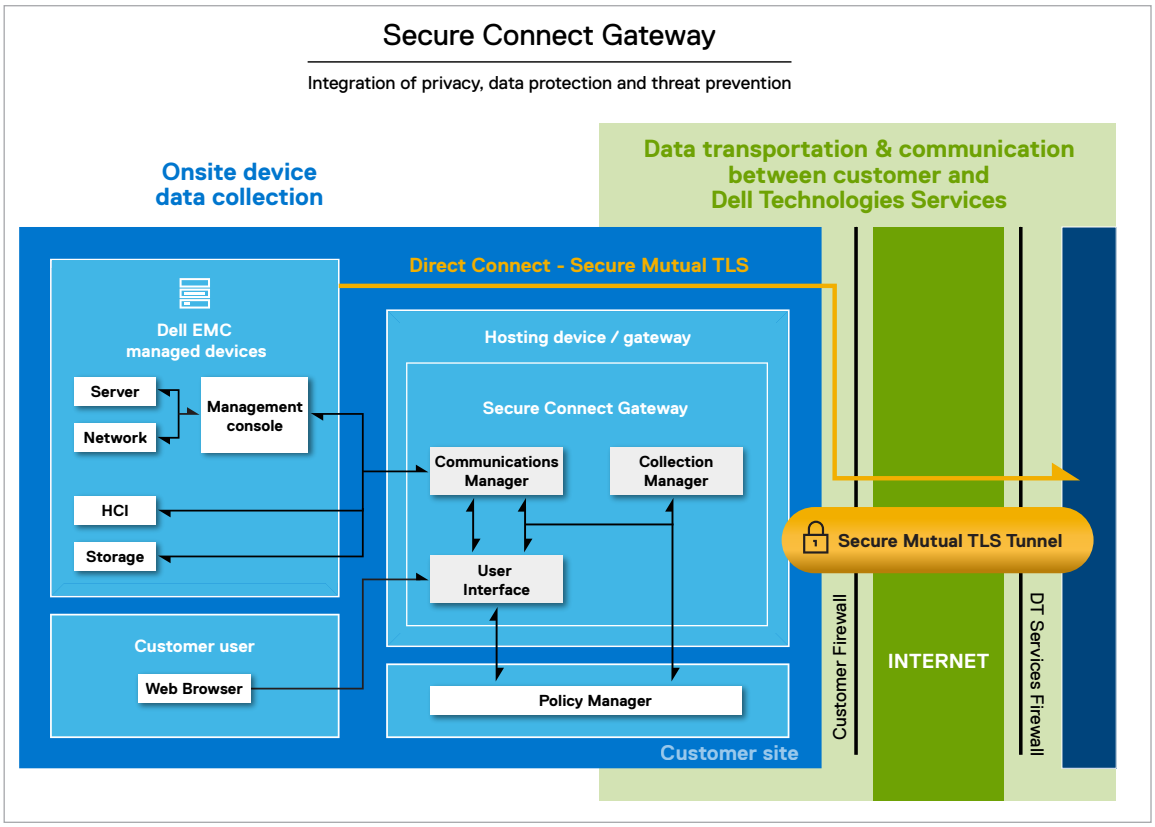
4: Detailed Approach to Security for Secure Connect Gateway

4-1: Secure onsite data collection

Minimizing firewall access points

The secure connect gateway aggregates communications across Dell EMC devices and acts as a single point of entry and exit in a customer's firewall for all IP-based remote services activity. See Diagram B. By minimizing the firewall access points for remote IT support technology, Dell Technologies reduces the security risk via the company's firewall.

Diagram B: (Excerpt from Diagram A – Security Architecture):



As an onsite gateway, the secure connect gateway is deployed virtually on a customer-supplied hypervisor. Each gateway server acts as a proxy, carrying information to and from managed devices. The secure connect gateway can also queue connect home events in the event of a temporary local network failure. These gateway servers have their own web user interface based on the underlying operating system.

For some customers, the direct connect version is appropriate for heterogeneous deployment of multiple Dell EMC hardware products. This solution acts as a single secure point of communication via the customer's firewall. It is integrated into the product's operating environment and thus, does not require a separate server to provide inbound remote support and call home functionality.

Minimizing firewall access points continued

For customers in a PowerEdge data center using the OpenManage Enterprise systems management console, the embedded Services plugin is an alternate implementation option. This connectivity plugin within the OpenManage Enterprise virtual appliance runs on a customer-supplied hypervisor. It acts as a services automation layer from managed server and chassis devices, and provides a single, secure direct connection to the Dell Technologies Services backend.

