DaaS with Analytics and Proactive Management

Security and Privacy

WHITEPAPER

Published: September 2017

This document applies to the September 2017 HP DaaS service update.
For additional information, please contact your HP representative.
4AA7-1182ENW

Table of Contents

Introduction

As more of IT is outsourced to the cloud, new security and management challenges arise due to the disaggregation and multi-tenancy of systems. This is compounded by the need to operate across enterprise, regulatory and geographic boundaries, all in the context of an increasingly complex threat environment. HP's goal is to provide our customers with assurance, insight and control when using HP's products and services in this new world.

HP relies on many different centers of engineering excellence to develop technologies ranging from embedded control points within devices through high level models of cross-boundary automated management. These provide a robust chain of trust from top to bottom. Additionally, HP is constantly exploring new mechanisms for the detection and mitigation of modern attacks of massive scale.

Security thought leadership

HP's commitment to security does not end with its products. The company plays an important role in advocating for security best practices within its partner ecosystem and in providing training and resources to hundreds of thousands of independent IT resellers and services providers worldwide. In fact HP was the first Master Training Partner selected by the Cloud Security Alliance. The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA operates the most popular cloud security provider certification program, the Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program of self-assessment, third-party audit and continuous monitoring.

As a well-established security technology vendor in cloud computing and information security globally, HP is well-positioned to offer vendor-neutral information security training focusing on real-world security processes and implementation. With learning centers worldwide, numerous partner facilities and customer's onsite locations, HP offers courses that draw from 35+ years of meeting complex technology training requirements.

Service-Level Security

In the 1950s, Edwards Deming and others introduced quality concepts such as Total Quality Management (TQM) to manufacturing. This first took hold in Japan, resulting in Japanese automotive quality greatly surpassing U.S. automotive quality. Quality transformation arrived in the United States in the 1970s, in the IT software arena in the 1980s and at HP with CEO John Young's 10X quality initiative. Its goal was to improve software quality by an order of magnitude within a decade. These quality initiatives focused on repeatability, building-in quality, managing quality, and going beyond testing.

Fast forward thirty years, and this comprehensive approach to quality has resulted in the development of significant capabilities to build cybersecurity resiliency into hardware, software applications and products, and HP's teaming with best-in-breed third-party technology vendors.

Security is maintained by deploying security controls at every layer. In the event of a failure at one layer, controls are in place in other areas to minimize breaches and maintain security at all times.

As a one-stop, cloud-based solution for managing an organization's devices, data, and users, HP DaaS applies industry-proven, service-level security in its architecture as well as its development processes.

HP DaaS Architecture

The HP DaaS with Analytics and Proactive Management (hereafter referred to simply as HP DaaS) architecture consists of the following:

- HP DaaS Backend – Cloud Service that uses the Internet to send tasks to and receive status updates from HP DaaS clients
- HP DaaS Portal- Security enhanced landing page to sign up, sign in and manage account(s)
- Identity Management Component (IdM) - Used to authenticate users
- Device Communication Gateway Component (DCGC) - Provides a security enhanced communication path between the HP DaaS server and all managed devices
- HP DaaS Core – Backend transactional processes that determines roles and privileges
- Services – Modules that provide the actual services to the users

