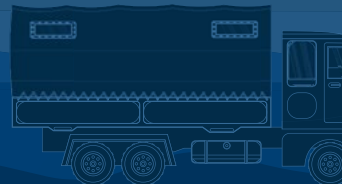
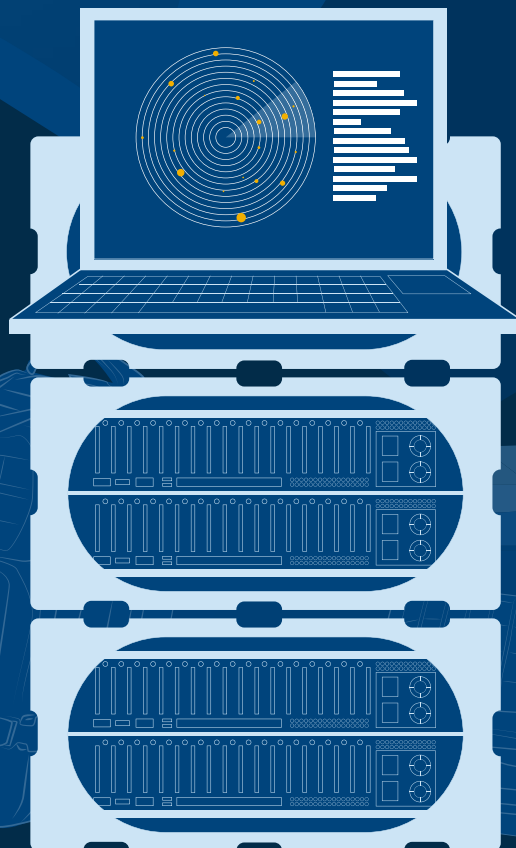
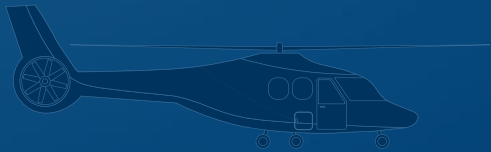


DELLTechnologies

Meet Changing Mission Requirements by Designing Solutions for the Rugged Edge



intel



Introduction

More work than ever is getting done in remote, unconventional and rugged settings outside of federal office buildings. No matter the environment, employees must have access to the technology they need to meet mission requirements. That might mean standing up a small data center in unusual places, such as a tank, relying on rugged technology that can withstand extreme conditions or shoeorning an entire computing environment into the overhead bin of a commercial airplane.

These scenarios have one thing in common: They require collecting and analyzing data in non-traditional IT environments. In many cases, commercial off-the-shelf (COTS) technology cannot meet these requirements. For example, if an agency needs technology that will be exposed to tough weather conditions such as high humidity, dust or extreme cold, a standard laptop or server likely won't work. The same challenges can arise in bumpy, shaky environments, like moving vehicles. Or perhaps users are looking for infrastructure customized to fit in small, constricted spaces, or within the confines of very strict security guidelines.

For many federal agencies and integrators, meeting today's unique mission needs requires further customization. This could mean reducing the size of a server by 75% or reconfiguring a mobile device to incorporate strict security measures.

To learn more about how federal systems integrators, technology and solution providers for Defense and federal agencies are designing and using IT in non-traditional IT environments, GovLoop partnered with Dell Technologies OEM Solutions and Intel to produce this survey. Without a doubt, the need for customization is on the rise:

- › 41% of respondents said that they had already begun using IT in non-traditional environments, and another 27% were very interested in doing so (see Figure 1)
- › Of those doing so, 42% said their use of IT in non-traditional environments has grown significantly in the last two years (see Figure 2)
- › And nearly 70% said it would grow significantly over the next two to four years (see Figure 3)

This report explores what agencies are looking for — and how industry is stepping up.

Agencies are more interested than ever in deploying IT in non-traditional IT environments. Here is what they said:

Figure 1: To what extent are you looking to deploy IT in non-traditional IT environments?