Acting as a secure communications broker

The secure connect gateway functions as communications broker between the managed devices, the policy manager, and the Dell Technologies Services backend support infrastructure. The gateway servers on which it is deployed are HTTPS handlers. The gateway leverages different communication methods including device discovery, event management, telemetry data collection and telemetry data management. Message types include:

- Device state heartbeat polling
- Data file transfer (connect home)
- Licensing usage data transfer
- User authentication requests
- Device management synchronization

All messages are secure using multiple protocols. In an upcoming section, we'll take a closer look at the additional security built into the secure connect gateway data communication and transportation including the use of the HTTPS protocol with end-to-end Transport Layer Security (TLS) tunneling and industry-standard encryption.

Customer control of authorization requirements and access permissions

If devices are monitored by secure connect gateway at a customer's data center, the customer can opt to use the policy manager to control the authorization requirements for remote access connections, diagnostic script executions, and other related activities. Customers can set access permissions for staff as well as technical support engineers who connect in remotely to diagnose and fix issues.

Security for authorization and permission management is assured by the following policy manager functions:

- The secure connect gateway regularly polls the policy manager for changes to the permissions and caches the permissions locally. In the case of the policy manager:
  - The rule set cache is automatically updated with configuration updates after its last polling cycle.
  - It is configured to receive messages as an HTTPS listener on a specific, agreed-upon port.
- When the secure connect gateway receives a remote access request or any other action, it enforces the policy received from the policy manager cache.
  - Permissions can be hierarchically assigned with policies based on device types or specific models in a device type.
  - Customers can accept or deny the requested action via the policy manager's web user interface. They can also create filters to set further restrictions on authorizations and actions.

Logging and audit trails

Customers enjoy an added layer of security for onsite data collection via the audit capabilities of the policy manager in the secure connect gateway. The policy manager records all remote services events and connections, diagnostic script executions, and support file transfer operations. It then stores them in its database as flat text audit log files. It tracks access to itself (the policy manager), policy changes, and all authorization or denial of access activities.

Customers have all of this information at their fingertips since:

- Audits are viewed through the policy manager web user interface and cannot be edited.
- Audit logs can also be configured to stream to a syslog server in their environment.

Secure Connect Gateway

Supported TLS 1.2 cipher suites:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Device control security option

Since customers do not always enable the policy manager for authorization and permission management, the secure connect gateway provides related security features through the device control option.

Customers can:

- Create custom groups based on device type, administrator group, organization or business unit, physical location of the device, or any other criteria they choose
- Define specific permissions and access rights by these device groups

All device management operations, including remote activity by technical support engineers, are logged. They must also be approved in the backend by a technical support agent.

In this way, customers maintain complete control and transparency over the devices that are managed through the secure connect gateway.

Two factor authentication and digital certificate management

Authentication is an important component of secure onsite data collection. The secure connect gateway uses a digital certificate as proof-of-identity of its deployment on the customer's gateway server. The certificate binds the identity of the gateway server to a key pair that is used to encrypt and authenticate communication with the backend. Dell Technologies Services' Certificate Authority (CA) is the central repository for the secure connect gateway key infrastructure.

Digital certificate management is used to automate the enrollment of the digital certificate through our private Certificate Authority. This:

- Enables programmatic generation and authentication of each certificate request.
- Ensures that the certificate is only issued and installed on the gateway server. The certificate cannot be copied and used on another machine.

The secure connect gateway connects and authenticates using the digital certificate deployed on our backend support infrastructure. Technical support agents connect to the secure connect gateway in the customer's environment using two factor authentication.

4-2: Secure data transportation and communication

Secure communication tunnel

All communications between the customer and Dell Technologies Services backend support infrastructure are initiated outbound by the secure connect gateway from the customer's site. It creates a secure end-to-end communication tunnel using industry-standard Transport Layer Security (TLS) 256-bit encryption over the Internet, and digital certificate authentication signed by Dell Technologies Services. The latter is detailed in the preceding section on secure onsite data collection.

