Hewlett Packard Enterprise

ebook

The Digital IT Transformation Journey:

Solutions for the Department of Defense

Table of contents

The Aruba Advantage
Aruba is the only company to combine advanced wireless LAN technology, military-grade cryptography, and security certification compliance to safely allow mobile devices to access networks that handle sensitive but unclassified, confidential, and classified information. Aruba provides the software to enable next generation secure interface between IT and IoT at the Intelligent Edge through the following:

- Follow me anywhere: Identity-based security follows the IoT and users as they move across the LAN, WAN and Internet
- Single-Pane-of-Glass: Central management to configure, monitor and troubleshoot a hybrid and heterogeneous environment
- Intelligent Edge control: Application-awareness is optimized for converged data, voice and video over wireless associated with everything from smart phones to IoT devices (sensors, meters, etc.)
- Future proofed architecture: Flexible and scalable network enables overlays to avoid upgrades and network redesigns.
- High-performance Wi-Fi: Aruba Adaptive Radio Management technology automates radio frequency management, eliminates site surveys, and maximizes performance areas.

Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks

Whether engaging in combat situations, defending the homeland, providing humanitarian aid or conducting disaster relief missions, the U.S. Department of Defense (DoD) relies on communications to build and maintain a common operational picture – a far greater challenge given cyber threats, the explosion of Internet of Things (IoT), and, of course, the fog of war and disaster response.

The U.S. armed forces must operate in a global theater with variation to the size, speed, and projection of surveillance and/or force necessary. Human and sensor intelligence must be collected, analyzed and proper actions must be taken. Agility is a cornerstone and faster, more secure networks are essential regardless of situation, mission or location. Whether it's a particular branch such as the Marines or joint forces and special operations, mobile-first is the default approach.

That's where Aruba can help by starting with a mobile-first approach to wireless communications. Aruba provides the latest networking and security solutions and has been deployed in thousands of federally-validated wired and wireless networks for the U.S. government, including the intelligence community, the purple agencies and the armed services branches. Aruba provides a secure and smart network that can be accessed whenever and wherever for greater efficiency, higher productivity, and better integration to modern warfighter communications, logistics and ISR networks.

Aruba at a glance

Aruba is the leading provider of federally-validated and policy-compliant wireless LAN (WLAN) solutions, incorporating centralized end-to-end encryption, role-based access control and stateful user-based firewall capabilities as integral components to its mobility-defined networks architecture. It eliminates the tradeoffs between reliable mobility and comprehensive mobile security and extends the Intelligent Edge to the IoT, from ruggedized smart phones, to base surveillance, to in-theatre, remote sensor packages.

Previously, with wired solutions, it took hours after arriving at a new location to get networking up and running, leaving some without access to critical information systems.

Aruba expedites the process and reduces the networking setup from hours to minutes by enabling the use of commercially available mobile devices to securely access networks that handle unclassified, confidential and classified data, all on a single network (where and when permissible). This allows secure mobility for U.S. DoD networks when and where it matters most.

Secure mobility for government networks

Government organizations, including defense and intelligence communities, are pulling the plug on wired networks and enabling employees, contractors, and, of course, warfighters to go mobile. Why? Because it's more secure than wired, streamlines operations, reduces their costs, and increases ability to successfully complete missions.

Aruba all-wireless solutions feature strong defense-ready security to protect information at every level. It also serves the public across a trusted wireless infrastructure that delivers mobility to defense facilities ranging from domestic offices and bases to forward command posts.

This modern mobility solution is certified secure for government use against government policies and has many accredited deployments, providing secure mobility.

Aruba enables secure mobility by linking access privileges to a user's unique identity and by employing all forms of standards-based security, including NSA-specified Suite B encryption, enabling both classified and unclassified transmissions. This allows authorized users to securely access networked resources based on who they are, no matter where they are, what devices they're using, or how they're connected.

Security certifications and compliance

The advantages of Mobility Defined Networks allow Aruba to rapidly and repeatedly achieve a number of government-required security certifications including:

- Common Criteria EAL-45
- FIPS 140-2/-12 Validation
- DoD directives 8100.2 and 8420.01
- Section 508 compliance for user interfaces

Click here for the full list of government security certifications and compliance.

Aruba is ready for service

Aruba solutions are easily deployed in any environment without changing the existing back-end wired infrastructure.

Aruba solutions are easily deployed in any environment without changing the existing back-end wired infrastructure. This eliminates the costs and complexities of managing separate policies for wired, wireless, and VPNs while using fewer ports and less wiring closet equipment. Aruba offers a turnkey solution that combines advanced wireless LAN technology, military-grade cryptography, and security certification compliance to safely allow mobile devices to access networks that handle sensitive but unclassified, confidential, and classified information.

For more information on Aruba networking and security solutions, click here.

http://www.arubanetworks.com/solutions/classified-mobile-networks/

http://www.arubanetworks.com/assets/eo/IB_FEDCERT.pdf

http://www.arubanetworks.com/assets/so/SO_Government.pdf

Pointnext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity

Introducing HPE Pointnext, an innovative IT services organization that combines our highly successful technology services consulting and support groups to create one world-class services organization. With these services, the Department of Defense (DoD) can modernize its infrastructure with the flexibility of a cloud, and maximize the value of its connected devices. Simply put: HPE Pointnext delivers the latest software-defined infrastructure needed to transform the department into a digital-first organization.

But digital transformation isn't something that happens overnight, and there isn't always a clear path to success. That's where we can help by figuring out which technologies to invest in and how best to implement them to meet the department's specific needs.

Having the right infrastructure in place is a critical first step on the digital transformation journey.

Three pillars of HPE Pointnext

HPE Pointnext is built on three types of services:

1. **Advisory and Transformation Services,** which design a unique transformation journey and roadmap that's tailored to the department's unique challenges.
2. **Professional Services** that specialize in flawless and on-time implementation, on-budget execution and creative configurations for software and hardware.
3. **Operational Services** with new ways to deliver IT by managing and optimizing on-premises and cloud workloads, resources and capacity.

