SupportAssist for business PCs

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

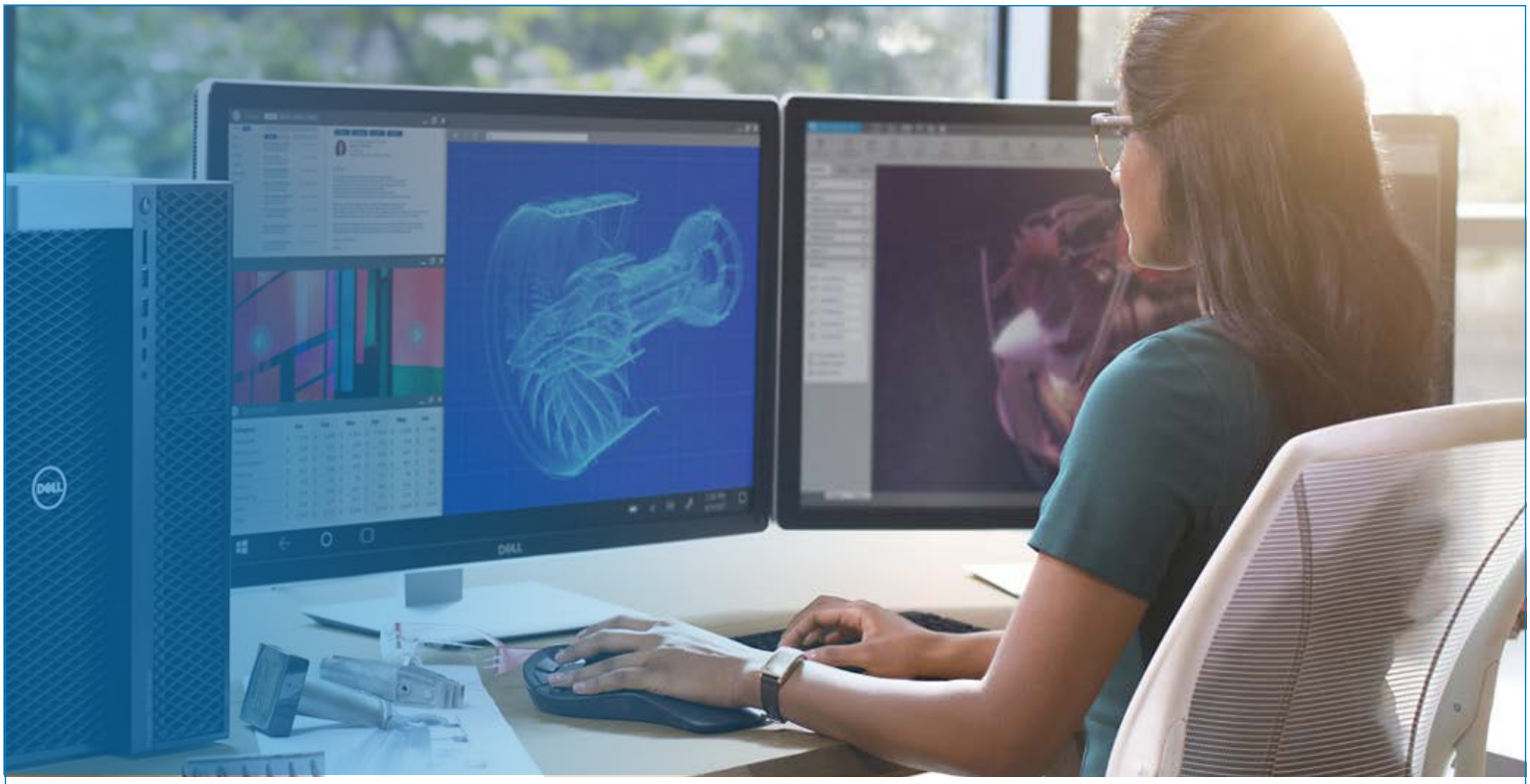
SupportAssist enables you to optimize your PC by removing unwanted files, optimizing network settings, tuning-up system performance, and removing virus and malware. It also identifies driver updates available for your PC.

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

Up to

60%

of IT leaders surveyed by Forrester leverage connectivity technology to reduce risk.