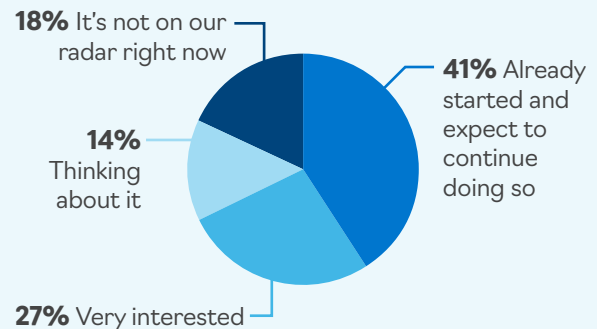


Figure 2: How has your use of IT in non-traditional IT environments changed over the last two years?

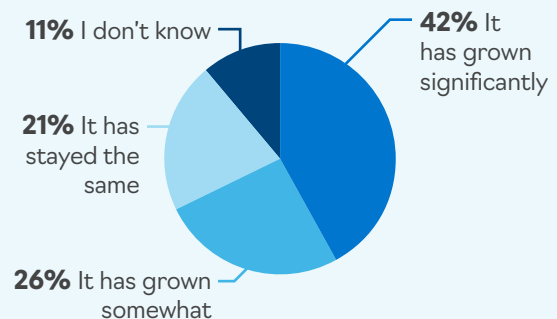
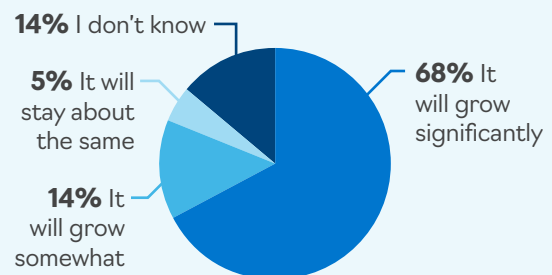


Figure 3: How do you expect the need to deploy IT in non-traditional environments to change over the next 2–4 years?



Here are a few definitions to keep in mind as you read:

Federal system integrator (FSI): an organization that builds or develops IT systems for federal agencies by combining some combination of hardware, software, networking and storage, often from multiple vendors. Examples include Leidos, Raytheon and General Dynamics, etc.

Technology and solution provider for Defense: an organization that makes devices from component parts acquired from other organizations, or produces parts and equipment that may be incorporated into solutions from another company. Examples include Dell Technologies, VMware, Thales, Digistor, Tracewell Systems, etc.

Federal/government agency: an organization responsible for the oversight and administration of specific functions. Examples include the Department of Defense (DoD), Army, Navy, Air Force, Department of Homeland Security, etc.

Operating at the Edge

For federal systems integrators and agencies — especially those that rely on immediate access to data to carry out successful missions safely — having the right information at the right time is critical.

Think about a Humvee with servers in the back, allowing Army personnel to process data and make decisions while on the move. Or an embedded computer inside a Navy ship, collecting and processing data while at sea. Agencies are taking advantage of information straight from the source — or as close to it as possible — to make time-critical decisions.

By collecting and analyzing information as close to the source as possible — often called edge computing — data can be processed in real time. This can be especially helpful in enabling decision-makers outside of traditional work environments to get things done quickly. It's a model that works well on the battleground, in a temporary mobile office, on an airplane, in a tank, often in rugged conditions, to make the right decisions based on current information, all with enterprise-level security.

According to the survey, the top driver for edge computing is the need to deploy computing capabilities closer to people or systems in the field. It also is seen as a way to support a more mobile workforce (see Figure 4).

Artificial intelligence (AI) and machine learning (ML) are important parts of effective edge computing. Instead

of residing in a typical data center environment, AI/ML capabilities can be embedded in sensors, gateways and other devices near the edge. Or, for example, a mobile user using edge data to make informed decisions might get help from a small form factor server imbued with AI/ML capabilities.

DoD has enthusiastically embraced AI and ML, using it for everything from threat detection to unmanned vehicles. The department continues to incorporate AI and ML into operations across key mission areas to enhance military decision-making, improve situational awareness and increase the safety of operating equipment and streamline business processes. In the area of predictive maintenance, for example, the military is using sensors combined with AI to predict parts failures, automate diagnostics, plan maintenance, provision spare parts and optimize inventory levels.

The lower latency, greater bandwidth and higher capacity of 5G wireless combined with devices and sensors on site can help support real-time applications, accelerating deployments at the edge. DoD considers 5G a foundational enabler for all U.S. defense modernization programs and recently awarded \$600 million for 5G experimentation and testing at five U.S. military sites. Projects include testing 5G-enabled smart warehouses, piloting 5G-enabled augmented/virtual reality for mission planning and training, and evaluating 5G technologies to enhance distributed command and control.

