Technical Research Report

PROWESS

What Is the Best Supply-Chain Solution to Verify Server Configurations?

Prowess evaluated supply-chain solutions from Dell Technologies and HPE to determine which tool delivers the most value to enterprise teams when verifying server hardware as it arrives from the manufacturer.

Executive Summary

The supply chain can be a point of security vulnerability. For organizations purchasing servers, bad actors can replace genuine parts with counterfeits or can breach security by introducing malicious components.

Server manufacturers address these security risks by providing verification tools. These supply-chain tools allow IT or security teams to confirm that servers are genuine, unaltered, and will work according to specification upon arrival.

With supply-chain security threats on the rise, Prowess Consulting evaluated two supply-chain security tools with the goal of determining which one adds the most value for enterprise users. Prowess tested the Dell Technologies Secured Component Verification (SCV) Tool for Dell™ PowerEdge™ servers and the HPE Platform Certificate Verification Tool (PCVT) for HPE® ProLiant® servers.

Prowess determined that the Dell SCV tool offers more value. It is faster; the Dell SCV tool completes a verification test of a single server in 95 percent less time than the HPE PCVT while requiring 43 percent fewer steps.[1] The SCV tool can also verify a Dell PowerEdge server without the operating system yet installed on the server and with power off which increases efficiency. Prowess found the user interface of the SCV tool to be more intuitive. Additionally, the SCV tool offers support for Windows and Linux operating systems whereas the HPE PCVT supports only Linux. The Dell SCV tool also provides the ability to verify servers both locally and remotely and in a one-to-many configuration, and, finally, it provides more detailed test reports. This research study details these findings.

Supply Chain Security

Enterprise IT operations and security teams continue to battle cybersecurity attacks in the supply chain. When a server ships from factory to customer, malicious actors have the opportunity to insert components containing malware, or they can even replace components with counterfeits. In fact, 84 percent of organizations that responded to a recent Forrester Research survey consider hardware security and supply-chain security to be critically or very important to their business.[2] And cybercriminals are quick to find ways to get around strengthened security. Server manufacturers do a good job of securing their supply chains, but because of growing threats, organizations will always need to verify the configuration of servers on arrival.

Verification Tool Evaluation

Given growing supply-chain security threats and the importance of ensuring that a bad actor has not modified a server, Prowess Consulting evaluated two OEM supply-chain verification tools to determine which tool adds the most value for enterprises needing to verify server components:

- The Dell™ Secured Component Verification (SCV) tool, which verifies Dell™ PowerEdge™ servers
- HPE® Platform Certificate Verification Tool (PCVT), which verifies select HPE® ProLiant® servers

As IT and security teams run lean, supply-chain solutions like these should not only ensure the correct components have been shipped, but they should be quick, easy to use, and comprehensive. Prowess evaluated how easy it was to use each tool by examining the user interface (UI), documentation, and number of steps to verify a server. We also looked at other attributes of the tools, including operating system support, out-of-band verification capabilities, support for one-to-many verification and thoroughness of the verification reports.

How Does the Dell™ Secured Component Verification (SCV) Tool Work?

When a Dell™ server is ordered with Dell SCV, a process is run at the factory that identifies the server's components and their unique identification numbers. The factory then creates a cryptographic certificate with the inventory information. The certificate is a Trusted Computing Group (TCG)-compliant platform certificate. This certificate is transferred to a hardware crypto vault on the server. Once a server arrives at its destination, the customer can use the Dell SCV application to verify the server and its components. Unlike the HPE PCVT, the Dell tool does not require that an operating system be loaded onto the server, which is a more efficient approach to testing. Once this verification is completed, the application generates a report that lists any mismatched components. The Dell SCV tool can verify all Dell PowerEdge servers.

How Does the HPE® Platform Certificate Verification Tool (PCVT) Work?

When a select HPE ProLiant server is ordered (the HPE PCVT does not work on all ProLiant servers), the factory runs a process that records the server's components. This server configuration information is recorded on a TCG-compliant platform certificate. Once a server arrives at its destination, a customer can use the HPE PCVT to verify that the server configuration matches the information on the TCG-compliant platform certificate.