Content

I: Introduction

A failure on a laptop can be both disruptive and frustrating. Such problems can severely impact an employee's productivity, and often at the worst possible moment. Because of this, corporate CIOs have become increasingly concerned about the quality and uptime of their computer 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. This is accomplished by sending system state information from end-user systems to the company's IT department, or to a hardware or software vendor, to resolve issues as soon as they happen - or prevent them from happening at all. Dell ProSupport Plus with SupportAssist technology alerts you to a failing hard drive by providing a single control plane from TechDirect portal – HP and Lenovo do not.[3]

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 do we adhere to the GDPR and other standards?

This paper evaluates these and other related questions as a means of assessing new data science-enabled technologies. It provides a brief overview of how SupportAssist provides predictive and proactive support - the technology differentiating ProSupport Suite for PCs as the only complete support service able to predict and fix issues before they become problems. 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 the proactive and predictive technology[2] that enables an organization to receive automated technical support for its systems. It monitors end user devices, proactively detects both hardware and software issues and provides insight into system usage.

When it detects an issue, SupportAssist automatically opens a support request with technical support. Depending on the type of issue, the alert may initiate a technical support request or 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 is the only complete support service that combines priority access to expert support, accidental damage repair, and the ability to predict and fix issues before they become problems: Learn more.

Key Features

Automated

- Optimize PC and push appropriate driver updates from TechDirect portal
- PC utilization insights based on service plan when issues arise IT is alerted, often before the end user knows something is wrong.
- Replacement parts are dispatched automatically.
- Provides insight into system usage.

Proactive

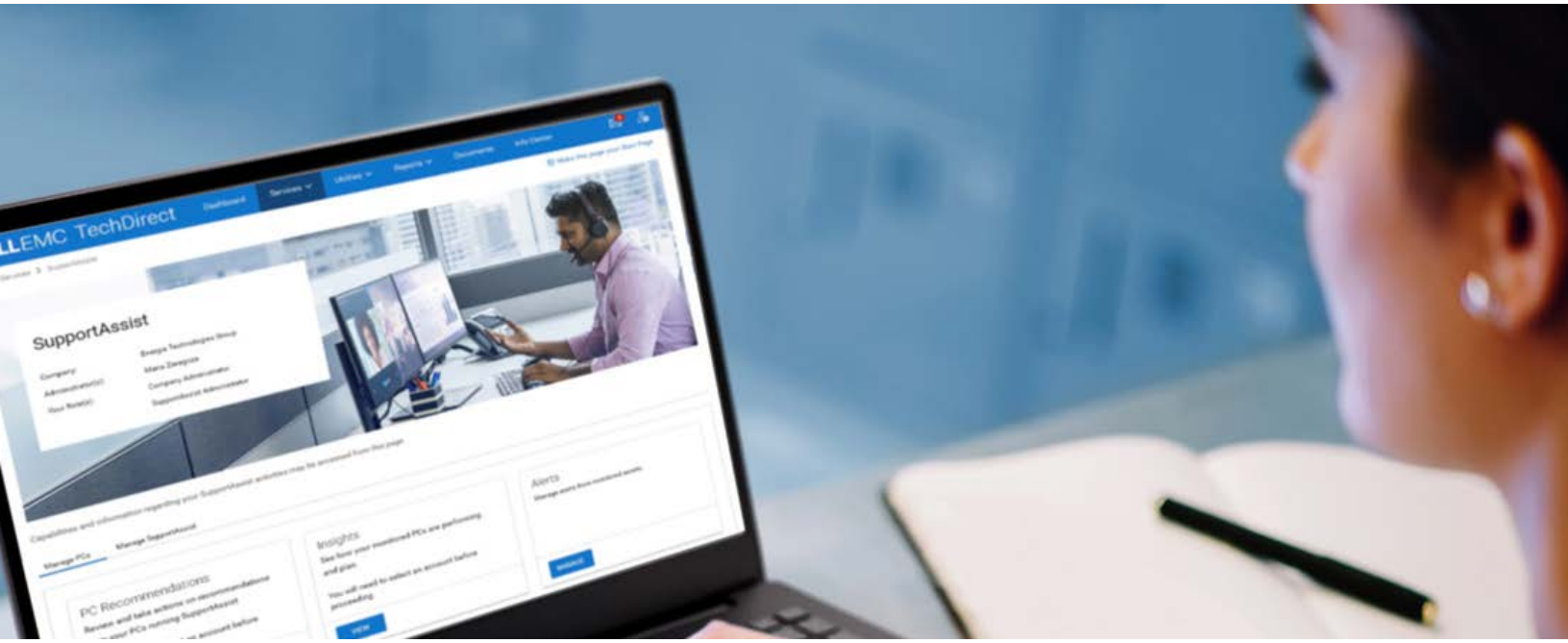
- Troubleshooting begins as soon as SupportAssist detects an issue.
- Technical support contacts the end user and starts resolving the issue.