Delivering digitization as your needs change

HPE Pointnext is a services organization built for the future to help customers optimize and leverage the ideal technologies, customers and operational foundations needed to accelerate their digital journey, all while providing a seamless customer experience. Building on our heritage of services leadership, HPE Pointnext will invest and focus in the following areas:

Optimizing infrastructure – Having the right infrastructure in place is a critical first step on the digital transformation journey. For decades, HPE's core strength has been rooted in infrastructure. Specifically, how to design, integrate and support solutions that perform and scale to meet the unique demands of the apps and data that drive businesses.

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

This helps leaders across organizations and IT focus on innovation and create value, rather than on operations.

HPE PointNext and DISA Procurement Requirements
HPE and HPE PointNext products and support services follow NIST 800-53 recommendations, and meet all Defense Information Systems Agency (DISA) DoD procurement requirements for Federal Risk and Authorization Management Program (FedRAMP) for services related to both server and management systems.

Security features delivered and supported for hardware products and services:

- Silicon Root of Trust
- **CNSA Suite**
- **Two Factor Authentication CAC**
- Prevent Firmware Attacks from OS
- Secure Erase of NAND Data
- **Common Criteria & FIPS 140-2 Level1**
- UEFI Secure Boot
- TPM 1.2 and 2.0
- **NIST 800-147b BIOS**
- **PCI-DSS Compliance**
- Secure Supply Chain

Security features delivered and supported from operating environment perspective:

- Firmware Runtime Validation
- Verified Boot
- Trusted eXecution Technology
- SIEM Tool Support
- Audit Logs
- Measured Boot

Curating a best-in-class ecosystem – Many of our customers struggle to determine which technologies and vendors can best solve their unique problem, and how to bring them together. A key ingredient to create successful solutions for our customers is our ability to collaborate with the right partners.

Removing complexity – HPE Pointnext experts help our customers go beyond the technology problem of digital transformation to address culture, measurement, skills, change management as well as new approaches to funding and IT consumption options.

This helps leaders across organizations and IT focus on innovation and create value, rather than on operations.

Building for speed – Our scalable approach is designed to deliver faster time to value for our customers, focusing on helping them build solid foundations in technology, process and people to enable them to learn quickly and continuously improve.

Ensuring a personalized consumption journey – HPE's Flexible Capacity allows our customers to expand capacity when necessary to meet the changing needs of unit and agency operations without delay or new purchase red tape, while making minimum capital investments, yet having complete flexibility for rapid response to increased demands.

Infrastructure service with on demand capacity

HPE Flexible Capacity is a service offering that allows you to transition your current environment, minimizing risk, improving time to value, and fully meeting data governance requirements so you have the security and privacy you need for on premise data types, but also the necessary flexibility and performance for cloud appropriate data whether you buy or lease. This takes you on a personalized consumption journey matching your needs today while ensuring future capacity to execute on your near or long-term operational and mission or business needs at the pace you set.

Learn more about HPE Flexible Capacity https://www.hpe.com/us/en/services/flexible-capacity.html

Here to help

Every time HPE Pointnext experts work with customers, they're not just receiving the knowledge and expertise of the team. They're also on the receiving end of decades of experience. We have developed industry leading IP and an extensive library of enterprise-class designs and blueprints from over 11,000 successful implementations. We know what works and what doesn't, because we've done it many times—both for own infrastructure and for thousands of customers.

For HPE, Pointnext is a redefined and future-focused organization with a new approach to services. It's a way we can make a difference in our customers' businesses, beyond providing the software-defined infrastructure they depend on. With HPE Pointnext, we will not only offer the necessary technology infrastructure and tools, but we will join our customers on their journeys to digital transformation.

Source:

https://news.hpe.com/hpe-pointnext-services-to-accelerate-your-digital-transformation/

https://www.hpe.com/us/en/services.html#benefits

HPE Synergy: Composable Infrastructure for Defense and Intelligence Agencies

Asymmetric warfare is disrupting the way we defend our nation. No longer does the biggest gun or best trained warfighter guarantee victory; our brave warriors are increasingly augmented by sophisticated and intelligent weapons platforms, logistics systems, communications, and surveillance systems. These systems are being adapted to deal with disruptive forces, from rogue nations, terrorists, and hacktivists, mostly through software that is rapidly changing in response to changes in mission and operational requirements. In essence, force modernization in defense and intelligence agencies is all about digital transformation.

Unlike their counterparts in the private sector who are free to pursue the latest and greatest commercial technologies to achieve their business objectives, defense and intelligence agencies must meet a range of additional requirements including security, procurement guidelines, global deployment and servicing, among others, in addition to the ability to operate in harsh conditions.

Ultimately, these types of requirements lead to long design-in and deployment cycles, resulting in often-obsolete technologies, operating as a sprawling infrastructure of thousands of disparate systems. These systems tend to be high maintenance and siloed, with little automation, incapable of rapid updates in response to feature and functionality change requests.

Limited ability to rapidly modify code, easily integrate, test and deploy new software and systems, and quickly access and mobilize critical information across various systems can substantially slow and undermine everything from mission-related tasks (such as battle planning) to force projection, to rapidly changing how bomb damage assessments are executed or how IEDs are characterized and linked to possible terrorist cells. The impacts of this inability to respond rapidly to changing conditions are seen not only in military mission zones where multiple missions run simultaneously, but also in other areas such as backend support functions like recruiting and training, procurement, and logistics. In these and myriad other critical functions (military healthcare, base facilities management, situational awareness through sensor fusion, and more), software, the underlying systems and their integration onto the workflow and workforce, and all associated data are now essentially the fuel that drives modern defense and intelligence agencies.

The HPE Composable Infrastructure solution delivers critical flexibility and agility by unifying compute, storage, network fabric, and management into a single, software-defined infrastructure, with shorter time to value, ease of scalability, and lower total cost of ownership.

Digital transformation: More than just "lift and shift"

Digitally transforming the infrastructure to reliably develop, deploy, and manage a wide range of applications residing on a varied and distributed set of systems, along with the massive amounts of data associated with those systems – often defined as workloads – isn't as simple as lifting and shifting them from bespoke, proprietary hardware over to the "cloud." Indeed, accomplishing this transformation requires far more than just funding. Necessary time, architectural changes, skill sets, and training requirements, as well as cultural and organizational changes will take center stage in this process. Also, providing a common platform

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

for Department of Defense (DoD) workloads using more traditional IT tools would not only be expensive and difficult, but would simply create a static infrastructure.