Our survey found that agencies are looking for technology solutions and capabilities that will help them operate efficiently at the edge.

Figure 4: What is driving the need in your agency to deploy IT in non-traditional environments? Respondents ranked options from highest to lowest need. Scores reflect cumulative distribution of rankings.

#1 Need to deploy compute capabilities closer and/or in the field (Cumulative score: 85)



#2 More mobile workforce (77)



#3 A need to incorporate advanced capabilities into field systems (68)



#4 Improving intelligence/data gathering (55)



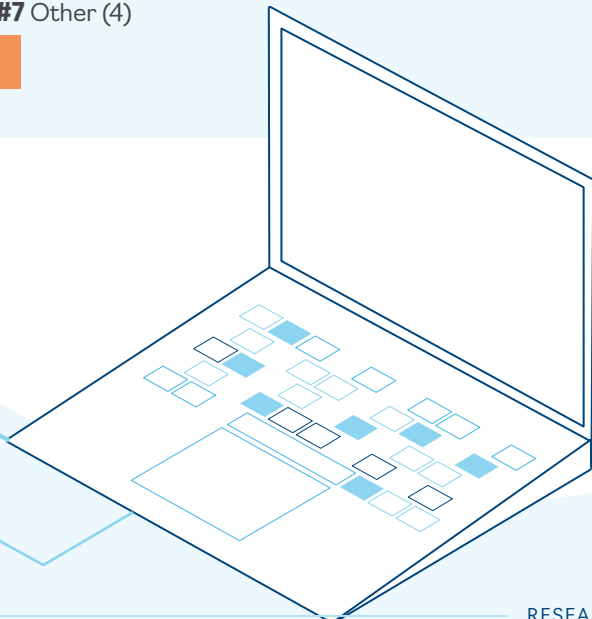
#5 Growing interest in Edge/Internet-of-Things (IoT) type of applications (53)



#6 Rugged solutions for dirty, dusty, harsh environments (37)



#7 Other (4)



Getting Exactly What You Need, Every Time

Analyzing data at the edge is helping many agencies make time-critical decisions. For example, the Agriculture Department is using edge computing to collect and analyze farming data, and the Federal Emergency Management Agency (FEMA) uses it in the field to help control the spread of diseases and viruses. But DoD may stand to gain the most from edge computing. Many military organizations are using edge computing in some capacity, and more are adopting the technology every year.

At the same time that agencies are embracing edge computing, vendors are developing innovative solutions to meet their needs. [Digital Harmonic's PurePixel](#), for example, enhances images to support threat detection and mitigation and uses ML for parameter optimization to automatically adjust their algorithms for the best possible output, while [Kinetica](#) developed a preconfigured solution that runs location-based and predictive analytics on both structured and unstructured data streams at the edge.

Even edge computing, however, has its limits under harsh conditions, or when personnel must operate in extremely confined spaces. In those cases, agencies need customized solutions designed for these unique environments. For example, even if an agency settles on a small form factor appliance that can fit in a backpack and withstand extreme environments, it may find that the unit doesn't have the additional security capabilities it needs. In those cases, agencies can partner with technology leaders like Dell Technologies OEM Solutions and Intel to develop exactly what they need.

"There are times when enabling insights at the edge requires more than the typical set-up," said Pete Miasiaszek, an account executive with Dell Technologies OEM Solutions. "It might require an extremely small footprint, or have to meet highly specialized security requirements or be able to withstand shock and vibration, extreme humidity or very dusty conditions."

The value of edge computing will only grow over time. According to [IDC](#), governments collect more data than any other industry, and most data is now collected at the edge. With the right technology to collect and analyze data at the edge, agencies can use that data to make mission-critical, real-time decisions.

Meeting Mission Goals on the Go

No area of the federal government conducts more daily business outside of the confines of an office building than the defense and intelligence communities. Whether in planes, jeeps, portable shelters or on the battlefield, missions must be accomplished regardless of obstacles.

The limitations of non-standard work environments can make it difficult for staff to use standard, off-the-shelf technology to do their jobs. Yet the missions are important, and workers need the right technology to accomplish those missions.