Predictive

- Using predictive failure analysis, SupportAssist detects signs of an impending failure.
- Support cases are created automatically when issues are predicted, virtually eliminating unplanned downtime.[3]

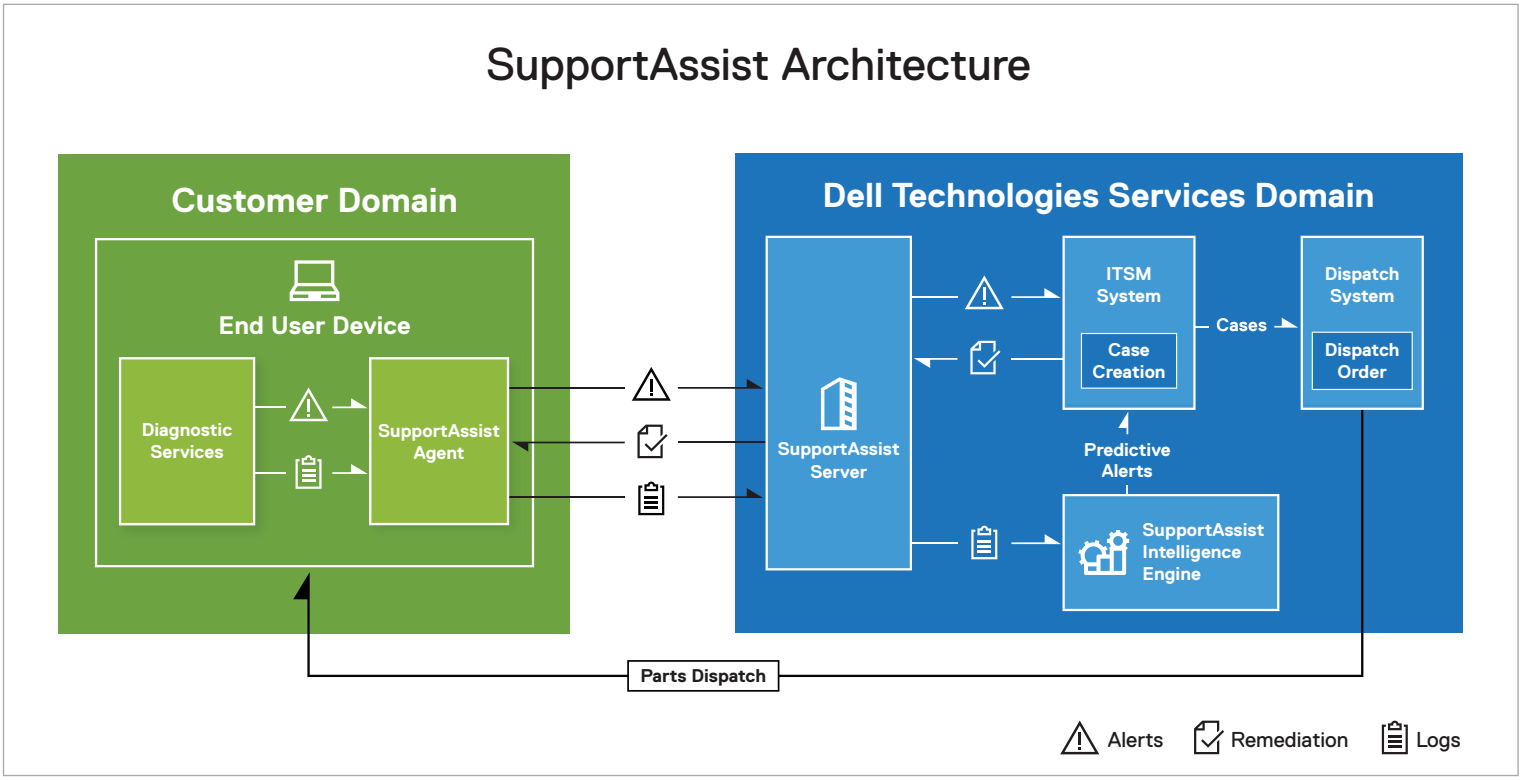
Available features vary based on the support plan purchased for a system.

