HP Device as a Service (DaaS)

HP DaaS Proactive Security

Frequently Asked Questions (FAQ)

For Customers

This document answers the most commonly asked questions related to the HP DaaS Proactive Security offering.

HP DaaS Proactive Security FAQ for Customers

Q: What is HP DaaS Proactive Security?

A: HP DaaS Proactive Security[1] is an add-on service to HP Device as a Service (DaaS) plans to enhance security and cyber threat protection. It includes software, analytics, and service elements. The service delivers enhanced security for devices through unique real-time threat isolation technology protecting against malware introduced through e-mail, browsers, and files, complementing the protection provided by a customer's existing security solutions. It extends the security insights and reports provided by HP TechPulse analytics. As a result, HP Device as a Service customers can better protect against, understand, and respond to threats. The Enhanced Proactive Security plan delivers a managed service from HP with specialized experts to monitor and enforce endpoint protection and analyze threats to help you strengthen your security position.

In addition, beginning in the U.S., HP has partnered with Aon to offer HP DaaS Proactive Security customers complete cyber security solutions that include assessment, incident response, and insurance services.[2]

Q: Why should I consider purchasing this service?

A: HP DaaS Proactive Security enhances the secure management capabilities of HP Device as a Service (DaaS). It provides real-time malware protection for computing endpoints, security and threat analytics, and specialized expertise to help strengthen an organization's security position.

Q: What Proactive Security plans are available and what are the differences between them?

A: HP DaaS Proactive Security is available with two plan options. The Standard, self-managed plan includes isolation software and provides access to security analytics and reports via the HP analytics dashboard and will be available for standard, enhanced and premium DaaS plans.

The Enhanced plan adds a managed service from HP with specialized cybersecurity experts to monitor and enforce endpoint protection and analyze threats for Windows 10 devices to help you strengthen your security position. The Enhanced, managed version of DaaS Proactive Security will require either an enhanced or premium DaaS plan.

Q: Which plan is right for your organization?

A: HP DaaS Proactive Security plans are designed to fit your needs for endpoint security whether you want to self-manage or have HP manage on your behalf.

- If you already have a self-managed, unified endpoint management solution for security policy setting and enforcement but want to take advantage of HP DaaS proactive malware technology and analytics and reports for a more proactive security position, the Standard plan may be the best option.
- It you want to offload day-to-day device security and management tasks to HP Service Experts[3], or if you don't have your own team focused on endpoint security, the Enhanced may be the best fit.

[1] System requirements for HP DaaS Proactive Security are: multi-vendor client devices running Windows 10 1703 or later with a minimum of 8 GB memory and 6 GB of free hard disk space to install the software client. HP DaaS Proactive Security requires HP TechPulse, which is included in any HP DaaS or HP DaaS Proactive Management plan. The HP DaaS Proactive Security Enhanced plan requires customers to be enrolled in an Enhanced or Premium HP DaaS or HP DaaS Proactive Management plan. For full system requirements, please visit www.hpdaas.com/requirements. iOS devices are not covered in the Standard plan.

[2] Purchasers of HP DaaS Proactive Security in the U.S, receive the Aon Cyber Quotient Evaluation (CyQu) self-assessment and security score. $0 retainer and one-hour consultation included with optional incident response services from Aon. HP onboarding service representatives will provide instructions.

[3] Security Experts available in the Proactive Security Enhanced plan only.

Q: Who can benefit from HP DaaS Proactive Security?

A: HP DaaS Proactive Security offers security capabilities for new and existing DaaS customers and was specifically developed for those who desire to improve their endpoint security posture and lack security expertise and/or bandwidth.

Q. What security analytics and reporting are available to customers via HP TechPulse through this service?

A: Through the HP TechPulse dashboard, HP DaaS Proactive Security customers will have access to analytics for device protection state and detected threats associated with the service's software. These analytics include detailed status of the agent software on managed devices, and identify devices where protection is not active, indicating the PC is at greater risk from malware-based attacks. In addition, the dashboard shows a wide range of protection metrics for actual threat isolation events across the enterprise including type and source of threats, as well as most impacted devices and most at-risk users.

Q: With the Enhanced, HP-managed plan, what tasks do the HP Service Experts perform?

A: With the Enhanced Plan, HP Service Experts manage and monitor the threat isolation protection that comes with HP DaaS Proactive Security and notify the customer with reports whenever protection has been disabled on a device. When threats are blocked, they perform deeper analysis and identify any NEW malware using kill chain assessment tools.

Q: Why is endpoint security so important?

A: Research shows that the weakest link in an organizations' security is often the endpoint. For example, an estimated 92 percent[4] of malware infections originate from email sent to an end-user device. While most organizations already have multiple layers of security, these layers all focus on protecting devices from *known* malware.

HP uses virtualization technology[5] to isolate risky activity from the host PC and to identify and protect against *unknown* malware. By isolating unfamiliar applications, attachments, links, and executable downloads, in separate micro-virtual machines, this service not only prevents the devastating effects of a cyber-attack but also gives you a full kill chain of the attack to help protect your entire enterprise.

Q: Is this solution meant to replace anti-virus?

A: This technology is not a replacement for detection-based anti-virus solutions. Such solutions are useful for a wide range of threats and may be required in highly regulated industries, but they can fall short in cases of ever changing malware and zero-day attacks. By providing proactive content isolation, instead of quarantine after detection, this solution delivers a last line of defense against application-level attacks.

Q: How is this approach to endpoint protection different from detection-based anti-virus solutions?