Dirty, dusty, wet, cold, hot, humid or unstable environments are common, especially in the military. As a result, the armed services typically require manufacturers to adhere to specific certifications around shock, vibration and temperature. That means that missions requiring this type of ruggedness can get exactly what they need.

If a mission needs a small, powerful server that can withstand vibration and harsh environments, for example, it can use devices tailored to fit their unique requirements. If soldiers need rugged tablets connected to roof-mounted antennas on a jeep to keep in constant communication while continuously collecting data, those devices can be developed specifically for that use.

Unique security requirements are another issue that traditional technology often can't accommodate. For example, a classified mission might specify hot-swappable solid state drive cards – something laptops usually don't provide. A mission might also require more physical security measures, such as locks or external casings. A top-secret mission may require mobile phones with certain capabilities disabled to ensure sensitive data remains protected. Respondents identified cybersecurity capabilities as their top priority (see Figure 5).

Figure 5: What features are most important for your non-traditional IT environments? Respondents ranked options from highest to lowest need. Scores reflect cumulative distribution of rankings.

#1 Cybersecurity capabilities (Cumulative score: 104)



#2 Compact and lightweight (103)



#3 Unique form factors that fit small spaces, such as hospital rooms, vehicles, transit cases, etc. (65)



#4 High CPU processing (61)



#5 Compliance with requirements specific to our organization, along with broader requirements, such as MIL-STD-810G (51)



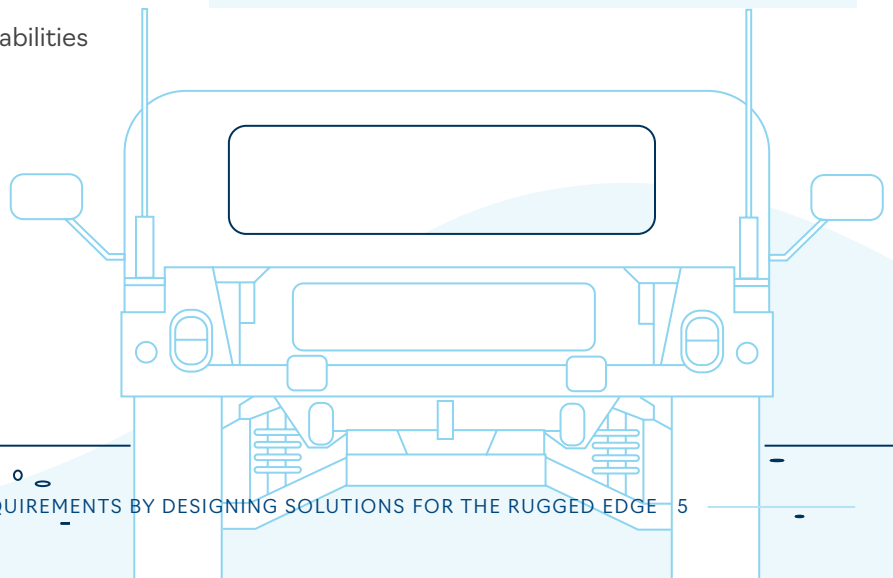
#6 Standardized COTS 1U/2U rack servers rugged products for dirty, dusty, wet, cold, hot, shaky environments (42)

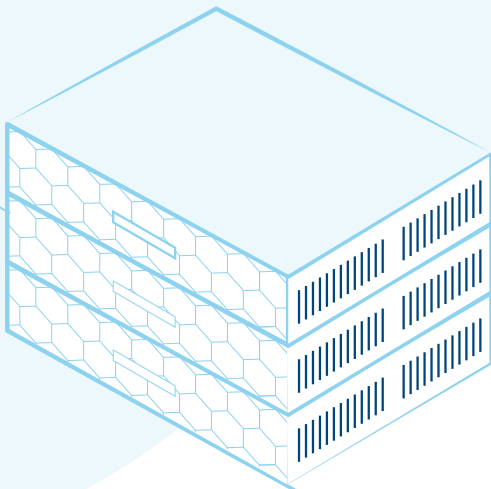


#7 Low power CPU processing (22)



#8 Accelerators FPGA/GPU (18)





Sometimes the challenge is something as seemingly simple as space constraints. A mobile hospital might have limited space for the technology required to run the facility, or a temporary command and control station may need to squeeze a lot of technology into a very small space. A situation might call for a lightweight, compact server that can fit into a transit case, or a laptop.