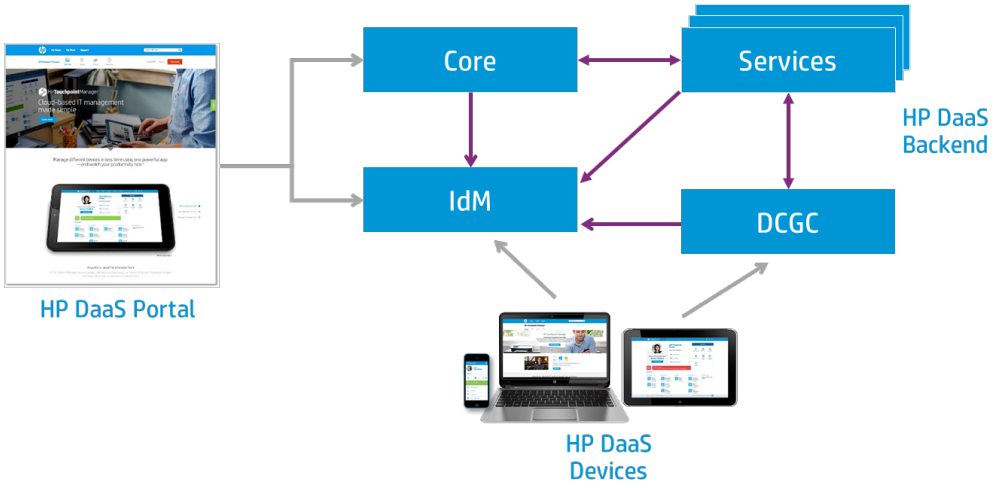

Figure 1: HP DaaS Architecture

From an architectural perspective, HP Daas has been designed to help prevent attackers from gaining control over user devices. The user's knowledge and approval are required prior to enabling management control. The user is able to determine what entity is requesting permission to manage the client (i.e., they are able to verify that all policy setting changes and execution commands come from HP DaaS). In addition the content and source of all communications from HP DaaS must be validated by the managed client, and the client is able to confirm that the provisioning was properly performed.

Depending on the operation system, an agent or client application is required and installed on each device during the provisioning process to provide the user with validated information regarding the HP DaaS request to manage their device.

Similarly, the HP DaaS server must know that the current settings, events, and results received from the managed device are accurate. The content and source of all communication from the managed device are validated by the server, and the means of validation is established as part of the managed device enrollment process.

Agent deployment and specifics

For devices running the Microsoft Windows desktop operating system, HP DaaS deploys a lightweight agent upon the enrollment of a user device for remote management. This agent checks in at regular intervals to receive commands from the server to perform specific tasks. The agent also communicates back to the server with the device-specific data it has collected, along with reporting the success or failure of server commands. HP follows a secure development process (detailed later in this document) for all software, including the HP DaaS agent software. This process involves the use of development best practices, security threat modeling, and static code analysis to protect against agent manipulation or hijacking.

The HP DaaS Windows agent uses Port 443 (standard SSL port) for all communications. When installed on Windows devices, the agent polls the server at least once every 24 hours. HTTPS is the only protocol used for any communications between the server and the client for all Windows devices. In addition, public key pinning is employed. This is a technique whereby the agent only connects (via HTTPS, of course) to a server that has a specific SSL certificate – in this case the HP DaaS production site certificate. The service also utilizes a different set of cryptographic keys as an additional level of digital signing and verification for every message exchanged between the server and the agent.

Note that HP DaaS does not install any certificates or otherwise tamper with the operating system's certificate store. As such, we do not introduce the system modifications made by the existence of adware.

HP Secure Software Development Lifecycle (SSDL)

Typical industry approaches to application security have been reactive and have failed to apply lessons from the quality field. The two prevalent approaches are:

- "Bury head in the sand" – characterized by reactive security patching. This approach relies on CVEs, with little work to avoid or minimize vulnerability introduction. This is most often seen in industry segments with a minimal security relevant regulatory burden.
- "Test security in" – noticeable by the lack of resiliency designed into applications. Instead, effort is applied to find and fix vulnerabilities during testing, in combination with security patching. This approach appears more commonly in the public sector, security regulated industries and healthcare. These segments must show compliance with regulations including the United States' Federal Information Security Management Act (FISMA), the Payment Card Industry Data Security Standard (PCI-DSS), the Health Information Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH).

However, security as a quality attribute needs to be applied at every stage of the lifecycle in the same way the quality field learned it decades ago. Key tenants include:

- Quality cannot be tested in; it has to be designed and built in, and then tested.
- It is much less expensive to find defects – in this case security defects and vulnerabilities – early, rather than late, in the lifecycle.

HP takes software security very seriously and, as a result, it has adopted a Secure Software Development Lifecycle (SSDL). Several goals are tied to this process:

- Reduce the cyberattack surface via secure software architecture
- Minimize code-induced vulnerabilities
- Protect the privacy and security of customer data and identities

To this end, HP includes specific security related procedures in its software development processes, performs milestone reviews to ensure security processes are successfully completed and delivers on-going security training to its software architects, developers, test engineers, program managers and their management.