That's where Hewlett Packard Enterprise (HPE) Synergy comes in. The HPE Composable Infrastructure solution delivers critical flexibility and agility by unifying compute, storage, network fabric, and management into a single, software-defined infrastructure, with shorter time to value, ease of scalability, and lower total cost of ownership. Such outcomes can enable DoD and Intelligence Community (IC) IT leaders to accomplish more simultaneous missions under rapidly changing conditions with fewer resources – in other words, adapt fluidly to mission changes, since no plan completely survives contact with the enemy.

Introducing HPE Synergy and Composable Infrastructure

Every so often, the IT community creates a paradigm shift and coins a new phrase. The latest entrant into our lexicon is "composable infrastructure," a framework in which hardware and software are architected as one so that composable infrastructure systems are built alongside the software that manages the environment. This unique and tight coupling ensures high performance, rapid deployment and full compatibility for supporting all DoD workloads across military zones and backend operations. Composable infrastructure frees administrators from the tedious burden of uncertainty about whether the hardware will support specific software applications or workloads or whether it can correctly provision for those workloads, as well as from concerns that workloads may be compromised to adapt to infrastructure limitations.

A critical challenge with traditional data center architecture arises when IT becomes bogged down in hardware silos. This often means increasing cost and complexity of the data center environment in order to get the level of performance and stability needed to run workloads. Even the cloud environment can present operational silos, with multiple cloud vendors adding to complexity. With converged and hyperconverged infrastructure, DoD and IC environments are fully fluid and extensible for all types of applications, and storage is distributed to various nodes that comprise the hyperconverged infrastructure cluster. Hyperconverged infrastructure leverages software-defined storage to work its magic and eliminates SAN. Composable delivers software-defined everything.

In particular, this revolutionary Infrastructure-as-a-Service (IaaS) approach makes it easier than ever to deploy new applications or provision services quickly, run workloads on any physical or virtual servers or in containers, and operate any mission-critical workload independent of infrastructure resources or compatibility concerns.

HPE Synergy is the first purpose-built heterogeneous platform for delivering capabilities to data centers that bridge traditional and cloud-native applications in a single infrastructure.

A software-defined storage environment includes software that manages storage on a local node. This software could be built into the hypervisor kernel or could run on a virtual machine. In a hyperconverged infrastructure environment, the storage management software layers align with similar layers in the nodes, resulting in a distributed, scaled-out storage environment, and a monolithic SAN is no longer necessary.

HPE Synergy is the first purpose-built heterogeneous platform for delivering capabilities to data centers that bridge traditional and cloud-native applications in a single infrastructure. Now IT administrators can manage any workload anywhere, at any time, by flexing their resource use to meet the ever-changing demands of the military mission for maximum responsiveness, agility, and efficiency.

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

HPE Synergy provides DoD and IC IT administrators the tools, processes, and efficiency gains they need to keep the country's citizens, interests, and allies safe.

Key features of the HPE Synergy family:

- **Composable Frame**
  The HPE Synergy frame is optimized to support a wide range of compute and storage options. The backend includes fabric interconnects that provide essential flexibility for storage and other interconnectivity needs.
- **Composable Management**
  The HPE Synergy Composer and Synergy Image Streamer combine to enable IT admins to deploy, monitor, update, and manage infrastructure throughout its life cycle from one interface. Composer templates dramatically accelerate provisioning of compute, storage, and fabric resources, while automatically copying images for each computing module to save time, money, and frustration.
- **Composable Compute**
  The HPE Synergy composable compute portfolio makes it easy to right-size computers for various workloads, providing myriad module options from among the HPE innovative Gen9 servers and the latest Intel® E5v4 and E7v4 series processors.
- **Composable Storage**
  HPE Synergy composable storage provides the ideal storage choices for every target workload, delivering high-density storage options spanning DAS, VSA, and all-flash arrays for the flexibility and agility to handle any data type, connectivity protocol, or service level requirement.
- **Composable Fabric**
  HPE Synergy Composable Fabric simplifies network connectivity by creating a pool of flexible fabric capacity that can be configured nearly instantly to rapidly provision infrastructure for a broad range of applications. Enabled by HPE Virtual Connect technology, the composable fabric eliminates up to 95 percent of network sprawl at the compute module edge, bringing "wire-once" simplified management between network and compute resources.

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

Delivering next-generation infrastructure security and compliance

Naturally, providing a secure and federal-standards-compliant infrastructure for the agencies responsible for national security is a priority for HPE Synergy. HPE is proactively improving the security of its environment to ensure that every link in the security chain provides the most effective cyber security protections possible. With each passing generation of operating systems and applications, server vulnerabilities are harder and harder to find. Undaunted, the adversaries we face simply look for alternate, weaker links in the defense systems, mobile devices, IoT, and other new attack services offer new opportunities for exploitation. On the server side, one of the latest and increasingly exploited vulnerabilities is the server firmware which can often range far into the million lines of code and can easily serve as a new backdoor into systems. HPE has designed a hacker proof firmware chipset that has a built in "root of trust" and allows HPE to proclaim its Generation 10 servers as the most secure servers on the planet.

Around this root of trust, HPE Synergy has been designed, tested and certified to achieve compliance with core federal standards. HPE Synergy complies with the National Institute of Standards and Technology, or NIST, NIST- 800-53 recommendations for risk management and will continue to adjust as needed over the next several years as NIST updates and introduces new standards.

The current security focus for HPE Synergy includes meeting requirements for both server and management systems set as specified by the Defense Information Systems Agency (DISA), specifically responsible for IT and communications support.

HPE delivers a seamless ownership experience while helping the Department of Defense on its modernization journey, getting the most from IT today and in the future.

