SupportAssist for Business PCs: Security Overview

Five key questions you may have about SupportAssist security – and their answers.

SupportAssist enables you to automate support from Dell Technologies by identifying hardware and software issues across your PC fleet. SupportAssist addresses system performance and stabilization issues, reduces security threats, monitors and detects hardware failures and automates the engagement process with Dell technical support.

SupportAssist also proactively collects telemetry data from your PCs and provides PC utilization and remediation insights based on your service plan.

Content

I: Introduction

A failure on a laptop can be both disruptive and frustrating. Such problems can severely impact an employee's productivity, often at the worst possible moment. Because of this, corporate CIOs have become increasingly concerned about the quality and uptime of their PC fleets.

Many CIOs have turned to the latest, most advanced technology, which uses insights gained from data science to process billions of data points and help IT administrators be more efficient. System state information from end-user systems is sent to the company's IT department or to a hardware or software vendor to quickly resolve or prevent issues. Dell ProSupport Plus with SupportAssist connectivity technology alerts you to a failing hard drive by providing a single view of your entire PC fleet from the TechDirect portal.

While this technology is needed to ensure uptime and efficiency, CIOs sometimes raise questions about the information it collects and how it is handled.

The following questions are considered critical:

- What data does SupportAssist collect?
- How is this data protected as it is transmitted back to the company's IT department or the computer vendor?
- Once it reaches its destination, is that data stored in such a way that it remains private and secure?
- How does Dell adhere to the GDPR and other standards?

This paper evaluates these and other related questions as a means of assessing data science-enabled technologies. It provides a brief overview of how SupportAssist, as part of the ProSupport Suite for PCs, delivers a comprehensive support service capable of predicting and resolving issues before they occur. It also provides a detailed look at how Dell Technologies Services secures sensitive data in its processes, data transportation, and data storage.

II: About SupportAssist

SupportAssist is Dell's smart connectivity technology[1] that enables an organization to receive automated technical support for its entire PC fleet. It monitors end user devices, proactively detects both hardware and software issues and provides insight into system usage.

When an issue is detected, SupportAssist automatically opens a support case with technical support, based on the service plan. The type of issue will determine whether the alert initiates a technical support request or triggers an automatic parts dispatch. SupportAssist collects both hardware and software data that is used by technical support to troubleshoot and resolve the issue.

Dell ProSupport Suite for PCs offers the most comprehensive support capabilities in a single solution — without the need to stack services.[2] Learn more.

Key Features

- Fleetwide proactive and predictive detection for faster issue resolution
- Quick analysis of health, application experience and security scores in a single screen
- Library of Dell-authored scripts to automate tasks and remediate issues across the fleet
- Automate creation and deployment of custom update catalogs for Dell BIOS, driver, firmware and applications
- Flexibility to tailor your views and dashboards in TechDirect

Available features vary based on the support plan purchased for a PC.

- With ProSupport Plus, end users receive the full set of SupportAssist features, including predictive issue detection and failure prevention.