Validation Process

Prowess ran the Dell SCV tool against a Dell PowerEdge server and the HPE PCVT against an HPE ProLiant server. See Table A3 in the Appendix for the hardware configurations. The manual and automated validation processes used by the Dell SCV tool and the HPE PCVT are outlined in Table A1 and Table A2 in the Appendix.

Validation Measurements

Table 1 summarizes the time it takes to run each verification tool on a single server in a pass scenario. (A pass scenario is when all the components found in the server match the manifest created at the factory.) The Dell SCV tool requires 31 seconds while the HPE PCVT requires 659 seconds or close to 11 minutes.[1]

Table 2 summarizes the time to run each verification tool on a single server in a fail scenario. (A fail scenario is when a component is found in the server that does not match the manifest created at the factory.) The Dell SCV tool requires 28 seconds, whereas the HPE PCVT again takes 659 seconds, or close to 11 minutes.[1]

Reviewing Table 1 and Table 2 tells us that the majority of the HPE PCVT test time occurs in the manual part of the test. Tables A3 and A4 in the Appendix show the individual components of the HPE PCVT manual test time. This data gives us insight into the testing components that contribute the most to the higher test time: installing the tool, downloading certificates, and building the hardware manifest.

HPE PCVT manual test steps with time (from Table A3):[1]

- Download the tool: 3 seconds
- Install the tool: 216 seconds
- Download certificates: 315 seconds
- Build the hardware manifest: 93 seconds
- Validation: 30 seconds

Table 1 | Prowess validation measurements (single server, pass scenario)[1]

Process Components	Dell™ SCV Tool	HPE® PCVT
Manual process		
Manual process time (seconds)	22	657
Automated process		
Automated process time (seconds)	9	2
Total process time		
Total process time	31	659

Table 2 | Prowess validation measurements (single server, fail scenario)[1]

Process Components	Dell™ SCV Tool	HPE® SCVT
Manual process		
Manual process time (seconds)	22	657
Automated process		
Automated process time (seconds)	6	2
Total process time		
Total process time	28	659

Table 3 illustrates the number of steps to run each tool. The HPE PCVT requires six IT admin manual steps, versus only three for the Dell SCV tool. Note that the automated test portion is counted as a single step for both tools.

Table 3 | Manual and automated steps required to run each tool[1]

Process Components	Dell™ SCV Tool	HPE® PCVT	Comments
Manual process			
Manual process steps	3	6	The Dell SCV tool requires 50% fewer manual steps taken by an IT admin.
Automated process			
Automated process steps	1	1	The tools are at parity.
Total process time			
Total process steps	4	7	The Dell SCV tool requires 43% fewer total steps taken by an IT admin.

Figure 1 illustrates the difference in testing time between the Dell SCV tool and the HPE PCVT. The SCV tool requires 95 percent less time. Figure 2 illustrates the difference in test steps between the Dell SCV tool and the HPE PCVT. The SCV tool requires 43 percent fewer steps.[1]