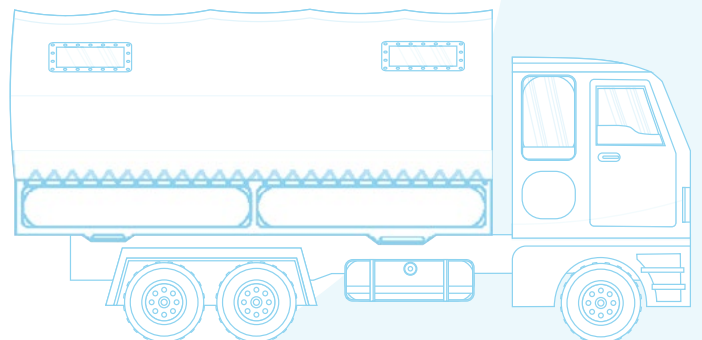
Most traditional data center products are too large to fit in these kinds of environments. Instead, the situation might call for technology with the same features and performance as full data centers – a small one-box data center that integrates computing, storage, networking and virtualization.

Sometimes, requirements call for a combination of these capabilities. For example, to ensure soldiers in the field can continue flight training they may have started at a base, they would need small, compact systems with full functionality. That might require packing capabilities for virtual reality, along with access to applications and data that enrich the experience. And because the training is taking place in the field, the entire unit must be hardened and ruggedized.

"It's about solving agencies' unique needs and requirements on standard solutions and architectures," said Greg Rahaman, Engineering Manager for Dell Technologies OEM Solutions. "If an agency wants to standardize on a single compute form factor yet wants to be able to quickly swap out components, they should be able to do that. If they want a small transit case solution with multiple CPU sockets and need field-replaceable parts coming out of the front for service and accessibility, they should have that available to them."

Civilian agencies are feeling the same need for customized solutions for use in non-traditional IT environments. Here's what respondents said in the survey:

- › Most have either begun deploying IT in non-traditional IT environments or are very interested in doing so.
- › Top use cases for deploying IT in non-traditional IT environments are training and simulation, mobile solutions in transit cases, and telecommunications/command and control systems.
- › Agencies are most likely to use this type of technology in the field or data centers.
- › Agencies value cybersecurity, size and weight, and form factor most highly.
- › When choosing a vendor to develop customized solutions for non-traditional IT environments, respondents value the ability to develop specialized designs and/or custom platforms, program management and a secure supply chain most highly.



When Standard Technology Doesn't Fit the Bill

In the field, failure is not an option. Personnel must handle tasks correctly, and make decisions on the go. These non-negotiables require having the right tools available, ready to use, secure and reliably. In many cases, that means using rugged laptops, secure mobile devices or small units that integrate server and storage technology. These technologies help the armed forces achieve their missions and make important decisions every day.

But there are times when even the most rugged or specialized device won't meet all needs. There may be very tight space constraints, unusually stringent security requirements or the need for even more durability than typical rugged devices provide. When that happens, the best solution is often working with integrators that can customize technology to fit specific requirements. Often, the best choice is finding an experienced federal systems integrator that can work with technology and solution providers for Defense to tailor and fully customize products to meet specific electrical, mechanical, software and system requirements.

With the right partner, almost anything is possible. If a federal agency requires mobile devices used by personnel to incorporate stringent security requirements, it can specify those requirements and get exactly what it needs from an experienced technology vendor. For example, communications software vendor [Hyponi](#) worked with engineers from Dell Technologies to develop a solution that allows users to access information and applications from a secure virtual smartphone without removing data from agency systems or copying it to their phones. The solution allows field agents to use their own devices, while ensuring that some information remains classified.

Similarly, the military often requires powerful servers or hyperconverged solutions that can work in extreme environments. Sometimes, however, other needs demand further customization. For example, a mission might require the strictest security measures, which may lead to customizing a server so that removing SSD drives is an option, or removing the camera and microphone from laptops to use in classified areas. That was the situation with DIGISTOR, a secure data storage vendor [looking to develop](#) a secure server that could withstand extreme conditions. Dell Technologies OEM

Solutions Custom Factory Integration division, working with DIGISTOR, developed a highly secure flash storage solution designed for harsh environments.