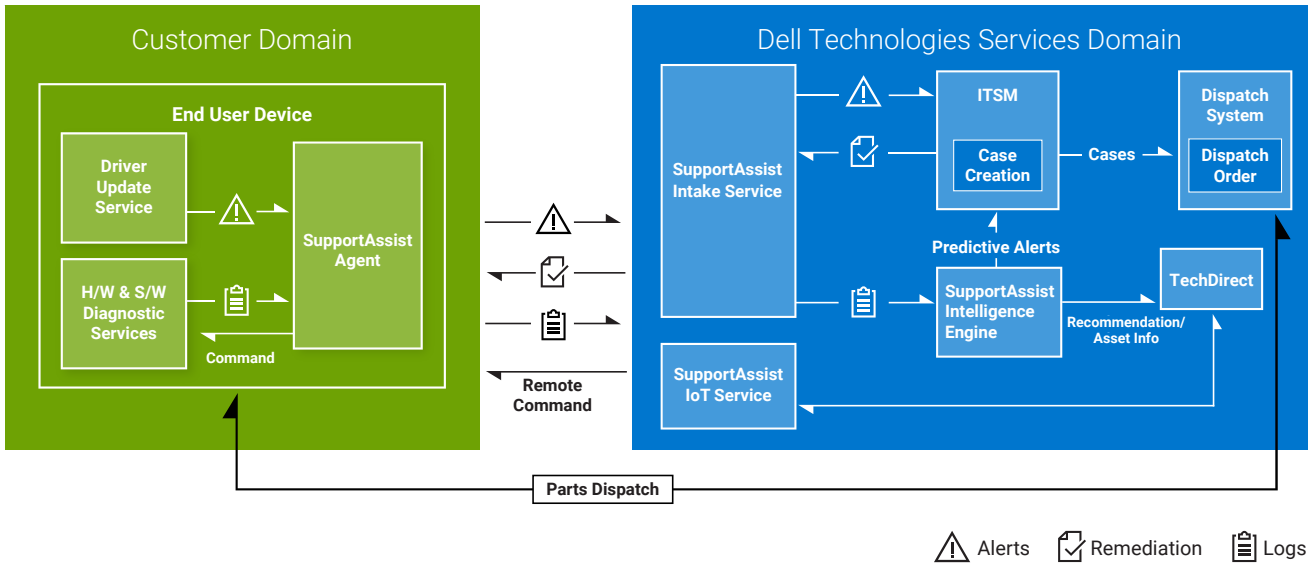
For a complete list of features and capabilities, please review the Administrator Guide.

III. SupportAssist Architecture

SupportAssist comprises a set of services that monitors systems continuously and runs schedule-based health checks on a device. This information is transmitted back to Dell Technologies' servers to analyze the data and provide recommendations.

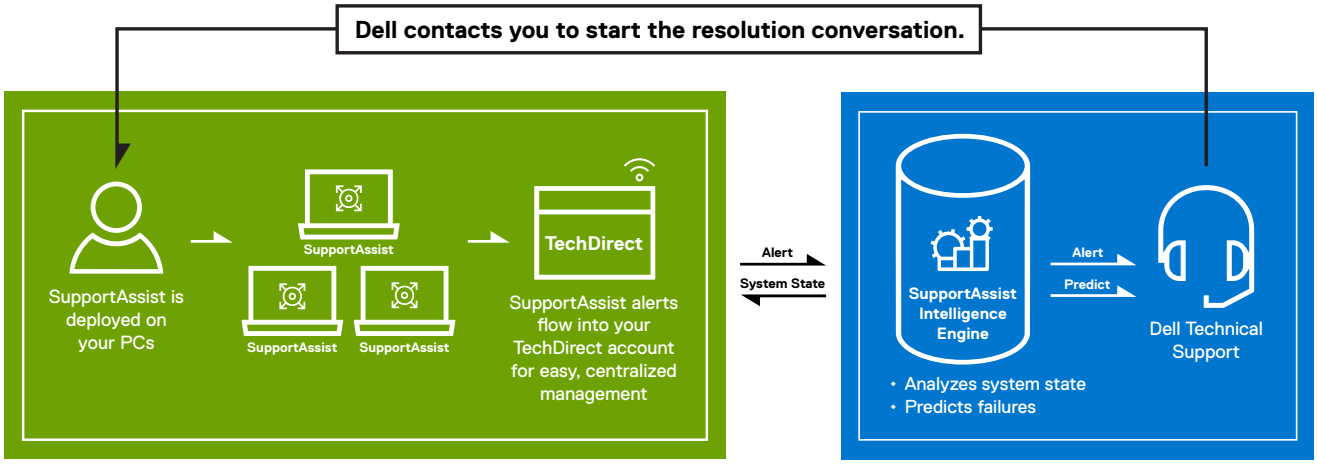
For a complete list of network, endpoint, ports, firewall or gateway requirements for SupportAssist deployment and remediation, view our deployment guide. Our remediation scripts are developed by Dell, tested and signed, then confirmed, before executing.

SupportAssist Architecture



Centrally manage SupportAssist using TechDirect

SupportAssist alerts can flow into an organization's TechDirect account for convenient, centralized management. Organizations with a ProSupport or ProSupport Plus service plan also can elect to auto-forward alerts to Dell Technologies Services.