There are seven stages in the SSDL process. Each stage is outlined below:

- **Training (Stage 1)** – Formal courses covering the SSDL process, security enhanced design, threat modeling and secure coding
- **Requirements (Stage 2)** – Planning for security at the very start of the software project, including a feature-by-feature security risk assessment
- **Design (Stage 3)** – Defining and documenting the security architecture; identifying critical security components
- **Implementation (Stage 4)** – Executing the designed protection scheme and the mitigation approach, along with peer code reviews and validations
- **Verification (Stage 5)** – Performing dynamic code analysis, fuzz testing and attack surface reviews
- **Release (Stage 6)** – Verifying the SSDL requirements have been met and no known vulnerabilities exist
- **Response (Stage 7)** – Executing the response tasks outlined during the Release stage

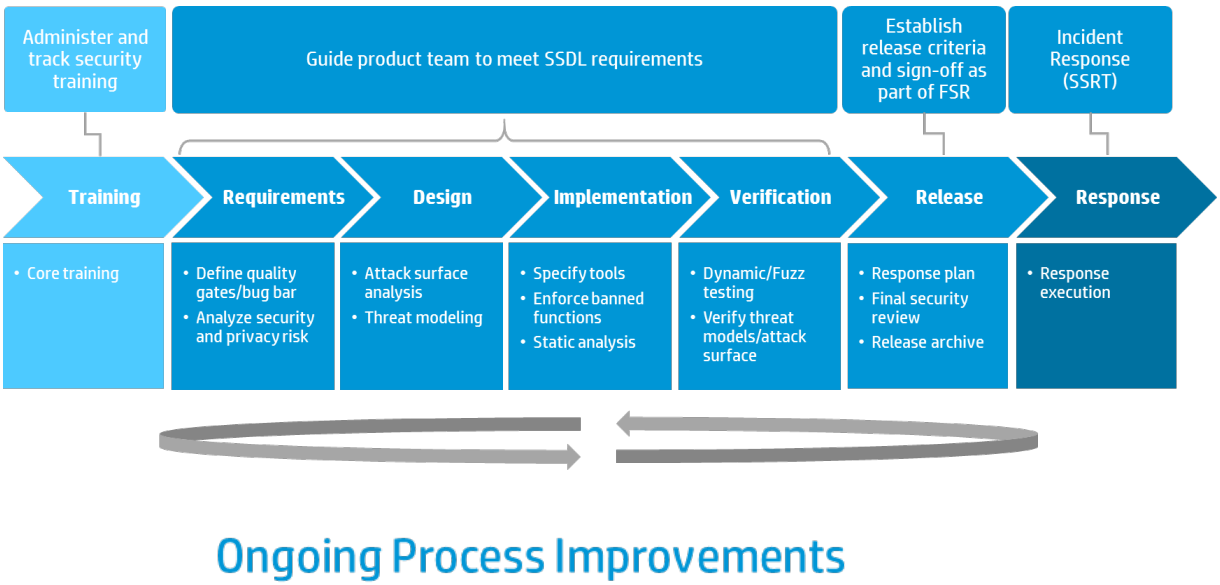

Figure 2: HP Secure Software Development Life Cycle

HP DaaS' Service-Level Security

This section describes how HP DaaS applies Service-Level Security to ensure security at various layers of communications.

Data center

The HP DaaS application is hosted by Amazon Web Services (AWS), more specifically Amazon Elastic Compute Cloud (Amazon EC2). Amazon EC2 provides scalable computing capacity in the AWS cloud. When using AWS, HP DaaS can leverage Amazon's more than fifteen years of experience delivering large-scale, global infrastructure in a reliable, secure fashion. For more information, please refer to the AWS information portal: http://aws.amazon.com/ec2/.