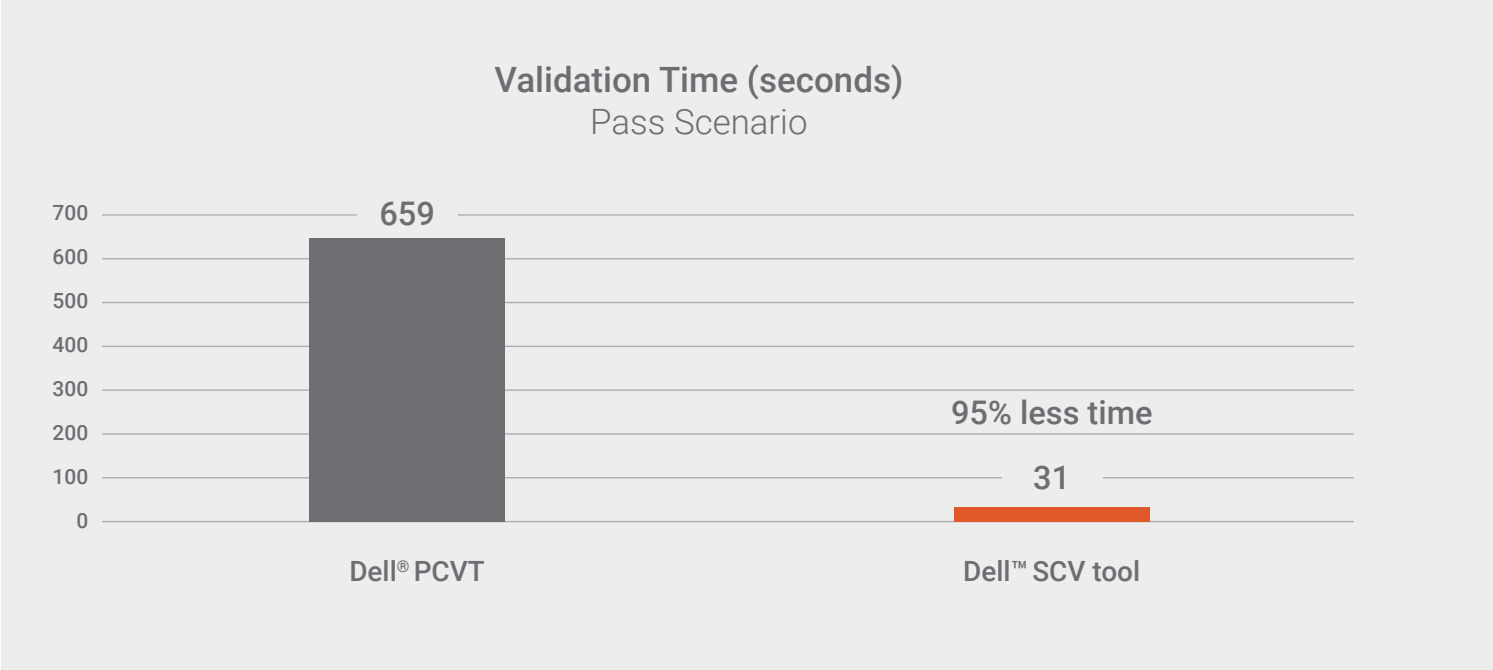

Figure 1 | The Dell™ SCV tool requires 95 percent less time than the HPE® PCVT[1]