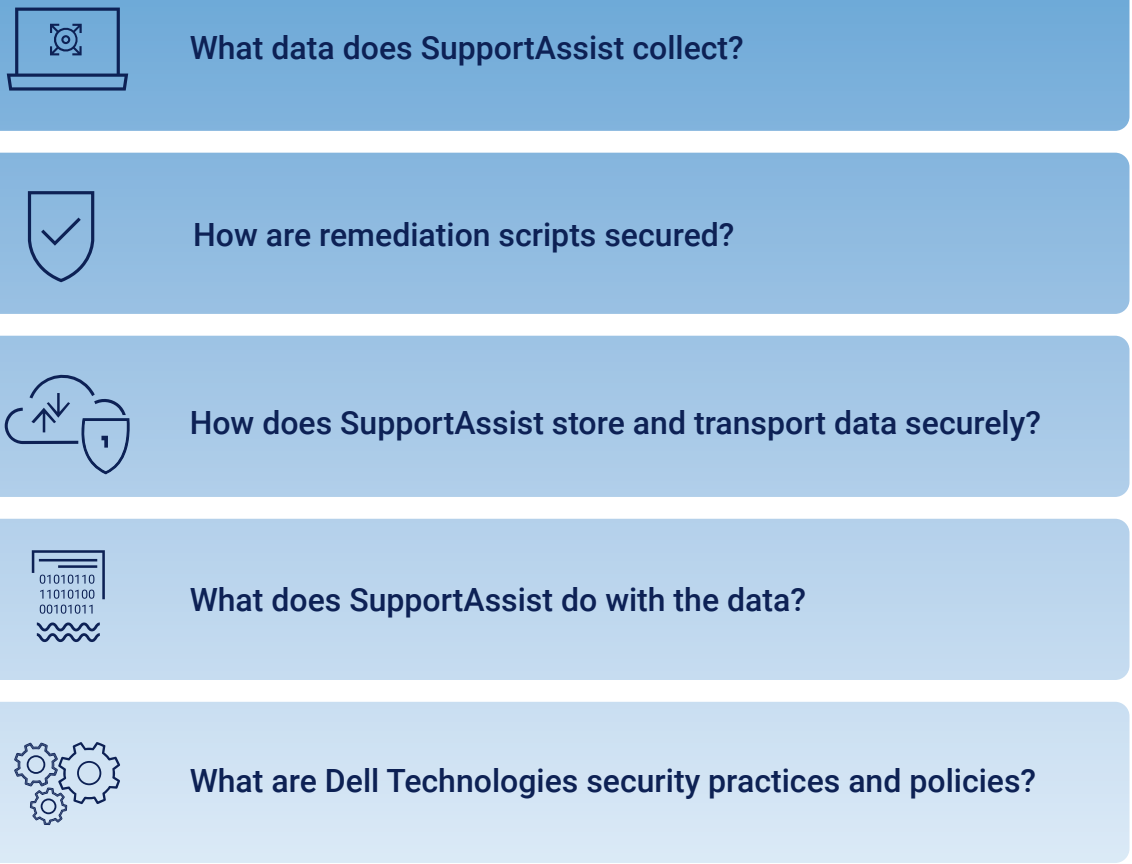


Centrally manage SupportAssist using TechDirect continued:

SupportAssist insights, a very useful analytic component, collect system utilization data that can be viewed within TechDirect. This includes CPU utilization, free drive space, maximum battery capacity, battery runtime and many more useful insights. TechDirect can display this information for all systems, for systems in a specific device group, or for an individual system. Customers are able to identify performance issues and make better business decisions (whether or not to upgrade or replace hardware, for example).

IV. SupportAssist Security

An organization's CIO or CSO may have questions about the types of data SupportAssist collects and how that data is managed. This section will answer these questions, showing how SupportAssist collects only the data needed to fix customer issues and then handles that data with optimal security in mind.



What data does SupportAssist collect?