At the physical layer, it is important to address the controls that are in place to secure facilities and the network. Customer and device data is stored in AWS data centers that are geographically distributed to provide redundancy. AWS is a recognized leader in cloud hosting. By partnering with AWS, HP DaaS inherits a cloud infrastructure that has been architected to be one of the most flexible and secure cloud computing environments available today. Some of its key security characteristics include:

- Designed for security – AWS cloud infrastructure is housed in AWS data centers, designed to satisfy the requirements of its most security-sensitive customers. The AWS infrastructure has been designed to provide high availability while putting strong safeguards in place regarding customer privacy and segregation.
- Highly automated – AWS purpose-builds most of its security tools to tailor them for AWS's unique environment and scale requirements. These security tools are built to provide maximum protection for data and applications. This means AWS security experts spend less time on routine tasks, making it possible to focus more on proactive measures that can increase the security of the AWS Cloud environment.
- Highly available – AWS builds its data centers in multiple geographic regions as well as across multiple Availability Zones within each region to offer maximum resiliency against system outages. AWS designs its data centers with significant excess bandwidth connections so that if a major disruption occurs there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.
- Highly Accredited - Each certification means that an auditor has verified that specific security controls are in place and operating as intended. You can view the applicable compliance reports by contacting an AWS account representative. For more information about the security regulations and standards with which AWS complies, see the AWS Compliance webpage. To help you meet specific government, industry, and company security standards and regulations, AWS provides certification reports that describe how the AWS Cloud infrastructure meets the requirements of an extensive list of global security standards, including: ISO 27001, SOC, the PCI Data Security Standard, FedRAMP, the Australian Signals Directorate (ASD) Information Security Manual, and the Singapore Multi-Tier Cloud Security Standard (MTCS SS 584). For more information about the security regulations and standards with which AWS complies, see the AWS Compliance webpage.

For detailed information on physical and environmental security, AWS access and network security, please read the AWS Overview of Security Processes whitepaper.

Network

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACLs), and configurations to enforce the flow of information to specific information system services.

ACLs, or traffic flow policies, are established on each managed interface, which manage and enforce the flow of traffic. ACL policies are approved by Amazon Information Security. These policies are automatically pushed using AWS's ACL-Manage tool, to help ensure that these managed interfaces enforce the most up-to-date ACLs.

Security enhanced access points

AWS has strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints, and they allow HTTP access (HTTPS), which allows you to establish a secure communication session with storage or compute instances within AWS. In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet service providers (ISPs). AWS employs a redundant connection to more than one communication service at each Internet facing edge of the AWS network. These connections each have dedicated network devices.

Application, host and administrator security

At the logical layer, different controls are implemented to secure the host systems and applications running on those systems, and for administrators who manage the host systems and their applications.

Administrator access to HP DaaS and customer data is limited and strictly managed. Only those individuals essential to performing a task are permitted access provided they meet the appropriate background checks and account management requirements.

Data security

Data exchanged with HP DaaS uses the AWS implementation of Transport Layer Security (TLS) v1.2, the newest form of the industry-standard Secure Sockets Layer (SSL) protocol. TLS helps to secure data at several levels, providing server authentication, data encryption, and data integrity. Because TLS is implemented beneath the application layer, it is a passive security mechanism that does not rely on additional steps or procedures from the user. This allows client applications and their users to have little or no knowledge of secure communications and still be better protected from attackers. These features help secure data from incidental corruption and from malicious attack, and are intended to avoid common web-based threats. In addition to the SSL encryption for network communication between the agent and the server, HP encrypts logs and "data at rest" (data stored in our server database). The encryption algorithm used is AES-256 in CBC mode. An example of data encrypted using this algorithm is device location.

Client devices managed by HP DaaS must have the operating systems and client side software set forth in the system requirements for HP DaaS. While HP DaaS can help enforce security policies to specific devices as defined by the DaaS administrator, there is no other security requirement for end user deployment other than his/her login email and password. The employee's login email and password are encrypted with AES-128 bit encryption through the TLS protocol upon logging in.

Independent verification

To ensure security for the HP DaaS solution, periodic penetration testing of the web application is performed by a cybersecurity organization. This security assessment service ensures that application security controls are in place and functioning correctly. This testing includes, but is not limited to, denial of service attempts, stress testing all of

the network interfaces, and fuzz testing of all file formats consumed by the component. Penetration testing performed by internal and external parties provides important insight into the effectiveness of security controls for our service. The outcome of these reviews and ongoing evaluation of the resulting controls are used in subsequent scanning, monitoring and risk remediation efforts. The results from this type of penetration testing contain sensitive and private information and will not be shared with customers.

