



# **HP Proactive Security Offer**

## **Frequently Asked Questions (FAQ)**

### **For Customers**

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



# HP Proactive Security FAQ for Customers

## Q: What is HP Proactive Security?

**A:** HP Proactive Security<sup>1</sup> is a protection-first approach to managing endpoint security. It reduces your risk from attacks and gives users the freedom to work securely from anywhere without increasing IT workload. Proactive Security integrates 1) multi-layered, government-grade anti-malware protection combining deep learning and isolation technologies – along with 2) actionable insights and 3) management by cybersecurity experts – delivered as a service.

## Q: Why is endpoint security so important?

**A:** Customers face a wide range of challenges with the emerging security threat landscape. Endpoint security is critical, but current approaches are falling short. With 350,000 new malware variants released every day<sup>2</sup>, protecting against these threats is increasingly challenging. Traditional, signature-based, anti-virus solutions help protect against known threats, but are ineffective against unknown, or zero-day, threats. Today, over 57% of new malware infections bypass, disable or are ignored by traditional anti-virus<sup>3</sup>. Zero-day threats are four times more likely to compromise organizations<sup>4</sup>.

Even when customers have the advanced security tools they need, they do not always have the expertise or capacity to deploy and manage them effectively. One recent report indicates an estimated shortage of 3.5 million cybersecurity experts worldwide<sup>5</sup> with 53% of companies reporting a shortage of cybersecurity skills<sup>6</sup>.

Many medium-sized organizations lack not just the expertise, but the budget to staff, train and deploy advanced protection solutions. Addressing the needs for endpoint security is now a major focus for IT.

Right-sized for medium businesses, HP Proactive Security is a smarter solution for endpoint security.

## Q: Why should I consider purchasing this service?

**A:** This service helps defend against cyberattacks without changing user behavior or increasing IT's workload. HP Proactive Security, is a managed security solution that provides proactive protection, reduces your risk, and gives users the freedom to work from anywhere.

## Q: Who can benefit from HP Proactive Security?

**A:** HP Proactive Security offers security capabilities for new and existing customers and was specifically developed for medium-sized organizations who desire to improve their endpoint protection position but lack sufficient, in-house security expertise and/or available administrative bandwidth to manage such solutions.

---

<sup>1</sup> HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements, please visit [www.hpdaas.com/requirements](http://www.hpdaas.com/requirements).

<sup>2</sup> AV-TEST Institute - <https://www.av-test.org/en/statistics/malware/>

<sup>3</sup> Ponemon Institute 2018 State of Endpoint Security Risk sponsored by Barkly, October 2018

<sup>4</sup> 2018 Data Breach Investigations report 11th Edition, Verizon

<sup>5</sup> <https://cybersecurityventures.com/jobs>

<sup>6</sup> ESG Global IT Survey 2018-2019 <https://www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse>



# HP Proactive Security FAQ for Customers

**Q: What plan options are available?**

**A:** HP Proactive Security is available in a single plan that includes the isolation software and deep learning endpoint protection and provides access to security analytics and reports via the HP analytics dashboard. The plan also includes a managed service from HP with specialized cybersecurity experts to configure policies and monitor endpoint protection and to analyze threats for Windows 10, macOS and Android devices to help you strengthen your security position. *For full system requirements, please visit [www.hpdaas.com/requirements](http://www.hpdaas.com/requirements).*

**Q: What does HP Proactive Security include?**

**A:** The table below summarizes the HP Proactive Security features.

## HP Proactive Security features

<p><b>Advanced deep learning anti-malware protection</b></p> <ul style="list-style-type: none"> <li>• Detection of both known and previously unseen threats</li> <li>• Static malware files and file-less threats protection</li> <li>• Cloud-based reputation analysis of files</li> <li>• Detects malware evasion techniques</li> <li>• No signature updates required</li> <li>• Multi-OS coverage for Windows 10, macOS® and Android™</li> </ul>	<p><b>Real-time threat isolation protection</b></p> <ul style="list-style-type: none"> <li>• Email attachment isolation</li> <li>• Chat link and file sharing protection</li> <li>• Protection from documents sent by phishing emails</li> <li>• File download protection</li> <li>• Corporate website whitelisting support for IT</li> </ul>
<p><b>Security analytics and reporting through HP TechPulse</b></p> <ul style="list-style-type: none"> <li>• Protection status and gap by length of time</li> <li>• Most impacted devices and users by prevented threats</li> <li>• Threats by type, source and over time</li> </ul>	<p><b>HP managed service</b></p> <ul style="list-style-type: none"> <li>• Analysis of threats by Security Experts</li> <li>• Detailed malware kill-chain analysis</li> <li>• Monitoring of isolation protection on endpoints</li> <li>• APIs for SIEM integration</li> </ul>

**Q: What security analytics and reporting are available via HP TechPulse<sup>7</sup> through this service?**

**A:** Through the HP TechPulse dashboard, HP Proactive Security customers have access to several security-related reports. These reports are designed to show the endpoint protection state for Sure Click Advanced, Sure Sense Advanced, Sure Recover and Sure Start, as well as reports on whether traditional endpoint antivirus is active on managed Windows PCs.

**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 Proactive Security work?**

**A:** An Onboarding Program Manager (OPM) contacts the customer via email to provide a Welcome kit and kickoff the onboarding process. This service does require the customer to install the appropriate software agents to devices covered by the plan.