SupportAssist automatically collects the data required for troubleshooting an issue and sends it securely to technical support. This data enables us to provide an adaptive, intelligent, and accelerated support experience.

The service tag, which is needed to identify the specific end user device being worked on, is the only information about the company collected from devices. When SupportAssist determines that a part should be proactively shipped, Dell uses existing contact information that is securely stored (encryption, retention policies, etc) with Dell Technologies servers.

The following system information is collected and sent once every 24 hours as part of routine system monitoring:

- **Schema version:** Version of the schema used for routine system monitoring
- **Agent version:** Version of SupportAssist deployed on the system
- **Service tag:** Unique identifier of the system
- **System model:** Model name of the system
- **Registration information:** Registration status of SupportAssist
- **OS version:** Version of the operating system running on the device
- **SP version:** Service pack of the operating system
- **UTC date:** Date and time when the routine system monitoring information was sent to Dell Technologies Services
- **BIOS version:** Version of the BIOS that is installed on the system
- **Status:** Status of the alert depending on the severity, for example, warning
- **Description:** Information about the system failure, for example, high CPU usage
- **Hard drive free space:** Free space available in the system hard drive
- **Memory usage:** Amount of system memory used
- **CPU Usage:** Amount of CPU used
- **Local date:** Date and time of the system
- **Last Boot Up Date:** Date and time when the system was last restarted
- **Windows Updated Run Date:** Date and time when Windows was last updated on the system
- **BSOD Count 24hrs:** Number of blue screen occurrences in the last 24 hours
- **Alert info:** Unique identifier of the alert

For more information on system-monitoring data collected from an active system, please visit our Dell.com page here.

All information is transmitted through secured channels.

How are remediation scripts secured?

Before being uploaded to the remediation platform, all Dell-authored remediation scripts are signed with Dell certificates and undergo extensive testing and validation to ensure they perform as intended without producing unexpected results. This serves as the basis for verifying the authenticity of the script before execution. For example, if a script is modified or replaced on the endpoint, the certificate signature validation will fail, and SupportAssist will block the script from execution. This prevents the execution of unauthorized or potentially harmful code. These scripts cannot be modified by anyone outside Dell, ensuring their integrity. It is recommended to test scripts on a designated group of PCs before broader deployment.

A different process is followed for custom workflow scripts. When customers upload their own scripts, the remediation system accepts both unsigned scripts and scripts signed with a customer certificate. The integrity of these scripts is preserved while in transit to PCs and when stored at rest. It is recommended to test custom scripts on a specific group of PCs before broader deployment.

TechDirect Connect and manage supports the creation of sites and groups, enabling customers to validate both Dell-authored and custom scripts on test machines. All information in the remediation console is secured within tenant boundaries in TechDirect, accessible only to users with appropriate roles assigned by the tenant administrator. Results can also be exported to a CSV file for further analysis.

How does SupportAssist store and transport data securely?

The data sent from SupportAssist to Dell Technologies Services is encrypted with 256-bit encryption and transferred securely using the Transport Layer Security (TLS) protocol.

An encryption key is generated at run time on each machine during installation of the package. The encryption key, along with the salt, is used to encrypt installed information. An industry-standard algorithm is used to encrypt data at rest.

In cryptography, salt is random data that is used as an input to a one-way function that "hashes" data, a password or passphrase. The primary function of salts is to defend against dictionary attacks or against its hashed equivalent, a pre-computed rainbow table attack.

All encryption keys are generated using secure random number generators. Data in transit is secured using TLS over Hypertext Transfer Protocol Secure (HTTPS). All encryption algorithms are industry standard, and data at rest is encrypted.

HTTPS is used in off-box communications for transmissions of user-provided feedback, diagnostic telemetry events, and querying an API on Dell.com or Microsoft Azure IoT Hub for system information used in the restore process. A secure MQTT is used for pub-sub approach.

Standard HTTPS is used to secure communications between the client and the backend infrastructure when transmitting or downloading content to the end user device. HTTPS or secure MQTT is used to secure transmittal of telemetry data, communication with a backend API on Dell.com or Microsoft Azure IoT hub, and the download of content retrieved from Dell.com.