ISO 27001 certification

The security of information systems and business-critical information needs constant measurement and management. ISO 27001 certification is verification of HP's commitment to deliver operational continuity and data protection.

ISO is the International Organization for Standardization. ISO is responsible for the development of a number of internationally recognized standards for products, services and systems. ISO 27001 certification is awarded upon the completion of an external audit by an accredited external certification body and is asset based (information, processes, people and technology). HP has achieved ISO certification across the Remote Monitoring and Management Services environment, for both Managed Print and Personal Systems Services.

ISO 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS) within the context of an organization. An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems, and consists of a number of supporting documents and guidelines defining the implementation and certification path.

Based on the principles of confidentiality, integrity and availability, HP's ISO 27001 certification covers:

- Information security policies
- Operations security
- Organization of information security
- Communications security
- Human resources security
- System acquisition, development and maintenance
- Asset management
- Supplier relationships
- Access control
- Information security incident management
- Cryptography
- Information security aspects of business continuity management
- Physical and environmental security
- Compliance

Data Collection, Retention, Privacy

Data collection

HP DaaS gathers specific data on devices and users in order to perform IT management tasks. A listing of the data collected follows.

Device data that are collected by HP DaaS may include the following groupings:

- Hardware – including battery, BIOS, disk, display/monitor, graphics, inventory, memory, network interface, PnP, processor, system clock, system slots, thermal and system performance data
- Software – including compliance, errors, inventory, performance, utilization and web application utilization data
- Security – including non-reporting devices, third party and operating system patch discovery/management, device location, device alarm, lock and wipe, security policy setting, security policy enforcement, security threats, storage encryption, user security settings, Wi-Fi provisioning, and Windows Information Protection violations data
- Windows Event Logs
- HP Warranty and Care Packs

User data that are collected by HP DaaS include:

- User email address
- Last logged on user account
- Number of consecutive failed logon attempts (resets to zero when a user logs on)

Data privacy

Data privacy is governed by the HP privacy policy for countries worldwide. This policy is updated periodically and can be viewed at http://www8.hp.com/us/en/privacy/ww-privacy.html

The privacy policy covers the following topics:

- Collection of personal information
- How HP uses your information
- How HP shares your information
- Children's privacy
- Your choices and selecting your privacy preferences
- Access to and accuracy of your information
- Keeping your information secure
- Changes to this statement
- Contacting HP
- Automatic data collection tools

Data storage

Data storage for HP DaaS is limited to the user and device information of paying subscribers.

Data retention

Data retention is an important piece of any compliance program and necessary to fulfill proper stewardship of data. HP's data retention policy incorporates the following data retention best practices:

- Maintaining data for shorter than necessary periods can violate contractual or legal requirements, or affect security.
- Maintaining data for longer than necessary periods can violate privacy regulations and is a top customer concern and sales inquiry.
- Once data is deleted, there is no obligation to provide it to the customer or law enforcement.

HP DaaS customer data is backed up nightly and retained. The data exists for disaster recovery purposes only; there is no "point-in-time recovery" as part of the service. Upon account cancellation, the HP DaaS agent must be uninstalled to prevent further data collection. Any paper documentation containing MBI, HBI or PII is destroyed by a secure shredding service. HP DaaS does not use or retain any paper documentation.

Furthermore, HP DaaS limits its user and device data storage to paying customers.

Service Monitoring & Reporting

HP DaaS provides service updates regularly to deliver the latest features and updates to customers. HP DaaS also notifies customers through various methods including email of scheduled or unscheduled updates and changes to the service. For planned service interrupting events such as service maintenance, customers are notified eight hours in advance.

To deliver optimal service, HP conducts ongoing service monitoring and reporting.

Service monitoring

The HP DaaS application and website are monitored on a 24x7x365 basis for reliability and performance. In addition, network performance and availability monitoring occurs on a continuous basis. All of the monitoring tools route any issues, warnings, and problems directly to service engineers. Exceptions are automatically raised to an internal ticketing system as high-priority work items requiring acknowledgement.