As part of enhancing hardware security to meet NSA and DISA requirements, as of the July 2017 HPE Generation 10 release, servers support:

- Silicon Root of Trust
- Commercial National Security Algorithm Suite (CNSA Suite)
- Two Factor Authentication Common Access Card (CAC)
- Prevent Firmware Attacks from OS
- Secure Erase of NAND Data
- Common Criteria & Federal Information Processing Standard (FIPS) 140-2 Level1
- United Extensible Firmware Interface (UEFI) Secure Boot
- Trusted Platform Module (TPM) 1.2 and 2.0
- NIST 800-147b BIOS
- Payment Card Industry-Data Security Standard (PCI-DSS) Compliance
- Secure Supply Chain

Likewise, to further secure the operating environment to meet DISA and NSA requirements, as of the July 2017 Generation 10 release, the servers support:

- Firmware Runtime Validation
- Verified Boot
- Trusted eXecution Technology
- Security Information and Event (SIEM) Tool Support
- Audit Logs
- Measured Boot

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

From the management security perspective, the next scheduled release of HPE OneView will include support for:

- Federal Information Processing Standard (FIPS) FIPS 140-2
- Common Access Card Personal Identify Verification (CAC PIV)
- 2-Factor authentication
- Scope Based Access Control
- SNMP Version 3

Looking ahead, as another step in a series of initiatives to further secure the HPE Synergy environment, HPE Synergy will also comply with the Federal Trade Agreements Act (TAA), which requires that products originate from the United States or another TAA-approved country.

As HPE Synergy continues to evolve to stay at the forefront of secure environments, watch for security measures to expand well beyond the server and management subsystems, to include storage, fabric, and physical management hardware.

HPE Synergy for Department of Defense and the Military

Like every organization, DoD has its own unique set of requirements and parameters. To balance the demands of this work with budgetary constraints, DoD leaders must effectively and strategically consolidate and manage resources, requiring a purpose-built ecosystem of high performance, secure, and integrated tools that can effectively eliminate obstacles among current business solutions. The tools must break down barriers between systems that stymie productivity, restrict collaboration, and hinder business processes.

HPE Synergy delivers on that promise with fluid resource pools, software-defined intelligence, and unified API that provide DoD the agility to rapidly develop and deploy applications and automatically update software to meet configuration requirements and maintain daily cyber security defense. The solution's composable infrastructure also delivers unmatched agility and investment protection with cloud-like economies of scale, helping rein in costs associated with legacy systems, while enabling faster data consumption and greater control over operations, compliance requirements, and security protocols.

HPE Synergy helps you unify your compute, storage and network with an optimized software-defines infrastructure.

In short, HPE Synergy provides DoD and IC IT administrators the tools, processes, and efficiency gains they need to keep the United States' citizens, interests, and allies safe and to address the infrastructure management challenges posed by an enormous, sprawling, and increasingly cumbersome IT environment. Defense will always be a dangerous job requiring pride, sacrifice, and courage. But it doesn't have to be — and shouldn't be — bogged down in antiquated systems that serve only to make the jobs of the armed forces and intelligence communities harder, not easier.

To learn more about the HPE Synergy Composable Infrastructure makes the country safer and easier to protect, visit www.hpe.com/synergy.

Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers

Virtually every defense and intelligence system is either already in or in process of being transitioned to the digital domain. As a result, all missions have a cyber component to them and all aspects of these systems must be hardened against cyber attacks. Software vulnerabilities in these systems has often been looked at through a traditional, narrow lens of the operating environment and applications running on top of this environment in a data center. However, the number of potential at-risk systems is rapidly expanding outward from the data center to mobile devices such as drones or even to military satellites and the networks connecting the data center to this new Intelligent Edge as new areas of vulnerability.

The cyber battlefield is asymmetric. Potential vulnerabilities are proliferating while at the same time cyber criminals and rogue nation states are getting smarter, and quickly adapting intrusion strategies and relatively inexpensive technologies to exploit new attack surfaces, often resulting in David and Goliath surprises (note, in this case David isn't the good guy). The need for strong cyber defense has never been more pressing: Global annual cybercrime costs are expected to grow to $6 trillion annually by 2021.[1] With breach attempts topping 500,000 per minute[2], while median time to detect a breach sits at 99 days[3], denial of service (DoS) and malware-infected firmware are increasingly common.

For the armed forces and the intelligence agencies, such risks can be highly damaging and unacceptable. Two recent, public examples include theft of the Joint Strike Fighter designs and the OPM's employee records including DoD records. What's not common knowledge is that there are over 15,000 DoD systems across over 4,000 worldwide locations, with the vast majority based on standard server architectures and connected through civilian networks, as well as to defense contractor and other non-defense systems[1].

In this environment of escalating risk, securing the infrastructure is no easy task. Infrastructure attack surfaces include the network perimeter, server applications and operating systems, data at rest and in transit, platform hardware, and even the firmware in the server itself. Manufacturers are certainly moving to make their offerings more secure, increasingly "hardening" attack surfaces such as software applications, hypervisors, and operating systems. But adversarial nation state cyber offense units and criminals stay a step ahead, sharpening the focus on lower-level attacks—including on the firmware.

Because firmware always loads more than a million lines of code before the OS even boots, the firmware and BIOS must be protected. Just a few lines of corrupt code hidden among those million lines of code could permanently brick a server, and an unauthorized driver or malware with kernel privileges could create a permanent denial of service (PDoS) attack by corrupting the data or devices required to properly boot the server.

[1] Cybersecurity Ventures, 2016

[2] CNBC, Biggest Cyber Security Threats in 2016 Derek Manky, Fortinet global security strategist

[3] Mandiant M-Trends, Trends from the Year's Breaches and Cyber Attacks, 2016

This means protecting networks only at the perimeter firewall level or servers at the software and OS level is no longer enough. Servers are now found in satellites that manage our GPS grid for fleet positioning and command and control communications, in our drones, and every conceivable system from backend systems to logistics to forward command posts. And increasingly parts of these systems rely on commercial standard hardware and software platforms, and are therefore susceptible to the same vulnerabilities and changes to them as any other industry.

Security certifications and compliance

A must for hardware used by U.S. defense and military agencies, HPE Gen10 servers comply with multiple security standards and encryption protocols. Among these are the Federal Information Processing Standard (FIPS) Publication 140-2, the National Institute of Standards and Technology (NIST) 800-147b, the payment card industry data security standard (PCI DSS), and Common Criteria.