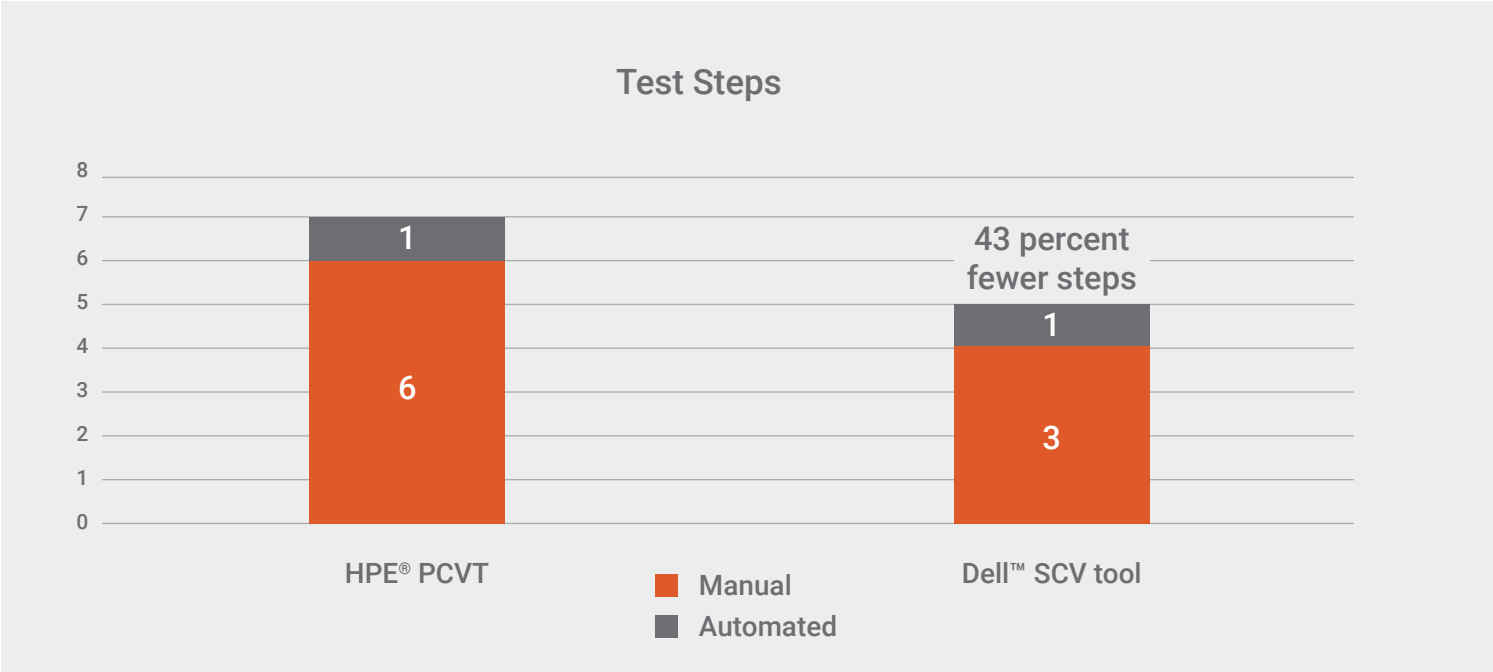

Figure 2 | The Dell™ SCV tool requires 43 percent fewer steps than the HPE® PCVT[1]

Observations

In addition to test time, Prowess assessed the tools across six other categories: security, ease of use, operating system support, out-of-band verification including one-to-many verification, scale-out verification, and reporting. Understanding what each tool offers within each category builds a complete picture of its value.

Security

Both the Dell Technologies and HPE tools support cryptographic verification. This means that the information about the components within each server is encrypted and saved in the server before it is shipped. This encrypted information is accessed at the receiving end to confirm that the same parts installed at the factory are intact in the server when it arrives at the customer site.

Dell Technologies Process

Dell Technologies generates a certificate that contains unique system component IDs during the factory assembly process. This certificate is signed in the Dell Technologies factory and is encrypted and stored in the Integrated Dell™ Remote Access Controller (iDRAC), the Dell™ server-management tool. The certificate is later downloaded and used by the Dell SCV application.

The Dell SCV tool validates the system inventory against the Dell SCV certificate. The tool generates a validation report detailing the inventory matches and any mismatches against the Dell SCV certificate. It also verifies the certificate and chain of trust, along with the proof of possession of the Dell SCV private key for iDRAC.

HPE Process

HPE issues a platform certificate at the factory. The platform certificate is an attribute certificate signed and encrypted by HPE. When the server arrives at its destination, the customer can use the HPE PCVT to verify the server's hardware manifest against the platform certificate. The tool generates a validation report listing failed certificates.

Ease of Use

The Dell SCV tool is designed to run quickly and easily (and remotely) from a simple UI. An entry-level sysadmin could be tasked with verifying PowerEdge servers with this tool. While it is easy to run the verification tool, the quality of the output is comprehensive. Additionally, multiple servers can be verified from a single host in a one-to-many verification scenario.

We found that the HPE PCVT, on the other hand, might require more advanced knowledge and skills for effective use. For example, this tool requires knowledge of the Go programming language to run the script for building the custom DiskScan library. Also, Prowess identified dependencies—both files and software needed for the program to run—that were not listed in the HPE PCVT documentation.

A Dell server can be verified with the Dell SCV tool either locally or remotely from a host machine. An HPE server can only be verified locally with the HPE PCVT.