All network components are located behind a firewall and are managed by a network security team. Network traffic is tightly controlled. All inbound traffic is transmitted via specific ports and only sent to appropriate destination network addresses. SupportAssist utilizes network bandwidth for various events that require connectivity to Dell Technologies Services infrastructure. The bandwidth utilized may vary based on the number of target systems that SupportAssist monitors. Please refer to the Data Collected from Connected PCs document to learn more about average data consumption.

What does SupportAssist do with the data?

SupportAssist uses the collected data to provide automated, proactive, and predictive support to customers. If there is an issue with a system, SupportAssist will generate an alert for a technical support agent to troubleshoot.

SupportAssist also uses collected data to predict when a component is about to fail, using artificial intelligence software based on data collected from tens of millions of Dell systems in the field. This predictive alert can be used to dispatch a part before it fails, resulting in optimal system uptime and data protection.

Finally, SupportAssist uses the data to detect and remove viruses and malware from user systems, to optimize operating system performance, and to provide recommendations on BIOS, driver and firmware updates.

System app usage provides insight into system usage with insights component.

Physical security

Dell Technologies Services hosts SupportAssist data, including the application, systems, network and security components, in a United States based data center designed to maintain high levels of availability and security. SupportAssist data is protected by using a wide variety of measures.

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

Physical and logical security measures keep stored data safe.

Logical Security

Data generated by SupportAssist 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 Dell Digital (IT) guidelines.

- **Auditing:** Monitored device logs are maintained, accessible only by Dell Technologies Services infrastructure and/or applications. These logs record all attempts to log into or access the operating system or the SupportAssist web server console.

IT-managed builds are hardened using Center for Internet Security (CIS) recommended controls by security best practices.

Finally, the SupportAssist 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. Relational databases, simple storage services, and data warehouses are all encrypted and use least privileges. No relational databases are public-facing. Data warehouses are secured using HTTPS.

What are Dell Technologies security practices and policies?

Development

Our internal Secure Development Lifecycle Standard (SDL) serves as a foundational reference for Dell Technologies product organizations, providing essential benchmarks for secure product and application development. Dell provides a defined SDL control catalog based on ISO/IEC 27034 and a standard based on the NIST Secure Software Development Framework (SSDF). These tools help Dell teams build secure products for customers and prevent security vulnerability and weaknesses from being introduced in Dell developed/supported software and hardware. These controls are mandated for adoption by Engineering teams during the development of new features and functionality. These controls encompass analysis activities, as well as prescriptive proactive measures focused on key risk areas.

Analysis activities, including threat modeling, static code analysis, scanning, and security testing, are integral components aimed at identifying and mitigating security defects throughout the development lifecycle. Additionally, the SDL includes prescriptive controls to help ensure that development teams proactively address specific security issues, including those outlined in industry standards like the Open Web Application Security Project (OWASP) Top 10 and SANS Top 25.

SupportAssist for Business PCs aligns with this robust SDL framework, employing the Dell SDL maturity model to implement security controls in accordance with industry standards. The DevSecOps program secures the modern software development and deployment processes at Dell by automating SDL controls and enforcing security policies in a Continuous Integration and Continuous Deployment (CI/CD) environment. These CI/CD tools automate the build, test, and deployment processes, ensuring code changes are integrated and tested continuously as part of the development workflow.

SDL engineers perform SDL Security assessments to identify security issues and vulnerabilities in software and provide recommendations to development teams to remediate these security findings. This assurance provides visibility into the maturity of our security practices and the security posture of our software and hardware.

This assessment includes:

- Vulnerability assessment through penetration testing.
- Third-party security testing conducted by respected vendors like SecureWorks.
- Evaluation of authentication, authorization, and identity management solutions.
- Thorough scanning of all third-party libraries and components using industry-leading software composition analysis tools.
- Communication of Dell Security Advisories for specific security enhancements.
- Rigorous data classification in collaboration with our Global Security organization, aligning privacy and security efforts to safeguard electronic data.
- Subjecting applications to security audits and governance procedures.