- **FIPS 140-1 Level 1**: FIPS is a set of standards that U.S. government agencies and contractors must use. The cryptographic module in HPE iLO5 firmware is in the process of achieving FIPS 140-2 Level 1 validation now. (Both the iLO3 and iLO4 devices are already FIPS 140-2 Level 1 validated.) With the iLO5 chipset, HPE Gen10 servers can operate in FIPS 140-2 Mode, which mandates high-grade encryption ciphers and shuts down insecure interfaces and ciphers that don't meet CNSA government standards.
- **NIST 800-147-b BIOS protection guidelines:** HPE Gen10 servers fully comply today with the NIST 800-147b guidelines. These guidelines support secure update mechanisms. Both the legacy BIOS and the UEFI firmware in HPE Gen10 servers comply with this NIST standard.
- **Payment Card Industry standards:** HPE Gen10 servers also adhere to PCI DSS, a broadly accepted set of policies and procedures to protect the safety of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information.
- **Common Criteria:** HPE supports the objectives of the National Information Assurance Partnership (NIAP) Common Criteria (CC) certification standard as well. These are guidelines to evaluate information security products to meet standards for government deployments. HPE is taking the iLO5 chipset from Gen10 servers and a set of ProLiant Gen10 C-Class blades through a Common Criteria certification as well as the FIPS 140-2 validation.

HPE Gen10 servers: The Fort Knox of compute for those protecting the U.S.

HPE Gen10 platforms, including ProLiant, BladeSystem C-Class, Apollo, and Synergy, are now established as the world's most secure industry standard servers.[4] As such, they can offer defense and intelligence agencies the best possible protection for their data centers and private clouds:

- HPE Gen10 Servers are the first industry standard servers to include a silicon root of trust (a highly reliable component to measure or verify certain critical security functions—and in turn can test and verify other security-related functions that depend on it) that's actually built into the hardware. This makes it possible to scan and monitor the firmware through integrity checks initiated from an immutable link embedded in the silicon hardware itself.
- HPE Gen10 servers can also recover to a known good state in the unlikely event that firmware becomes compromised in any way.

[4] Based on external firm conducting cyber security penetration testing of a range of server products from a range of manufacturers, May 2017

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

From the silicon root of trust, to specific networking and storage options and rack infrastructure, HPE has built in an arsenal of security features to help prevent, detect, and recover from cyber attacks. These options can combine to deliver an unprecedented level of security to protect highly sensitive infrastructures such as those of defense and intelligence agencies.

Offerings include:

HPE has built in an arsenal of security features to help prevent, detect, and recover from cyber attacks.

- **HPE's Integrated Lights On (iLO5) server management controller:**
  - HPE's iLO management chipset (iLO5) provides secure, out-of-band management functionality regardless of the server hardware or OS status and is available whenever the server is connected to a power source—even when the main power is switched off. It offers strong authentication, highly configurable user privileges with strong authentication processes, and encryption of data, keystrokes, and security keys.
  - iLO5 provides the silicon root of trust, ability to scan and monitor the chain of trust, and ability to securely recover.
  - The iLO Advanced License can deliver two-factor authentication via either Kerberos authentication (using a trusted third party to authenticate between a client and a host server) or, to meet more stringent requirements such as those of the U.S. Defense Information Systems Agency (DISA) and the U.S. National Security Agency (NSA), via protocols for a smart card used to identify military personnel, DoD employees, and contractors that's known as the Common Access Card (CAC).
  - Especially important for government contractors and agencies, HPE's iLO Advanced Premium Security Edition license delivers the highest level of commercial encryption capabilities when in the Commercial National Security Algorithm suite (CNSA) mode. CNSA is a suite of cryptic algorithms approved by the US National Security Agency for protecting secret and top secret information within the U.S. government. This license also provides continual runtime detection of firmware validity, secure erase of the iLO5 NAND/NOR memory, and secure recovery to authenticated states.
- **HPE server options and management solutions such as:**
  - Network adaptors with a root of trust, device-level firewalls, United Extensible Firmware Interface (UEFI) secure boot, and audit logs for tracking changes, as well as the ability to proactively protect networking traffic with packet inspection and capture.
  - Smart Array Controllers with Secure Encryption licenses to protect data at rest on attached storage devices.
  - Enterprise Secure Key Manager (ESKM), a Federal Information Processing Standards (a set of standards mandated for use by United States government agencies and contractors), or FIPs, 140-2 Level 2 validated and Common Criteria-certified, key management solution that works with Secure Encryption to provide centralized control and audit records for encryption keys.
  - HPE SATA Solid State Drives (SSDs) and Hard Disk Drives (HDDs) that include digitally signed firmware to ensure valid operations. Both can erase data using methods compliant with the NIST Guideline for Media Sanitization (NIST 800-88r1) to erase data once the drive reaches end of life.
- **Additional secure components in the server chassis, such as:**
  - A factory-installed Chassis Intrusion Detection Switch provides assurance that the server chassis hasn't been tampered with after production. It detects and alerts administrators if the chassis hood has been opened or closed at any time from production onward.

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

  - The Trusted Platform Module (TPM) securely stores information to authenticate the server platform and enables a measured boot process for the OS, which monitors OS initialization to see if OS startup has been compromised. TPM also supports specific capabilities such as Microsoft® Windows BitLocker Drive Encryption.

- **HPE G2 Advance or Enterprise racks:**
  - These allow easy additions of third-party security hardware solutions, enabling setup of two- or even three-factor authentication for the data center with solutions such as RFID readers and biometric solutions.
  - Side panels are modified to reduce the risk of unauthorized access from an adjacent rack.
- **HPE Power Distribution Unit (PDU) sensors:**
  - These rack options offer increasing levels of physical security through external sensors available with the PDUs. Advanced PDUs provide intrusion detection monitoring of the racks at a level unavailable from any other server OEM.
- **Top-of-rack (ToR) switches:** Network traffic is increasingly targeted as an attack surface for malware and threats to enter a data center infrastructure. Security vendors' abilities to analyze networks for malware relies on accurately monitoring network traffic—not always a given. A more secure alternative comes via HPE's partnership with Arista Networks® to provide secure hybrid IT solutions built on Arista's industry-leading software-defined data center infrastructure portfolio.
  - Arista Fixed ToR Switches are built specifically for the data center.
  - The 700 series includes a number of switches that have been tested and approved for use on the DoD Unified Capabilities Approved Products list and Assured Services Local Area Network (ASLAN).
  - These ToR switches include such security-enabling features as:
    - The Extensible Operating System (EOS) to automate insertion of security services.
    - Data Analysis (DANZ) security monitoring tools for end-to-end monitoring for sensitive cloud environments.