As a result, secure connect gateway connections have the following properties:

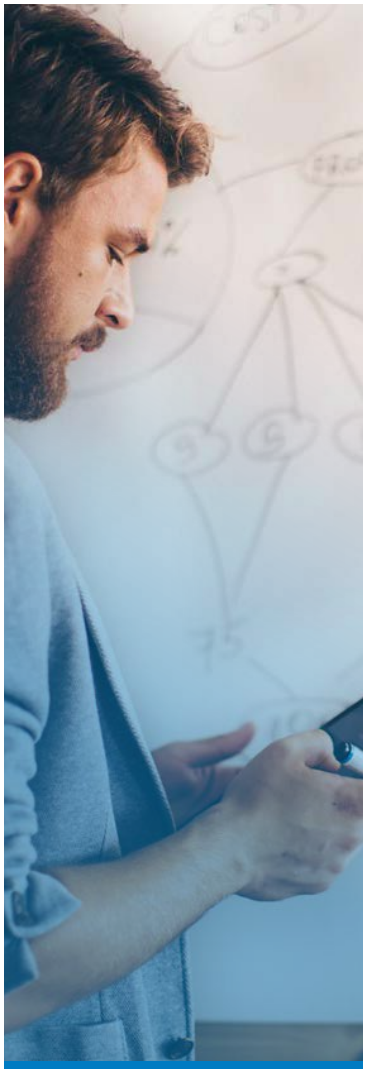
- **Reliable data transfer:** Each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.
- **Private and secure session via TLS:** Symmetric encryption using industry-standard algorithms generates unique keys for each connection. Communications cannot be modified during the negotiation without being detected.
- **Authenticated parties**: Since this connection is secure, it identifies the communicating parties and authenticates them using public-key cryptography. This approach prevents spoofing and man-in-the-middle (MITM) attacks.

Communications using the secure TLS tunnel

The gateway server uses the TLS tunnel to ensure a secure environment for the following functions: heartbeat polling, remote notification and remote access. In this section and per Diagram C, we take a closer look at these core communication processes and protocols for the automated, proactive and predictive experience from our technology.

Heartbeat polling

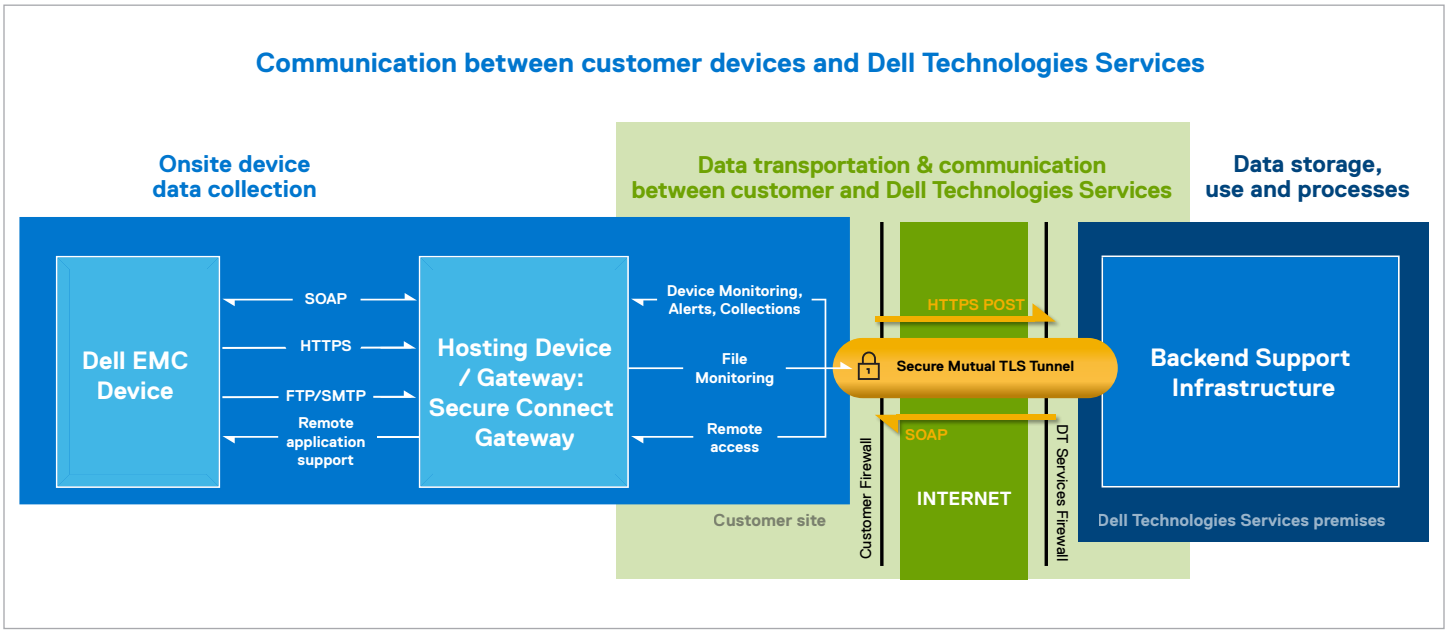
Customer systems must be connected to benefit from the secure connect gateway experience. Heartbeat polling checks the connectivity status of devices and regularly communicates telemetry data collected to the backend. The data also identifies the gateway server on which secure connect gateway is deployed.