GDPR

Dell has implemented measures designed to ensure that we have the necessary processes and procedures to comply with our obligations under the GDPR. Dell tracks developments in privacy laws worldwide and ensures compliance with its applicable obligations under the relevant privacy legislation. Where Dell acts as a processor, it does so according to a mutually agreed form or otherwise to a standard Data Processing Agreement form. For more information, please visit the following links:

- Dell's GDPR Information Security Corporate Statement and Controls Summary
- Dell's Commitment to GDPR Compliance
- Dell's Compliance FAQs for Dell Technologies Customers

Secure processes and proven industry practices maintain the security of SupportAssist.

Security validation testing

Third-party security assessments are conducted regularly against the SupportAssist application and its supporting infrastructure.

Application assessments include data transport and API security, static and dynamic source code analysis, Open Web Application Security Project (OWASP) crosschecks, and third-party libraries.

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

Change management

The Dell Technologies change management process follows ITIL Foundation best practices as dictated by the corporate change management board. All changes are managed via change request tickets. Those accessing the 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.

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 and change management process.

Authentication

SupportAssist uses Dell MyAccount for authentication with Dell Technologies Services infrastructure, application random symmetric key, JWT 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 SupportAssist 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-aware community

Dell offers a 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, the developer community is part of Dell's Security Champion program which is designed to foster Shift Security Left in the software development practices.

Incident reporting

At Dell Technologies, all are required to promptly report any suspicious activity, cybersecurity issues, or threats to our Computer Security Incident Response Team (CSIRT) via email at security@dell.com.

Vulnerability response

Dell Technologies is committed to minimizing risks associated with security vulnerabilities in products, applications, and cloud services. To achieve timely vulnerability response practices, Dell adheres to the guidelines outlined in the Dell Technologies Vulnerability Response Standard (VRT) Standard. Dell actively participates in various community efforts including the Forum of Incident Response and Response Teams (FIRST) and the Software Assurance Forum for Excellence in Code (SAFECode). Dell's processes and procedures align with the FIRST PSIRT Services Framework, as well as other standards including ISO/IEC 29147:2018 and ISO/IEC 30111:2019.

Dell Technologies strives to address vulnerabilities in products, applications, and cloud services in the shortest commercially reasonable time. The exact timelines may vary depending on the specific vulnerability and its impact, such as the complexity of the vulnerability effort/impact to remediate. The Product Security Incident Response Team (PSIRT) coordinates the response and disclosure of all product vulnerabilities reported to us. All Dell Technologies product vulnerability disclosures are made available online at Dell Security Advisories, Notices, and Resources page. For more details on Dell's Vulnerability Response practices, see Dell's 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 Technologies, 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.

An industry leader in defining product security best practices and enhancing the cause of secure development.

Industry affiliations continued

- Dell Technologies is an active member of The Forum of Incident Response and Security Teams (FIRST). FIRST is a premier organization and a recognized global leader in incident and vulnerability response.
- Dell actively participates in The Open Group Trusted Technology Forum (OTTF). OTTF leads the development of a global supply chain integrity program and framework.
- 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.

Industry security standards

- Dell 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)
- The Forum of Incident Response and Security Teams (FIRST)
- The Open Group
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)

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

V. Conclusion

SupportAssist connectivity technology offers intelligent automation and remediation capabilities to enable maximum uptime for an organization's fleet of Dell desktop and laptop computers. Dell Technologies Services is able to provide this cutting-edge technology with optimal security by focusing on secure processes, secure data transmission, and secure data storage.

For questions and more information, visit **Dell.com/SupportAssist**

[1] For supported systems and requirements, please refer to our user guide (SupportAssist for Home PCs version for personal use) or administrator guide (SupportAssist for Business PCs version for PC fleet management) and click "supported PCs". Proactive and predictive capabilities depend upon your active service plan and Dell Technologies business rules. For ProSupport Suite for PCs capabilities, view our administrator guide and click "Connect and manage capabilities and Dell service plans". For Dell Care Suite, Premium Support Suite, or Alienware Care Suite for PCs capabilities, view the user guide and click "SupportAssist capabilities and Dell service plans".

[2] Based on Dell analysis, December 2023.