Other cases might require resizing standard technology to fit in extremely tight spaces. To satisfy that need, [Tracewell](#) [partnered with Dell Technologies OEM Solutions](#) and Intel to develop a powerful, hardened hyperconverged computing system that can fit in the back of a jeep. To accomplish the goal, engineers essentially cut a rugged server in half and integrated it into a MIL-SPEC transit case, while ensuring that it met all requirements.

Questions to Ask Before Embarking on a Customized Solution

- Does the vendor have a dedicated engineering team that can tailor and fully customize products to meet your specific needs?
- Does the vendor have a long track record of success with customization and cutting-edge technology?
- Does the vendor have the buying power to guarantee production consistency, so the product can continue to be delivered as designed?
- Does the vendor provide lifecycle support services?
- Can the potential partner supply program management handle all regulation and compliance requirements?
- Does the vendor have a broad portfolio for easy integration of solutions from edge to cloud?
- Does the vendor have a deep focus on security, from the chip level to delivery and support?
- Does the vendor provide extended warranties, and will it honor all existing warranties?

Sometimes, it's a matter of developing a solution that provides greater levels of performance in a smaller footprint, or enclosing the required technology in a durable, weatherproof case. Other times, it's about reconfiguring technology to make it even easier to use and reposition. For example, most traditional data center products are accessible only from the back, but that won't work in tight environments where access is critical. From a serviceability standpoint, everything may have to be at the front, because it's often a very narrow space that doesn't allow for access any other way.

Some requests can be very unusual but are feasible with the right engineering expertise. Rahaman recalled several such cases. One mission required combining a standard smart card reader with a high-performance computing platform for space-constrained environments. The result was a secure solution that met all requirements. Other divisions have requested color-coded servers in their mobile data centers. When a different color represents each workload, users can more easily find what they need quickly.

Survey respondents identified a wide array of factors they consider when looking for a partner (see Figure 6), but three stand out:

- The ability to develop specialized or custom platforms
- Program management capabilities
- Secure supply chain

“Just about anything is possible if you define the specs and get the best engineering expertise you can,”
Rahaman said.

Figure 6: What capabilities are most important in selecting a technology vendor or partner?