A: This technology works through proactive isolation and containment rather than detection. Sources of potential attacks, such as malicious websites, email attachments and infected links are opened in isolated containers that allow the malware to detonate inside a hardware-enforced virtual machine at the CPU level. This approach keeps the threat from infecting the endpoint or spreading across the network. Because documents and browser tabs are opened in isolation, even zero-day threats are contained.

[4] 2018 Data Breach Investigations report 11th Edition, Verizon, 2018*8*

[5] HP Sure Click Advanced technology is included with HP DaaS Proactive Security and requires Windows 10. Microsoft Internet Explorer, Google Chrome™, and Chromium™ are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe® Acrobat are installed.

Perhaps best of all, these containers are created in the background so there is no impact to the user workflows and people can work the way they normally do, eliminating the risk of visiting a malicious website or opening an infected file.

As a contrast, traditional and "next generation" anti-virus (AV) solutions operate on a detection method rather than HP's isolation technology:

- Traditional AV solutions work on a detection mechanism that must be constantly updated.
- This is an increasingly challenging approach as new malware has rapidly grown to thousands of new malicious software "products" introduced almost daily.
- The AV solution provider must update their databases regularly.
- Companies deploying the AV solution must also update or refresh their solution routinely.
- Next Generation AV solutions are also detection-based but not tied to a comparison database.
- Next Generation AV solutions use machine learning and other software algorithms to identify malware and other malicious actors.
- Next Generation AV solutions can provide a "false positive" by incorrectly categorizing software as malicious and erroneously block good software.

Q: Can this service be customized?

A: *Some* customization is available. For example, individual customers can create a whitelist of websites and email domains that will not be subject to isolation. Beyond whitelisting, other customizations including blacklists, group policies, etc., are not available with this service currently.

Q: How does the customer onboarding process for HP DaaS Proactive Security work?

A: Customers are onboarded the same way as they are with HP DaaS Proactive Management. A Service Manager contacts the customer via email to provide a Welcome kit and kickoff the onboarding process. For new customers, onboarding for HP DaaS Proactive Security coincides with onboarding for HP Proactive Management. If the customer is already a user of HP Proactive Management, Proactive Security license activation is added.

Note: This service does require the customer to install a separate agent to devices covered by the plan. See the *HP DaaS Proactive Security – Service Definition* document for more details on the customer onboarding process.

Q: What operating system does HP DaaS Proactive Security support?

A: HP DaaS Proactive Security requires Windows 10 1703 or later operating system.

Q: What browsers are supported?

A: Supported browsers Include:

- Internet Explorer (32-bit and 64-bit version 9 and later)
- Google Chromium-based browser (32-bit version 55 & later)
- Google Chrome (then current 64-bit version)
- Firefox (then current 64-bit version)
- Edge

Q: What are the hardware requirements for HP DaaS Proactive Security?

A: System requirements for HP DaaS Proactive Security are multi-vendor client devices running Windows 10 1703 or later with a minimum of 8 GB memory and 6 GB of free hard disk space to install the software client.

Q: What is the value-add from the Aon components?

A: Even with the most proactive security protection of computing endpoints, breaches can happen. Aon services help organizations ensure they are prepared to quickly mitigate an incident and protect against financial damages.

HP DaaS Proactive Security customers in the U.S. can take advantage of Aon's Cyber Quotient Evaluation (CyQu), a powerful cybersecurity resilience assessment tool with a security scorecard with industry benchmarking. In addition, customers of HP DaaS Proactive Security are eligible for a $0 incident response retainer and one hour of consultation if a breach[6] occurs. Finally, because of the strong security foundation provided by HP DaaS, you may also be eligible for cyber insurance policies with enhanced terms and conditions[7] and a streamlined application process through Aon.

Q: Is HP DaaS Proactive Security priced separately from an HP DaaS plan?

A: Yes, HP Proactive Security is priced separately from HP DaaS plans. Like the HP DaaS plans, pricing is on a per device per month basis. Contact your HP representative or an authorized partner for more details.

Q: Is HP DaaS Proactive Security only available to HP DaaS customers? Are there other requirements?

A: Yes, HP DaaS Proactive Security is only available to new or current HP DaaS customers. HP DaaS Proactive Security requires HP TechPulse, which is included in any HP DaaS or HP DaaS Proactive Management plan. The HP DaaS Proactive Security Enhanced plan requires that customers be enrolled in an Enhanced or Premium HP DaaS or HP DaaS Proactive Management plan.

Q: In what countries is it available?

A: HP DaaS Proactive Security is a worldwide offer that will be available in the same countries and languages as HP DaaS plans with Proactive Management. Initially, the Aon components will be available in the U.S. only with additional countries being added over time.

Q: When will HP DaaS Proactive Security be available?

A: HP DaaS Proactive Security will be available to customers in April 2019.

Q: Where can I learn more about HP DaaS Proactive Security?

A: For more information, visit: hp.com/go/DaaS.

Q: Where can I find more information about HP DaaS?

A: Additional information about HP DaaS and its related services and options is available at www.hp.com/go/DaaS.

4AA7-4572ENW - March 8, 2019

[6] Purchasers of HP DaaS Proactive Security in the U.S receive the Aon CyQu self-assessment and security score. $0 retainer and one-hour consultation included with optional incident response services from Aon. HP onboarding service representatives will provide instructions.

[7] Cyber insurance policy eligibility and quotes based on a variety of factors including the organization's HP DaaS Proactive Security plan, industry type, Aon's CyQu report, and carrier selected.