Industry-leading authentication secures connections against spoofing and man-in-the-middle attacks

Communications using the secure TLS tunnel continued

Diagram C: Security Architecture



Remote notification or connect home function

The secure connect gateway serves as a secure conduit for devices to send event files to the backend. This includes errors, alerts, warning conditions, health reports, configuration data, and script execution statuses.

- When an alert is generated, an event file is generated and sent to the gateway.
- The file is received by the secure connect gateway through the HTTPS listener services.
- For legacy products that use FTP and/or SMTP listeners for the secure connect gateway, the files are encrypted and transferred.
- The gateway compresses the file and sends it to the backend through the TLS tunnel. It then deletes the file from the listener directory.
- The file is then decompressed in the backend for analysis.
- The secure connect gateway can also send the files to the backend through the encrypted communication tunnel. In addition, the gateway can be configured to use the failover channels, namely, FTPS or the customer email server.

System monitoring data is collected from various components of an active system to enable Dell Technologies Services to provide an adaptive, intelligent and accelerated support experience. The system ID, which is needed to identify the specific system being worked on, is the only information about the company collected from devices. When we determine that a part should be proactively shipped, we use existing contact information that has been securely stored on Dell Technologies servers.

A complete list of system-monitoring data that is collected from an active system - including data collected outside the routine 24-hour cycle - may be found in the Reportable Items documents for Secure Connect Gateway and the Services plugin for OpenManage Enterprise.

Remote access

Our technical support teams also remotely access the devices at a customer site to troubleshoot issues or perform device-specific actions. Asynchronous messaging ensures that the remote access session is initiated by the secure connect gateway from the customer site. Next, a secure remote access session is established as follows:

- After session authentication at the Dell Technologies Services backend, a technical support agent requests device access including service request number, if available, and other device or user identifiers.
- The remote access request is queued in the backend until the gateway sends the device's heartbeat message to the backend to retrieve it.
- In response, the backend server sends a response that includes request information, the backend server address and a unique session ID to connect to the gateway.
- The secure connect gateway uses its local repository to determine the local IP address of the device. Then, it checks the cached policy from the policy manager to vet connection permissions.
- If permitted, the secure connect gateway establishes a separate persistent TLS connection to the backend server. The TLS connection is always initiated by the gateway. The backend server can never initiate an inbound connection to the gateway server. This ensures there is no vulnerability to outside attacks.

Communication flows through the tunnel between the secure connect gateway and the backend server until it is terminated or times out after a period of inactivity.

Network security

All network monitoring components are located behind a firewall and are managed by our network security team. Network traffic is tightly controlled. All inbound traffic is transmitted via specific ports and only sent to appropriate destination network addresses.

4-3: Secure data storage, use and processes

Security for storage and use

Physical security

Dell Technologies Services hosts most secure connect gateway data, including the application, systems, network and security components, in a US-based data center designed to maintain high levels of availability and security. The data is protected by using a wide variety of measures, including physical security. Features include, but are not limited to:

- On-premise security guards
- Cameras
- False entrances
- Vehicle blockades
- Specialized parking lot design
- Bulletproof glass and walls
- Use of an unmarked building

Access to data centers where the infrastructure resides is restricted to authorized personnel. Access is controlled via smart card.

Logical security

Data generated by secure connect gateway is stored in compliance with the Dell Privacy Policy.

Logical access to Dell Technologies Services infrastructure (servers, load balancers, network shares, etc.) is restricted through internal tools which are audited and evaluated as per IT guidelines:

Logical security continued

- **Server and database security:** Servers and operating system components reside on standard images that have undergone security reviews. There are regular reviews of security updates used by the application, including those published by Microsoft and other software vendors. When critical security updates are issued, they are first tested on non-production images and generally applied to live servers in a timely fashion to avoid risks.
- **Auditing:** Monitored device logs are maintained, accessible only by authorized Dell Technologies Services infrastructure and applications. These logs record all attempts to log into or access the operating system or the secure connect gateway web server console.