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



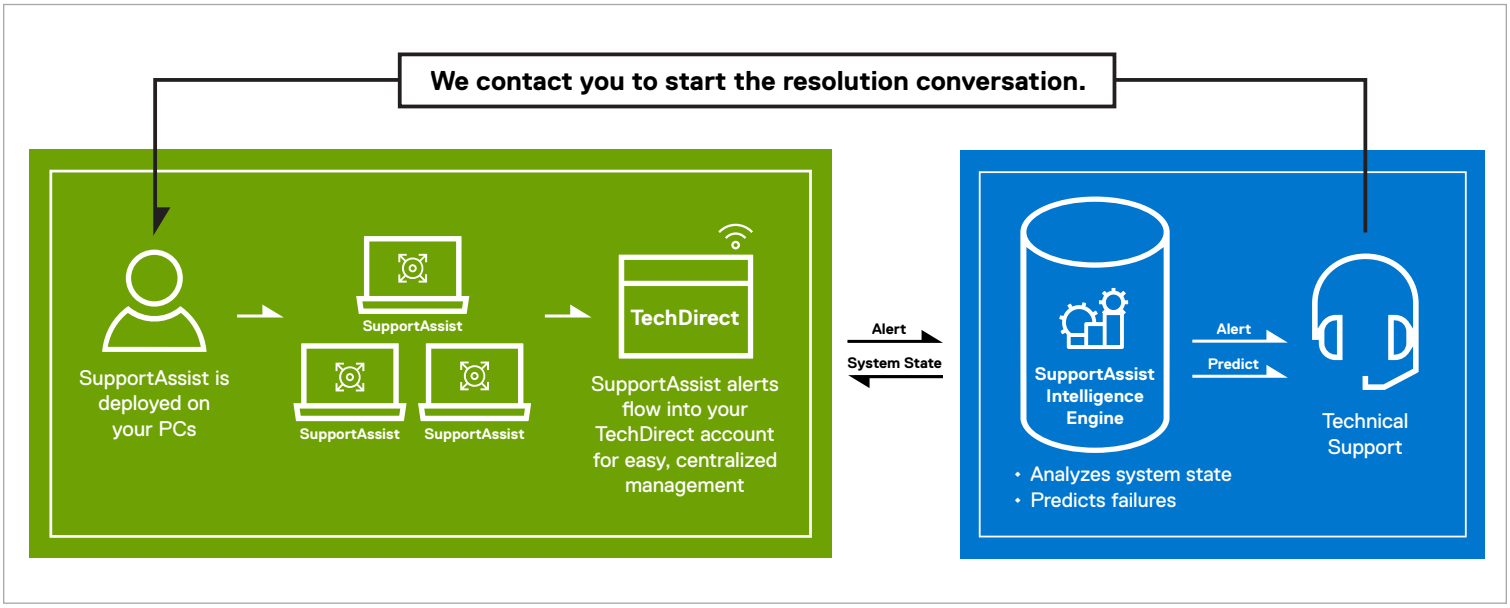
III. SupportAssist Architecture

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 the organization's IT department or to Dell Technologies Services to analyze the data and provide recommendations.



Centrally manage SupportAssist alerts 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.