Leading the charge to a more secure infrastructure

Security threats will only continue to increase as attacks become more complex and attack surfaces shift from network perimeter, software, and applications to the physical platform itself. HPE is committed to increasing the level of security so that customers with even the most sensitive IT environments, such as U.S. defense and military agencies, can be confident that their data center infrastructure is secure from threats—all the way down to the firmware level.

Building on the foundation of unparalleled security enabled by Gen10 servers, along with networking and storage options, and rack infrastructure, HPE now delivers a cloud-like compute experience with the security and control of the data center.

This compute experience also offers agility (ease and speed of deployment, reduced latency, and increased performance) and flexible, pay-as-you-go consumption models to compete with the public cloud—resulting in hybrid IT that delivers the advantages of on premises, with the pros of off premises.

For more information on Gen10 servers, click here.

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers

Threats to the United States and our allies continue to change dramatically and grow. As a result, our national security and defense organizations must change and add capabilities to combat these daunting threats. The saying goes, "Don't bring a knife to a gun fight." The same could be said for bringing underpowered and unreliable technology into rugged battle terrain and other harsh environments.

As modern warfare becomes increasingly focused on intelligence, surveillance and reconnaissance, our military units require more intelligence at the edge of our networks, capable of operating in many different climates and altitudes, across multiple jurisdictions and theaters, without compromise of performance, disruption or delay.

Increasingly the line is blurring between purely military operations and non-military applications – both can occur in a multitude of environments; meaning the technology required to support those missions must be adaptable, rugged, and lightweight, and capable of performing in a wide range of conditions.

Battle-proof technologies

Intelligence agency and Department of Defense systems architects, battle planning and ISR field officers, as well as purchasing leaders and technology manufacturers, all have their work cut out for them. The brains of modern operations—servers—must be deliberately engineered to fit neatly within compact spaces and impose the least possible weight burden. They should be able to withstand both high and low temperature environments, handle the elements such as sand, dust or moisture, and remain unaffected by bounces, bumps, and vibrations.

And those are just the form factor and environmental considerations. Additionally, ruggedized systems must withstand electromagnetic interference (EMI) challenges.

To meet the demands of modern defense, servers must also be agile and flexible in their performance. They need to be capable of processing massive volumes of structured, unstructured, and semi-structured data for rapid and in-depth data analysis, resource planning, and other intelligence functions essential to gaining an advantage in a conflict. The most cost-effective approach is to leverage open standard platforms that incorporate the latest chipsets and innovations for the highest speed and lowest power consumption in a ruggedized form factor. HPE is the world's leading provider of commercial servers with a long-standing history of converting commercial innovation into ruggedized platforms.

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

Introducing HPE ProLiant DL380RS Gen9

HPE, the global leader in enterprise equipment has developed an entire line of high-performance, rugged technologies based on the ProLiant DL380, the best-selling server in the world. HPE Rugged delivers optimized SWaP-tuned platforms using industry standard technology and leveraging HPE's advanced technology capabilities.

The ProLiant DL380RS Gen9 meets all MILSPEC 810G ruggedization requirements for austere field deployments and space and weight uses (SWaP) in air, land, and sea environments. Software-defined capabilities enable Rugged Hyperconverged platforms for use in DoD and resilient, scalable enterprise systems with no single point of failure—a necessity in tactical deployments—through StoreVirtual technology.

HPE Rugged technologies are powered by Intel® Xeon® E5-2600v3 and E5-2600v4 series, providing exceptional performance and scale for handling variety of workloads across Microsoft® Windows, Oracle® Solaris, Canonical® Ubuntu, and Microsoft Azure environments. Given the core architecture and ecosystem options are the same as the commercial world, IC and defense organizations can mix and match government off-the-shelf and commercial off-the-shelf options in an almost infinite set of permutations. Development and integration can be handled in pristine environments like SPAWAR or in theater – shipboard, airborne, and forward command post.

HPE offers ruggedized and battle-proof server technologies that perform in every terrain.

The ruggedized DL380 is tested against and fully meets military standards including:

- **Operational Temperature:** -10C to +50C with solid state drives, MIL-STD-810F, Method 501.5, Procedures I/II
- **Storage:** -40C to 75C, MIL-STD-810F, Method 501.5, Procedures I/II
- **Humidity:** MIL-STD-810F, Method 507.4: 48 hour, 95% RH 40-65C with humidity option
- **Altitude:** MIL-STD-810F, Method 500.4: 12,500ft operation with 40,000ft transport
- **Vibration:** MIL-STD-810F, Method 514.6 Procedure I: 4.43 GRMS, 5-20000Hzz, 60min/axis w/solid state drives
- **Shock:** MIL-STD-810F, Method 516.6, Procedures I/V: 20g, 11msec functional shock; 40g 11msec crash hazard shock
- **EMC:** MIL-STD-461F CE102 & RE102: Meets using CORESYSTEMS Optional 461 EMI Kit

Roadmap for the future

While most ruggedized systems are deployed for extended periods of time, often ranging into decades, the ability to replace systems as they fail, or when new generations become available, is critical to keeping up with countermeasures from adversaries. One key area of attack across both military and non-military environments is, of course, cyber-security related. HPE recently introduced its Gen10 platform including the next generation of Gen10 servers across the entire spectrum of HPE servers, from Synergy down to desktop servers and everything in between, including a next generation of DL380s.

While there is always a delay between introduction of mass market commercial servers, each successive generation of server architectures is applied to Mil-Spec and Gen10 will not be an exception to this rule of thumb. Dates are not available yet, but our track record is nine for nine with prior generational conversion from commercial to Mil-Spec, delivering a sustainable and scalable platform and roadmap for your future ruggedized needs.

Gen10 will provide ruggedized or hardened security down to the firmware level, a new and growing point of attack for would-be adversaries. For more details on Gen10 see page 12 of this eBook.

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR

HPE 3PAR: Managing cross-mission data with analytics and multi-Petabyte range storage.

The Department of Defense (DoD) and the intelligence agencies (IC) are grappling with rapid growth in data volumes, types, and requirements around collection, aggregation and dissemination, processing, and visualization. It's not just a matter of buzz phrases like "big data analytics," as there are clear, real-world points of growth, including sensor data collection and fusion.