IT-managed builds are hardened using recommended Center for Internet Security (CIS) Controls security best practices. Industry-standard security guidelines also are implemented on all servers and network equipment.

Finally, the secure connect gateway ecosystem employs both local high availability within its data center and identical infrastructure in a separate data center. The only exceptions are technologies that are intrinsically high availability, such as big data clusters and private clouds. For data analytics, Dell Technologies Services leverages cloud environments that we fully control and manage, including private, hybrid and public clouds.

We utilize a repeatable, secure development process for products and applications

Authentication

For secure connect gateway, Dell MyAccount is used for authentication with Dell Technologies Services and OS login groups for on-the-box authentication.

Groups, such as the database administration team and the operational support team, that have access to secure connect gateway components, are assigned separate duties and access rights. All updates to the production environment go through a defined change control process that incorporates checks and balances.

Security for processes

Security-aware community

We offer a multi-level role-based security training curriculum to educate new and existing employees on job-specific security best practices and how to use relevant resources. Dell Technologies strives to create a security-aware culture across its entire community. In addition, our developer community is part of Dell's Security Champion program which is designed to foster shift-left security in our software development practices.

Development

Our internal **Secure Development Lifecycle Standard (SDL)** is a common reference for Dell Technologies product organizations to benchmark product and application secure development activities against market expectations and industry practices. It defines security controls that product teams should adopt while developing new features and functionality. The SDL includes both analysis activities as well as prescriptive proactive controls around key risk areas. The analysis activities, such as threat modeling, static code analysis, scanning and security testing, are intended to discover and address security defects throughout the development lifecycle. The prescriptive controls are intended to ensure that development teams code defensively to prevent specific prevalent security issues including those found in the Open Web Application Security Project (OWASP) Top 10 or SANS Top 25. The secure connect gateway has

Development continued

adopted the Dell SDL maturity framework to implement security controls in alignment with industry standards.

The code for secure connect gateway is developed using the Agile development methodology. Code is integrated continuously using industry-standard automation software. Code versions are checked in and controlled using secure group permissions.

Every software release undergoes a security assessment in accordance with our security policies and includes:

- Vulnerability assessment using penetration testing
- Third-party security testing using multiple best-in-class vendors such as Secureworks
- Assessment for authentication, authorization, and identity management solutions
- All third-party libraries and components are scanned with industry-leading solutions for software composition analysis. In addition, Dell Security Advisories are communicated for specific security improvements.
- Data classification with our Global Security organization. This process brings privacy and security together to ensure that electronic data is protected.

Applications are also subjected to security audits and governance.

Change management

The Dell Technologies change management process follows ITIL Foundation best practices as dictated by our corporate change management board. All changes are managed via change request tickets. Those accessing our system to initiate changes are required to undergo ITIL training, as well as familiarization with the SDL. All updates and upgrades applied to backend infrastructure are version controlled for proper tracking and traceability. The team employs an automated build process to apply new builds or revoke any build or hot fix that was deployed.

The application installed at a customer's premise may be upgraded based on the customer's preference. Every release promoted to Dell.com/support contains information on the changes introduced with any known limitations.

All new features and changes are groomed by our product management team and are prioritized using a plan-of-record change process which goes through the change control board for review and approvals.

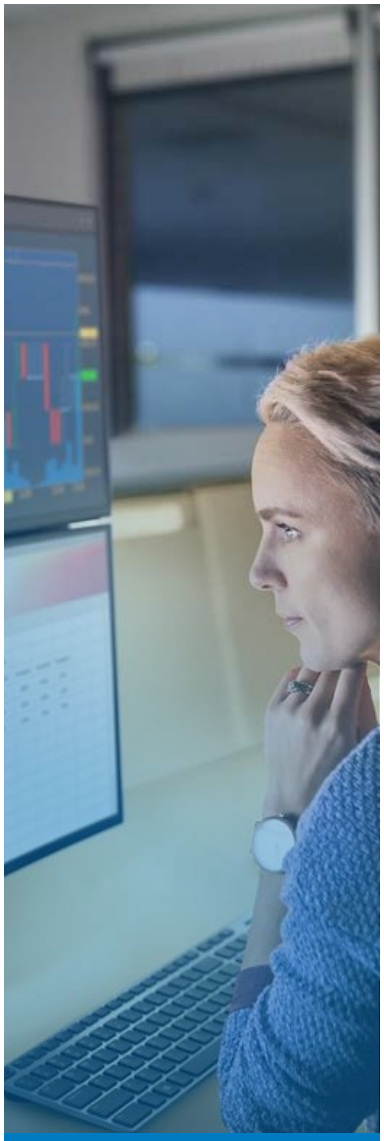
Supply chain risk management

Dell Technologies follows industry-leading best practices at each stage of the plan-source-make-deliver-return lifecycle. We take a comprehensive approach to securing our supply chain, including driving international SCRM standards and best practices, in order to remain a trusted ICT supplier in the global marketplace.