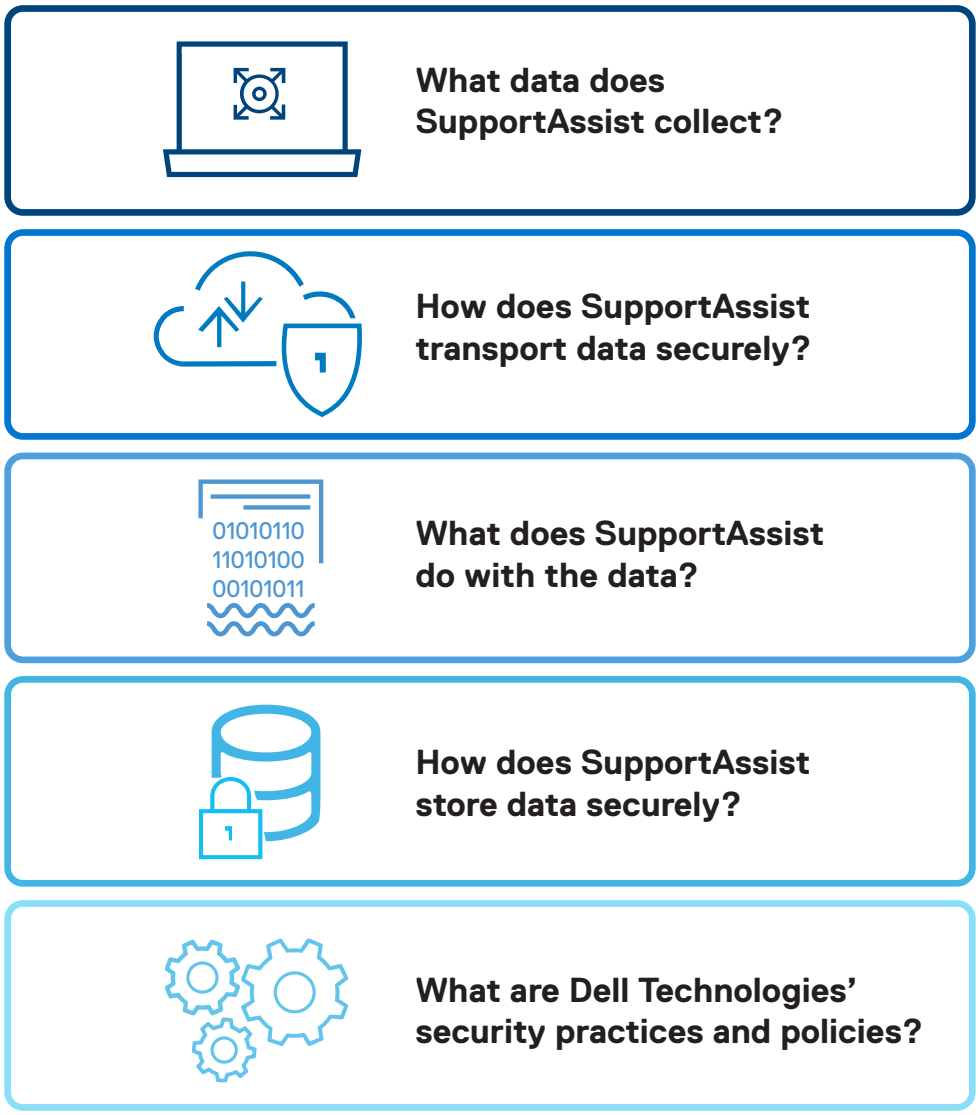
Centrally manage SupportAssist alerts using TechDirect continued:

A very useful analytic component of SupportAssist, called SupportAssist Insights, collects system utilization data that can be viewed within the TechDirect console. This includes CPU utilization, free drive space, maximum battery capacity, and battery runtime. 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 the following questions about what types of data are collected by SupportAssist for business PCs and how they are handled.

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, we use existing contact information that has been securely stored on 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
- **Source:** Source from where the alert was generated
- **Type:** Type of the alert, for example, predictive alert

Some SupportAssist data, such as CPU utilization, free drive space, maximum battery capacity, and battery runtime, is securely transported to the SupportAssist Intelligence Engine. PC utilization telemetry information CPU and memory utilization. In addition, the Insights component collects static and dynamic system, OS, network, application and memory information.

A complete list of system-monitoring data collected from an active system – including data collected outside of the routine 24 hour cycle – may be found here.

All information is protected by encryption during data transfer.

How does SupportAssist 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 for system information used in the restore process.

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 is used to secure transmittal of telemetry data, communication with a backend API on Dell.com, 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. Table 1 provides the average network bandwidth that SupportAssist utilizes for monitoring 100 systems for one month.