Operating System Support

The Dell SCV tool supports both select Windows operating systems and Linux distributions, whereas the HPE verification solution only supports select Linux distributions. The Dell SCV tool supports Red Hat® Enterprise Linux 8.x, Red Hat Enterprise Linux 9.x, and SCVApp for Windows Server® 2019 and Window Server 2022. The HPE PCVT supports the CentOS® Linux distribution.

Out-of-Band Verification

The Dell SCV solution supports out-of-band verification. This means that an IT admin can control a PowerEdge server from a host if the server has a working iDRAC connection. The IT admin can verify the server configuration, even if the server is powered off or does not have an operating system installed. In addition to out-of-band verification, the Dell Technologies solution supports one-to-many verification. The Dell SCV tool allows a system admin to open multiple Dell SCV sessions, one per server, and run the verification test.

The HPE solution does not support out-of-band verification. The HPE PCVT must run on the server itself, which requires that an IT admin power up the server and install the Linux OS prior to verification. It also does not support one-to-many verification.

Scale-Out Verification

Prowess looked at scaling out verification in the case that tens or hundreds of servers needed to be verified. When more than one server needs to be verified, the fact that the Dell tool can the server configuration even if it is powered off or does not have an operating system installed drives huge time savings.

Verifying 10 Servers:

Dell scenario:[1]

- Open 10 shells to run tests: approximately 30 seconds
- Set up and run parallel verification on 10 servers using the one-to-many configuration through iDRAC connections: 31 seconds/server x 10 servers = 31 seconds
- Total is approximately 30 seconds + 31 seconds: approximately 1 minute

HPE PCVT scenario:[1]

- Set up and run an 11-minute verification test on 10 servers serially: 11 minutes/server x 10 servers = 110 minutes
- Total: 110 minutes or nearly two hours

Verifying 100 Servers

Dell SCV scenario:[1]

- Open 100 shells to run tests: approximately 5 minutes
- Set up and run parallel verification on 100 servers using the parallel one-to-many configuration through iDRAC connections: 31 servers x 1000 servers = 31 seconds
- Total: Approximately 5 minutes + 31 seconds = approximately 6 minutes

HPE PCVT scenario:[1]

- Set up and run the 11-minute verification test on 100 servers serially: 11 minutes/server x 100 servers = 1,100 minutes
- Total: 1,100 minutes or more than 18 hours

Reporting

The Dell SCV tool provides a robust report that documents any missing or modified hardware components. The HPE PCVT report reveals only whether certificates on the server under test (SUT) have changed—it does not list which components are missing or modified. As seen in Figure 4, the missing hardware description in the HPE tool is just a line item under "Platform Components Verification Status," instead of the full component-by-component breakdown that the Dell SCV tool provides (Figure 3).

```
C:\Program Files\Dell\SCVTools>scv validatesysteminventory -r 172.17.40.89 -u root -p calvin
Downloading SCV Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "C4CT5S3" matches Certificate: Match
Validating System Inventory: Mismatch
---------------------------------------------------------------------
Mismatch Inventory Summary
---------------------------------------------------------------------
Memory 9: Mismatch
Memory 10: Mismatch
Memory 11: Mismatch
Memory 12: Mismatch
Memory 13: Mismatch
Memory 14: Mismatch
Memory 15: Mismatch
Memory 16: Mismatch
HardDrive 4: Mismatch
HardDrive 5: Mismatch
Network 5: Mismatch
Network 6: Mismatch
PCIE 1: Mismatch
---------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_C4CT5S3_2022_12_09_13_23_56.log
---------------------------------------------------------------------

C:\Program Files\Dell\SCVTools>
```

Figure 3 | The Dell™ SCV tool outputs details on failed components

Figure 4 | The HPE® PCVT only reports that the platform components are invalid

Findings

Based on testing and observations, Prowess determined that the Dell SCV tool delivers more value to server customers than the HPE PCVT. The following list is a summary of our findings.