Even the level of instrumentation is accelerated and requires data management, therefore causing data growth in everything from ships to planes to ground vehicles. Often, these highly visible theatre-facing points of data growth overshadow equally important traditional operating areas with critical workloads from recruitment and matriculation of new inductees and employees to medical clinic healthcare records. Across the board, today's net-centric operations are all software-defined and data-driven and must be hardened against attack, delivering a whole new meaning to the phrase "killer app."

Applications are everywhere, secure and hyper-connected, from the data center to mobile apps and IoT. It's important to move from the abstract to concrete visuals and numbers, if simply back-of-the-envelope in nature. Consider this: An MQ-9 surveillance drone doesn't just create a streaming video feed. Instead, it has 368 cameras, each collecting 12 fps simultaneously. There's often also a parallel FLIR (forward looking infrared) imaging feed, as well as an active laser feed for target acquisition. In addition, there are on-board sensor fusion data processing feeds, and, of course, instrumentation and GPS feeds describing the functional health and location of the drone.

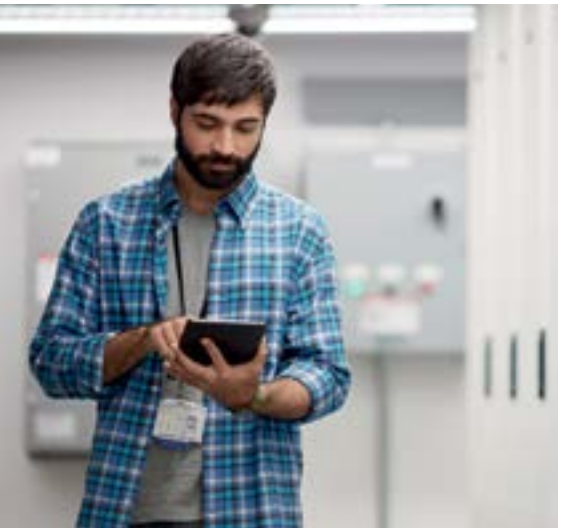
Even with data compression and efficient use of bandwidth, which greatly reduces the data rate (though some offset will be incurred for encryption and metadata), we're talking about a capable and reliable process with the performance level you need at several terabytes/minute data rates[1]. But there are also big data analytics examples not associated with the pointy tip of the spear. The Defense Threat Reduction Agency (DTRA) is doing data mining and analysis of patents to track origins and matriculation of dangerous pathogens that could be converted to WMDs[2].

And then there's the matter of creating a storage snapshot for replication, or storing some or all of this data for comparison and further analysis by more complex machine-learning algorithms in high performance computing environments. In many cases usage patterns dictate use of systems that can rapidly retrieve large data sets in a relatively short period of time for processing in streaming formats, or even in-memory. Of course, this is precluding use of any traditional tape back-up or spinning disks such as those found in legacy data centers, or their back-up and archive support systems. In essence, your underlying information management infrastructure will need to be modernized to handle the deluge of data in the agency and across the theatre just as much as the high-performance computing required for big data analytics and visualization.

[1]"Sierra Nevada fields ARGUS-IS upgrade to Gorgon Stare pod", Stephen Trimble, FlightGlobal.com, July 2nd, 2014

[2]"Big Gains foreseen for Big Data in Military Applications", Amreen Kahn, DefenseNet, May 16th, 2017

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information



Hybrid IT will be just as important for your data as it is for your apps

Currently, many of the DoD and IC data center platforms, let alone fielded military platforms, are not set up to handle heterogeneous platform nor cross-mission data integration and correlation. Even within each siloed platform, application (or workload), portfolios often exhibit the following constraints:

- Inflexible, discrete on-premise systems for computing and storage
- Support for less than a Terabyte of in-memory database or analytics processing
- Tier-1 supporting storage based primary on traditional spinning disk storage with upper limits in hundreds of Gigabyte ranges
- Tier-2 storage that's overprovisioned, must be manually tuned, accessed through low-bandwidth links, and largely meant for back-up and recovery.

The DoD and IC are under the same federal mandates to pursue data center consolidation, virtualization and use of cloud (though, often for multiple reasons described in other chapters of this eBook, private cloud), and COTS (commercial-off-the-shelf) software including databases, analytics tools that support developing interoperability frameworks such as those being proposed by NIST. Application rationalization, an expected prelude to proper spend on consolidation projects, must be accompanied by an equivalent exercise for information management and analytics assets. Database, records management, and other data repositories must be consolidated and virtualized with an eye toward shared services inclusive of robust back-up, recovery, and archiving of both new cloud and shared services, as well as existing assets.

Across the board, today's net-centric operations are all software-defined and data-driven and must be hardened against attack, delivering a whole new meaning to the phrase "killer app"

DoD and IC data center modernization on the information management side will require all of the following:

- Options to handle in-memory data processing (databases, analytics, etc.) into the multi-terabyte range
- Support for virtualization with VMs and containers to support a vast ecosystem of vendors and open source offerings
- Shift to an all flash environment for most performance-oriented workloads (solid-state arrays) capable of affordably reaching into multi-Petabyte range
- Convergence of compute and storage to reduce complexity and cost
- Automated cloud-based environments for back-up, recovery and archiving
- Predictive analytics to proactively identify disk failures as well as application I/O bottlenecks and remove them before they occur

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

HPE provides a range of solutions to support all of these design modernization requirements. Over the last five years, HPE has moved into a leadership position through its acquisition of 3PAR, SimpliVity, and Nimble. SimpliVity marries the most popular server on the market, the DL380, with industry leading SimpliVity, hyperconverged software to deliver built-in, appliance-like data protection and support for VMs and containers into 100 Terabyte range (up to 16 TB per node). Nimble delivers the simplest, predictive storage with analytics-driven support, taking next-generation storage into the low Petabyte (PB) range. 3PAR provides the most flexible unified storage for tier-1 all-flash enterprise data center ranging up to over 18 PBs in a single rack, yet starting at the same price points as SimpliVity and Nimble.

SimpliVity has efficiency as a primary goal, met through collapsing server and storage into a single system, supported with always-on deduplication and compression and native back-up and recovery. SimpliVity replaces the need for multiple systems and software packages with a single appliance, purpose built for virtualized workloads. For example, SimpliVity is a great starting platform for Hadoop data lakes or object storage environments supporting sensor fusion exploratory or limited-scope projects.