44% Ability to develop specialized designs and/or custom platforms



44% Program management



38% Secure supply chain



31% Engineering services



25% Extended product lifecycle



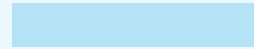
25% Lifecycle product support



25% Financing



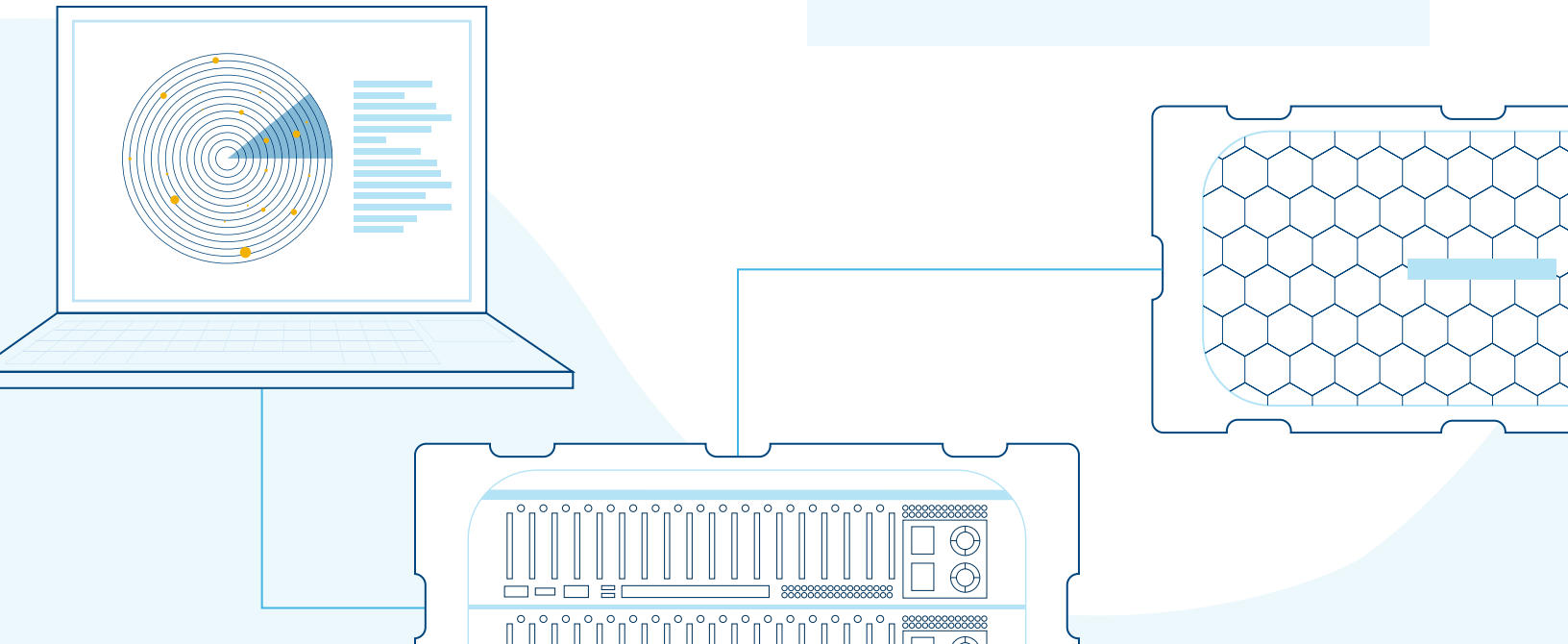
19% Global support



19% Lifecycle product management



6% Vendor's solvency



How Dell Technologies OEM Solutions Helps

Dell Technologies OEM Solutions has a team of engineers and program managers dedicated to designing, engineering, testing and marketing customized solutions built on tier 1 infrastructure to meet specific mission requirements. Customers gain direct, dedicated access to 100% in-house engineering, hardware and software development support to customize solutions from laptops to rack servers, and from edge to cloud.

OEM Solutions can:

- › Deliver cost-effective and innovative technologies that work
- › Customize solutions for when standard off-the-shelf offerings don't meet the need
- › Make customer transitions easier and less disruptive with long-life solutions
- › Protect sensitive data and enable cyber-readiness
- › Help federal system integrators focus on their IP and competitive differentiation, not the hardware it runs on
- › Provide real-time intelligence to soldiers, agents and government organizations
- › Strengthen capabilities across land, sea and air

No matter the mission requirement, Dell Technologies OEM Solutions in collaboration with Intel can deliver custom solutions built to withstand demanding environments beyond the desk and data center. OEM Solutions can meet any need, from robust and hardened chassis designs to extended environmental specifications to constrained footprints.

For more information visit:
DellTechnologies.com/OEM/Military

Conclusion

Agencies are collecting and analyzing more and more data outside of the traditional office environment, often incorporating cutting-edge resources that include artificial intelligence and machine learning. Many are adopting edge computing models, where data is collected and analyzed as close to the source as possible — on the battlefield, in a temporary hospital, underground or in the air. Sometimes, data collection and analysis also happens in harsh environments, including high humidity, driving rain or snow, extreme heat or in an environment subject to strong shocks or vibrations. These unique conditions often require unique solutions unavailable in the commercial world.

When standard OEM offerings don't fit the bill, agencies turn to customized solutions built to their specifications. The combination of a creative solution provider for Defense and experienced technology company like Dell Technologies OEM Solutions can result in true innovation. Whether it's an Intel-powered rack-mounted server that can house multiple thin clients, a smart card reader integrated directly into a hardened server, a ruggedized hyperconverged infrastructure or a customized Intel based mobile solution that meets specific security requirements, agencies today can get the solution that meets their exact requirements.





About Dell Technologies OEM Solutions

Dell Technologies OEM Solutions partners with customers to design their innovative in-market solutions by leveraging Dell Technologies tier 1 infrastructure and capabilities including engineering, program management, global support, global secure supply chain and much more. This allows companies to bring ideas to the world faster, create better customer experiences and drive their customers' digital transformation.

For more information visit:
DellTechnologies.com/OEM/Military



About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | [@govloop](https://twitter.com/govloop)