The service is polled every minute in accordance with response thresholds:

- Server side response to be <400ms
- Browser response time to be <3 seconds

If a threshold is exceeded, the following automatic escalation process occurs:

- An email alert is sent to a corresponding Matrix Engineer on call
- A push notification to the mobile device of the Engineer on call is sent
- An email is sent to the Operation Team distribution list

The service utilizes different monitoring tools including:

- **New Relic** - Monitors various components of the system and more importantly, helps identify and debug bottlenecks when they appear. Most of the applications/services have been instrumented for New Relic thereby providing continuous data collection and near real-time performance metrics.

- Amazon **CloudWatch** - Monitors for events related to provisioning, service failures, and threshold attainment (such as memory consumption). Transaction monitoring and testing of all available services to simulate critical customer scenarios (incrementally increasing the number of users and device ratios to transaction available) are accomplished with a third-party monitoring solution. This third-party solution monitors for events related to the portal, trial sign-up, application sign-in and scale group availability.

Service reporting

After each development sprint and/or service update release, all incidents are reviewed and categorized to identify the most significant problem areas. A post-mortem quality of service (QoS) meeting is held to review findings, identify root causes, and implement changes for improvement.

Service uptime availability is also monitored daily and reviewed monthly. The ratio of failures to successes gives HP DaaS its availability for the month.

Although HP DaaS does not disclose internal incident logs or historical data on availability to customers, HP demonstrates its commitment to quality of service targeting 99.9% uptime.

Security for User Access & Control

Access rights

HP DaaS uses role-based administration to control application access rights. There are two key roles available for any HP DaaS account:

- An IT administrator role is the primary account holder and is responsible for managing devices on behalf of employees at a company.
- An Employee role is a user that an IT administrator has authorized as a user within the company's account and can manage the devices he/she personally uses to carry out his work.

HP designed HP DaaS to perform centralized and secure IT management. Consequently the following controls govern the behavior of accounts:

- An IT administrator is allowed to modify (via a centralized dashboard) any policy setting that a user can modify.
- An IT administrator can prevent a user from changing any setting that is under his/her control. The user's ability to *view* the managed settings is controlled by policy.
- The current state of all settings can be retrieved, whether the accounts are controlled by the administrator or under control of the user.

Identity management

There are currently two Identify Management mechanisms supported: HP DaaS User Login ID and Azure Active Directory federation.

HP DaaS Login ID requires the password to be at least 6 characters in length; one capital letter, one lowercase letter and one number. Strong passwords, such as those using a combination of letters and numbers, is recommended, but not required. Password history is not retained, and a forced change of the password on a periodic basis is not available at this time. With HP DaaS Login ID, the password recovery is done based on the user submitting his/her email address to receive a reset link. Adding a new user is as simple as entering the user's email address into the new user administration and inviting them to the system. Users can be removed from the system by removing the user in HP DaaS.

Session management

Currently there is no limitation on the number of sessions a user can have. User sessions timeout after 30 minutes of inactivity and device sessions timeout after 24 hours of inactivity. A user account is locked after five consecutive failed authentication attempts. To recover a password, the user may submit his/her email address to receive a reset link.

Field validation

Field validation is used to protect form input fields in the HP DaaS application. Validation is provided by data type (string, date/time, currency, etc.) and business rules (required or recommended). Fields may also be secured by business role and operation (read/write). Additional validation may be applied using scripting functions.

Conclusion

HP recognizes that the threat landscape changes rapidly. The evolution of cyberattacks began with file deletion and website defacement in the late 1990s, then moved into the monetization stage with stolen credentials and ransomware. Most recently attacks are being waged by nation-states that are extremely well funded and intent on bringing down power grids and rendering tens of thousands of computers and mobile devices inoperable.

Addressing these risks is a mission HP embarked on more than forty years ago. HP's legacy of innovation in security threat detection and protection and current security-focused investments inform the design of applications such as HP Daas with Analytics and Proactive Management. The result is the delivery of a secure cloud-based IT management solution built on an integrated security platform that spans the application, physical data center, and end-user access. With built-in security features, HP DaaS offers even organizations with limited IT resources a tool they can trust to simplify everyday management of their devices, data and users with multiple and strong layers of security.