- The Dell SCV tool offers cryptographic verification of components, extending supply-chain security to the customer sites to deploy PowerEdge servers confidently and rapidly. The Dell SCV tool runs a verification test in 95 percent less time than the HPE PCVT and requires 43 percent fewer steps.
- The Dell SCV tool takes less than a minute (31 seconds) to verify a PowerEdge server and to deliver in-depth results. The HPE PCVT takes almost eleven minutes (659 seconds) to verify an HPE ProLiant server and to deliver bare-bones results.
- The Dell SCV tool's hardware-integrity-verification process is more automated and takes fewer steps and administration as compared to the HPE solution. The Dell SCV tool takes four steps to verify a PowerEdge server, whereas the HPE PCVT takes seven steps to verify an HPE ProLiant server.
- Because of its simple UI and robust documentation, the Dell SCV tool can be used by an entry-level system admin, whereas the HPE PCVT will require a more skilled system admin due to its more complex setup process.
- The Dell SCV verification solution supports more operating systems than the HPE PCVT verification solution. The Dell SCV tool supports Red Hat® Enterprise Linux 8.x, Red Hat Enterprise Linux 9.x, and SCVApp for Windows Server® 2019 and Window Server 2022. The HPE PCVT supports the CentOS® Linux distribution.
- The Dell SCV tool supports out-of-band capabilities, meaning it can verify a PowerEdge server that does not yet have the OS installed. The HPE PCVT requires that an OS be installed.
- The Dell SCV tool allows a system admin to open multiple Dell SCV sessions, one per server, and verify servers in parallel without loading an OS on the SUTs. For example, if 10 servers are configured for testing, the entire setup and test would take approximately one minute. On the other hand, the HPE PCVT verifies servers serially. It requires approximately 11 minutes to set up and run the verification test for each server. Thus, to verify 10 servers with the HPE PCVT would require approximately 110 minutes or nearly two hours.
- When comparing pass-fail scenarios for the Dell SCV tool versus the HPE PCVT, we found that the Dell SCV tool provides a more robust and comprehensive hardware-verification report for the fail scenario. Specifically, the Dell SCV tool documents which components fail, whereas the HPE PCVT only documents that certificates are incorrect.

Conclusion

When choosing a server vendor, IT and security teams should be aware of tools that can make ownership easier to drive costs down. The Dell SCV tool can deliver superior value when compared to the HPE PCVT across seven categories: test time, security, ease of use, OS support, out-of-band support and one-to-many verification, scale-out verification, and reporting. With the Dell SCV tool, organizations that want to keep their supply chain secure have another reason to purchase PowerEdge servers.

Appendix

Table A1 | Steps to manually validate configurations

HPE® PCVT Process		Dell SCV Tool Process	
Step	Manual	Step	Manual
1	Download the HPE PCVT.	1	Download the Dell SCV validation app.
2	Install the HPE PCVT on the server.	2	Install the Dell SCV app on the server.
3	Download the encrypted certificates issued by the HPE factory from HPE Integrated Lights Out (iLO®) tool using Redfish® APIs. HPE uses an iLOREST tool to connect to iLO and utilize the Redfish APIs.	3	Run the validation command.
4	Save the certificates into the HPE PCVT directory.		
5	Use the PCVT tool to generate a hardware manifest, create a folder, run a collection, and then export the results to the HPE PCVT.		.
6	Run the validation command.		

Table A2 | Steps to automatically validate configurations

HPE® PCVT Process		Dell SCV Tool Process	
Step	Automated	Step	Automated
1	Compare the hardware manifest to the certificate manifest.	1	Download the certificate generated at the factory from its storage place in the Integrated Dell™ Remote Access Controller (iDRAC).
	Verify the platform certificate signature and then the chain of trust to the HPE Root CA.		Verify the Dell SCV signature and chain of trust.
	Verify the system's initial attestation key (IAK) certificate and then the chain of trust to the HPE Root CA. Save certificates into the HPE PCVT directory.		Challenge iDRAC for proof of possession of the Dell SCV certificate private key.
	Verify the system Initial Device Identifier (IDevID) certificate and then the chain of trust to the HPE Root CA.		Collect current inventory.
	Output a status for each step.		Compare the current inventory to the certificate inventory.
			Output a status for each step.