If, on the other hand, you need a dedicated all-flash array (AFA), Nimble provides a robust always-on set of data services, easily configured with built-in app-aware snaps and replication, delivering 6-nines High-Availability. Nimble also provides a minimum of 5X data compression through automated, non-invasive procedures including variable block deduplication and compression, zero pattern elimination and zero copy clones and thin provisioning – all without performance penalties.

SimpliVity has efficiency as a primary goal, met through collapsing server and storage into a single system, supported with always-on deduplication and compression and native back-up and recovery.

If you need even greater availability, configurability, and scale, 3PAR offers large data center and multi-site 6-nines HA with zero RPO/RTA and can be paired with composable infrastructure platforms like Synergy for rapid set-up and tear down of multiple workloads (great for dev/test environments often associated with big data analytics and a cadre of data scientists and developers using say R-Library), or large scale high-performance computing (HPC) environments like the Apollo series (great for SAP Hana and other in-memory databases that use large datasets to create and mine patterns in support of machine learning).

Of course, data governance is a key consideration and there are several guidelines that must be taken into account. At the base infrastructure level, data governance starts with data protection. SimpliVity, Nimble, and 3PAR all have built-in schemes for disaster recovery. In the case of SimpliVity, for example, typical restore of 1TB of data (a VM or set of VMs) takes 60 seconds. Nimble has a global data collection and pattern recognition system called Insight, and is capable of isolating potential faults, eliminating potential problems before they happen 86% of the time. Similarly, 3PAR transfers diagnostic information such as system health information, configuration and performance data, and system events classified as telemetry data (metadata) to a 3PAR central monitoring system for remote diagnostic analysis and proactive fault detection.

Table of Contents	Introducing Aruba: The Intelligent Edge for Defense and Intelligence Networks	PointNext: Taking Digital Transformation to the Next Level with HPE Flexible Capacity	HPE Synergy: Composable infrastructure for Defense and Intelligence Agencies
Gen10: Cyber Hardening Defense and Intelligence Infrastructures with the World's Most Secure Servers	Meeting the Demands of Modern Defense with ProLiant DL380 Mil-Spec Servers	Overhauling Your Information Management Layer to Support the Age of Information Warfare with 3PAR	For more Information

Encryption of data at rest and in transit is also a core baseline security requirement in DoD and IC environments. Since SimpliVity runs on the DL380, it inherits all of the encryption specifications for the DL380 (see the DL380-specific chapter in this eBook). Nimble SmartSecure encrypts data with the AES-256-XTS cipher for encryption and decryption of all data volumes, or optionally just specific data volumes, leveraging the Intel AES-NI instruction set on later-model arrays in the Nimble CS-Series[3]. When an encrypted volume is set offline and deleted, the corresponding volume key is marked inactive, effectively shredding the data.

Nimble storage adheres to NIST guidelines as outlined in the FIPS-140-2 policies[4] (evidence of tampering noted in level 2 versus level 1). 3PAR already has extensive use in the DoD and IC and adheres to all relevant security guidelines and policies for encryption at rest (AES encryption with 256 and 512-bit keys) and FIPS 140-2[5]. Drives in the 3PAR AFA are self-encrypting drives (SED) and encryption cannot be turned off and any attempt to remove encryption forces a data shredding process.

Handling the information management at the Intelligent Edge

As mentioned earlier in this chapter, between the rapid increase in IoT such as drones and other sensors, and even smaller modular data centers being placed on ships and in forward command posts, large increases in edge intelligence is unavoidable. Nimble can serve as a remote storage platform front-ended by Moonshot and Aruba networking for edge data collection, processing, and visualization. SimpliVity and Nimble can locally support what was once running in large data centers in distributed edge environments including VMs, containers and databases running on top of them, ranging from Microsoft SQL to edge IoT analytics like GE® Predix or visualization using Tableau.

In many cases the intelligent edge for defense and IC use cases may be in environments where you would need to rely on preventative maintenance to assure continuous availability of information systems. Nimble all-flash storage fabric has best-in-class predictive analytics to predict and prevent problems before they happen without costly or specialized local support. Where problems arise from external, non-IT causes, built-in support to reliably and automatically mirror that local set of data into secondary flash in the cloud provides rapid mission continuity.

[3] https://cdm-cdn.nimblestorage.com/2017/03/17154128/SmartSecure-Encryption-Technical-White-Paper.pdf

[4] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2422.pdf

[5] https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA4-7605ENW.pdf

HPE, your one-stop shop for end-to-end information management and analytics – now and into the future

SimpliVity, Nimble and 3PAR all have built-in schemes for disaster recovery

The near-term future is set for information management. Hybrid cloud will be the approach in the federal government – including the DoD and IC – based on more server-based storage through hyperconverged platforms, the next stage of grid computing. Where separate larger storage volumes will be needed, by default, they will be all-flash arrays with automated software for granular back-up and retrieval over high-bandwidth cloud connections. As described in the sections above in this chapter, HPE is making the right acquisitions and, in parallel, internally engineering and productizing state-of-the-art systems to satisfy these market needs. Additionally, HPE laboratories is conducting research and development into successive generations of memory that will be far denser, faster, and frugal in power consumption.

In May 2017, HPE labs demonstrated a 1,280-core system with 160 TB of shared memory (standard volatile direct access memory), the largest of its kind and the first tangible implementation of our vision for "the Machine." The demo performed a typical BDA graphing analysis that searched for an insider cybersecurity threat, a common use case for DoD and IC platforms and applicable to countless other cases they face. Within the next few years HPE Labs plans to test further advancements in the Machine roadmap including optical interconnect between core processing modules and even larger repositories of non-volatile memory, coined "memristors[6]."

Memristors involve a dynamic non-linear device filled with atoms moving meters per second vs. a static device and joule heating drift diffusion for different carriers, ballistic and interfacial thermal transport and thermophoresis effect. The process examines temperature and electronic behavior in memristor cells during diffusion switching patterns. A scanning thermal microscopy technique is also used for x-ray absorption for temperature mapping. Based on what we know now, all are relevant to the IC though clearly still in an R&D phase.

HPE labs is continually innovating and helping the IC to respond to changes in the cyber threats we face globally.

Learn more at

www.hpe.com/us/en/storage/3par

a00017560enw, July 2017

Hewlett Packard Enterprise