Table 1. Average data consumption

EVENT	FREQUENCY OF THE EVENT	DATA CONSUMPTION (IN KB)
Registering SupportAssist	Once after deployment	802
Sending routine PC monitoring information	Once every 24 hours after deployment	241
Sending periodic PC monitoring information	Every 30-45 days after deployment	210435
Sending alert and PC state information	When an alert is detected	30
Verifying PC warranty information	Once after deployment	7
Creating support request	When an alert qualifies for creation of a support request	159
Checking for updates	Once every week	30
Checking for configuration updates	Once every 24 hours	31
PC insights	Once every hour	2320

Note: For drivers, BIOS, and firmware updates, the data consumption value varies depending on the number of updates.

Physical and logical security measures keep stored data safe

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, and also to optimize operating system performance.

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

How does SupportAssist store data securely?

Physical security

Dell Technologies Services hosts most SupportAssist data, including the application, systems, network and security components, in a US-based data center designed to maintain high levels of availability and security. SupportAssist 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 SupportAssist is stored in compliance with the Dell Privacy Policy and transactional data is deleted after six months.

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.

- **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 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. No data is stored on the client after transmission.

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

Learn more about our Supply Chain Assurance practices here.

What are Dell Technologies' security practices and policies?

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.

SupportAssist code 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 Private Bug Bounty programme for SupportAssist for Business PC
- Assessment for authentication, authorization, and identity management solutions
- Open source libraries are reviewed and approved by our legal team. All third party libraries and components are being 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.

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 holistic and 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.

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, 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.

Change management

The Dell Technologies change management process follows ITIL Foundation best practices as dictated by its 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 hotfix 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.

Authentication

SupportAssist uses Dell MyAccount for authentication with Dell Technologies Services infrastructure/application 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.

SupportAssist undergoes regular third-party security validation testing with multiple best-in-class vendors including Private Bug Bounty.

Security-aware community

We offer 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, our 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

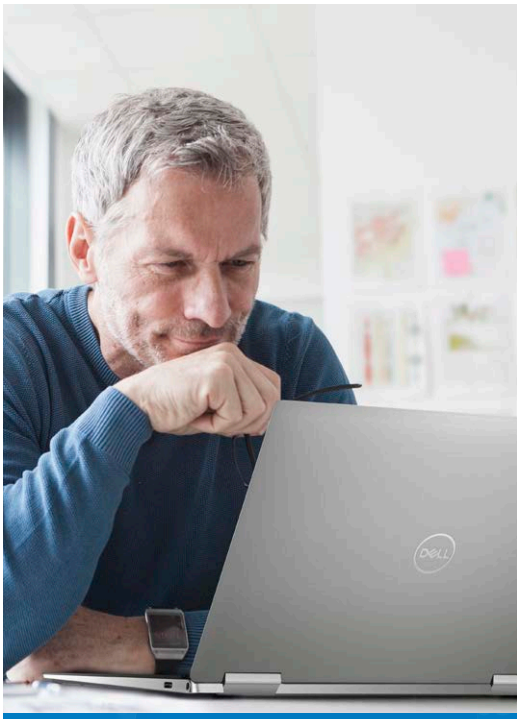
Anyone at Dell Technologies who observes suspicious activity or suspects a cybersecurity issue or threat is required to report the incident immediately to our Security Response Center (SRC). SRC will be our centralized Computer Incident Response Team (CSIRT).

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 and cybersecurity organizations provide access to the report and details of the breach to customers depending on the severity of the incident and the nature of the breach.

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.

Learn more about our
Vulnerability Response Policy



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

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 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.

Industry affiliations continued

- 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.

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)

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

V. Conclusion

SupportAssist technology offers both proactive and predictive 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 **DellTechnologies.com/SupportAssist**

[1]Source: "Innovation Leaders Need IT Services To Drive Transformative Outcomes" study conducted by Forrester Consulting on behalf of Dell EMC, October 2018.

[2]SupportAssist automatically detects and proactively alerts Dell to: operating system issues, software upgrades, driver updates and patches, malware, virus infected files, failures of hard drives, batteries, memory, internal cables, thermal sensors, heat sinks, fans, solid state drives and video cards. Predictive analysis failure detection includes hard drives, solid state drives, batteries and fans. Not available on Linux, Windows RT, Android, Ubuntu or Chrome based products.

[3]Based on a Principled Technologies test report, "Dell ProSupport Plus with SupportAssist warns you about hardware issues so you can fix them before they cause downtime" dated April 2019. Testing commissioned by Dell, conducted in the United States. Actual results will vary.

DELL Technologies