Table A3 | Prowess validation time measurements (pass scenario)

Process Components	Dell™ SCV Tool Time (Seconds)		HPE® PCVT Time (Seconds)
Manual process		Manual process	
Download the tool	2	Download the tool	3
Installation	15	Installation	216
Validation	5	Certificates	315
		Build the hardware manifest	93
		Validation	30
Manual process time (seconds)	22	Manual process time (seconds)	657
Automated process	**Dell SCV Tool Time (Seconds)**	**Automated process**	**HPE PCVT Time (Seconds)**
Download from iDRAC	1	Verify the manifest	<1
Verify Dell SCV signature	2	Verify the platform certificate	<1
Challenge Integrated Dell™ Remote Access Controller (iDRAC)	1	Verify the IAK certificate	<1
Collect inventory	2	Verify the IDevID certificate	<1
Compare inventory	1	Status	<1
Status	2		
Automated process time (seconds)	9	Automated process time (seconds)	2
Total process time			
Total process time	31	Total process time	659

Table A4 | Prowess validation time measurements (fail scenario)

Process Components	Dell™ SCV Tool Time (Seconds)	Process Components	HPE® PCVT Time (Seconds)
Manual process		Manual process	
Download the tool	2	Download the tool	3
Installation	15	Installation	216
Validation	5	Certificates	315
		Build the hardware manifest	93
		Validation	30
Manual process time (seconds)	22	Manual process time (seconds)	657
Automated process	**Dell SCV Tool Time (Seconds)**	**Automated process**	**HPE PCVT Time (Seconds)**
Download from Integrated Dell™ Remote Access Controller (iDRAC)	1	Verify the manifest	<1
Verify Dell SCV Signature	1	Verify the platform certificate	<1
Challenge iDRAC	1	Verify the IAK certificate	<1
Collect inventory	1	Verify the IDevID certificate	<1
Compare inventory	<1	Status	<1
Status	2		
Automated process time (seconds)	6	Automated process time (seconds)	2
Total process time		**Total process time**	
Total process time	28		659

Table A5 shows the server configurations. However, these configurations are not relevant to the test time results. The verification tools are run on a baseboard management controller (BMC), which is a small, specialized processor.

Table A5 | Server configurations

	Dell™ PowerEdge™ R760	HPE® ProLiant® DL360 Gen10 Plus
CPU	Intel® Xeon® Gold 6430 processor	Intel® Xeon® Gold 5317 processor
Number of CPUs	2	1
Cores/threads per CPU	32/64	12/24
Cores/threads total	64/96	12/24
Frequency (Base/SCT/MCT)	3.4 GHz	3.0 GHz
Storage controller 01	Dell™ PowerEdge RAID Controller (PERC) 965i	HPE® Smart Array® E208i-a SR Gen 10
Disk	480 GB Dell™ NVM Express® (NVMe®) ISE 7400	800 GB SAS SSD
Number of disks	2	2
Storage controller 02	Not application (N/A)	N/A
Disk	1.92 TB Dell™ NVMe® CM6 RI	N/A
Number of disks	2	N/A
Storage controller 03	N/A	N/A
Disk	3.2 TB Dell™ NVMe® V2 AGN MU.2	N/A
Number of disks	2	N/A
Installed memory	1,024 GB	64 GB
Memory DIMM	DDR5	RDIMM
Memory speed	4,400 megatransfers per second (MT/s)	3,200 MHz
Number of memory DIMMs	16	4
OS	CentOS®	CentOS®
OS version	8.6	8.6
OS kernel	4.18.0-372	4.18.0-372
BIOS	0.2.29	SMBIOS 3.4.0

[1] Based on Prowess testing as of December 2022. For testing and configuration details, see the Appendix. Results may vary.

[2] Forrester Research, Inc., "BIOS Security – The Next Frontier for Endpoint Protection." Commissioned by Dell Technologies. June 2019. www.delltechnologies.com/asset/en-ae/solutions/business-solutions/industry-market/dell-bios-security-the-next-frontier-for-endpoint-protection.pdf.