Learn more about our Supply Chain Assurance practices here.

Incident reporting

Anyone at Dell Technologies who observes suspicious activity or suspects a cybersecurity issue or threat is required to report the incident immediately to our Computer Security Incident Response Team (CSIRT). This includes a weakness or gap in a security process that could affect our environment or, result in a breach of systems and/or data. The CSIRT then launches a full inquiry into the incident, and the person reporting the incident provides all artifacts and details necessary for the CSIRT to carry out the investigation. The CSIRT team uses the CSIRT Incident Response Plan which details a formal process to respond and resolve Dell internal and non-customer-facing cybersecurity incidents. These incidents may pose potential threats to Dell assets, computer networks or data processing equipment as well as Dell and its applicable subsidiaries, staff, service provider, partner or customer information.



Industry collaboration on product security best practices

Vulnerability response

Dell Technologies strives to help our customers minimize risk associated with security vulnerabilities in our products by providing customers with timely information, guidance and mitigation to address threats from vulnerabilities. Our Product Security Incident Response Team (PSIRT) is responsible for coordinating the response and disclosure for all product vulnerabilities reported to us. All Dell Technologies product vulnerability disclosures are available online.

Learn more about our Vulnerability Response Policy

Industry affiliations

Dell Technologies participates in multiple industry-wide groups to collaborate with other leading vendors in defining, evolving and sharing best practices on product security and in further enhancing the cause of secure development. Examples of industry collaboration include:

- Dell, through its EMC entity, co-founded and currently chairs the Board of Directors of The Software Assurance Forum for Excellence in Code (SAFECode). Other board members include representatives from Microsoft, Adobe, SAP, Intel, Siemens, CA and Symantec. SAFECode members share and publish software assurance practices and training.
- Dell Technologies is an active member of The Forum for Incident Response and Security Teams (FIRST). FIRST is a premier organization and a recognized global leader in incident and vulnerability response.
- We actively participate in The Open Group Trusted Technology Forum (OTTF). OTTF leads the development of a global supply chain integrity program and framework.
- Dell was one of the first 9 companies assessed by the Building Security In Maturity Model (BSIMM) project back in 2008 and has continued to participate in the project. A Dell Technologies representative is part of the BSIMM Board of Advisors.
- Dell employees were founding members of the IEEE Center for Secure Design, which was launched under the IEEE cybersecurity initiative to help software architects understand and address prevalent security design flaws.

Visit our Security and Trust Center for resources and solutions to help you find answers to your enterprise security questions.

Industry security standards

Our employees are actively involved in standards bodies and industry consortia, which focus on developing security standards and on defining industry-wide, security practices, including:

- Cloud Security Alliance (CSA)
- Distributed Management Task Force (DMTF)
- The Forum for Incident Response and Security Teams (FIRST)
- International Committee for Information Technology Standards (INCITS)
- International Organization for Standardization (ISO)
- Internet Engineering Task Force (IETF)
- The Open Group
- Organization for the Advancement of Structured Information Standards (OASIS)
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)

ISO 9001 certification

Dell Technologies is ISO 9001 certified. The company conducts regular quarterly audits and compliance review for all its development and manufacturing centers.

Podpisany certyfikatem wystawionym dla Jacek Piekarski (Certyfikat kwalifikowany). Utworzony w dniu: 2023-09-13 14:54:29 +0200

5: Conclusion

Our connectivity technology delivers an effortless IT support experience with automated proactive and predictive alerts that ensure maximum uptime for critical data center infrastructure. Customers partnering with Dell Technologies Services can be assured of our commitment to providing a reliably private and secure experience for the collection, communication, transportation, use and storage of their telemetry data.

For questions and more information, visit **DellTechnologies.com/SecureConnectGateway**

1 Source: "The Role Of IT Services Providers Expands To Strategic Collaboration", a commissioned study conducted by Forrester Consulting on behalf of Dell Technologies, April 2021

2 Source: World Economic Forum Global Risks Report 2021. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

DELL Technologies