For larger customer with more complex environment, the HP Proactive Security Enhanced Onboarding service provides a managed service to integrate HP Proactive Security into the customer's overall security stack. Enhanced Onboarding delivers design and deployment services along with policy setting and custom configuration.

<sup>7</sup> HP does not track or monitor details that identify which URLs a user visited. The reporting focuses on identifying threats and their source in HP TechPulse. HP TechPulse is GDPR and ISO 27001 compliant.



# HP Proactive Security FAQ for Customers

**Q: How is HP Proactive Security priced?**

**A:** HP Proactive Security pricing is on a per device per month basis. Contact a services sales specialist for details.

**Q: In what countries is it available?**

**A:** HP Proactive Security is a worldwide offer available globally in English. The Aon components are available in the U.S. only with additional countries being added over time.<sup>8</sup>

**Q: Organization security information is very sensitive. Are the HP Service Experts under NDA for organizations they serve?**

**A:** Yes, HP Service Experts are under NDA and do not share sensitive security or privacy information. In addition, HP has achieved ISO27001 certification to ensure that rigorous end-to-end processes and controls are in place to protect customer data.

**Q: What tasks do the HP Service Experts perform?**

**A:** HP Service Experts manage and monitor the threat isolation protection that comes with HP 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: How does the HP Service Team analyze and investigate threats and add value for customers? What type of expertise do they apply in addition to monitoring and administering?**

**A:** The HP Security Expert teams manage the threat isolation protection that comes with HP Proactive Security. These highly trained experts:

- Monitor client protection status and notify the customer with reports and other details whenever protection has been disabled on a device.
- When threats are blocked by HP Sure Click Advanced, perform deeper analysis and identification of NEW malware using kill chain assessment tools. Such analysis can ensure the customer has a clear view of the nature of a threat and the application it targeted.
- When threats are blocked by Sure Sense Advanced or Sure Click Advanced, notify the customer so the customer can respond as needed, or update HP on whether additional action on an identified threat, such as release from quarantine, is needed.

These alerts, deep investigation of and notification about highly malicious events provide valuable insights that enable customers to further improve their defenses against attack. Based on the findings, customers can make more informed decisions on content trust settings, conduct targeted training of end users and adapt company policies to protect their devices, data and identities.

Note that the Sure Click “zero-day” threat analysis by HP Service Experts is a deep forensic investigation process that triggers after a malware event has been blocked or isolated by the agent. It is not a “real-time,” 24/7 monitoring service. The HP Sure Click Advanced client agent automatically isolates untrusted or malicious content, ensuring protection before the analysis. Also, the plan does not include remediation or mitigation services in the event of a breach. Mitigation and remediation services are available as a separate service from HP partners including Aon.

---

<sup>8</sup> Available in the U.S. and select countries in Europe. Purchasers of the HP DaaS Proactive Security Service in the U.S receive the Aon CyQu self-assessment and security score. \$0 retainer and one-hour free consultation included with optional incident response services from Aon. HP onboarding service representatives will provide instructions.



# HP Proactive Security FAQ for Customers

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

**A:** This service is not a replacement for signature-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 polymorphic malware and zero-day attacks. However, in some cases, customers may find it more economical to replace their existing antivirus solution with a combination of Microsoft's free Defender product, backed by HP Proactive Security artificial Intelligence (AI) and isolation technology. These additional layers provide a powerful last line of defense against device-level and application-level attacks.

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

**A:** HP provides a multi-layered approach, focused on AI-based detection of malware, backed by proactive isolation and containment, rather than signature-based detection of known threats.

The deep learning engine of HP Sure Sense Advanced has been trained to recognize and distinguish malware from harmless files, with an advanced neural network trained against literally hundreds of millions of known malware samples. This training enables the engine to automatically recognize both known, and previously-unseen, malware types, which enables it to continuously adapt to new threats, without signature updates, and with a low rate of false positives.

In addition, since the most frequent source of attacks against end user PCs occurs through downloads from malicious websites, email attachments and infected links, HP Sure Click Advanced will open untrusted content 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. It also allows the behavior of the content to be monitored for suspicious behavior. Because documents and browser tabs are opened in isolation, even zero-day threats are contained.

Best of all, these containers are created automatically 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 and deep learning technologies:

- 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: 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 and Aon have a strategic collaboration to deliver complete security solutions to HP Proactive Security customers in the U.S. HP provides endpoint security as a service and Aon provides security



# HP Proactive Security FAQ for Customers

assessment, response, and insurance services. Together, we deliver end-to-end solutions for customers.

The first step in ensuring a strong security position and plan is to know where you stand, HP Proactive Security customers in the U.S. can take advantage of the Aon Cyber Quotient Evaluation (CyQu), a powerful cybersecurity resilience assessment tool. The CyQu assessment tool delivers a security scorecard with industry benchmarking so customers better understand their security profile.

In addition, customers of HP Proactive Security are eligible for a \$0 Incident Response (IR) retainer from Aon to have mitigation experts standing by to reduce the impact of any breach. This offer includes one hour of consultation if a breach occurs.

Finally, customers may also be eligible for security breach insurance policies through Aon. HP customers are eligible for enhanced cyber insurance, based on the superior level of security afforded to businesses with HP Proactive Security.

**Note:** *Insurance is a highly regulated industry, so HP and our partners cannot directly participate in any direct marketing, sales, or consultative services regarding insurance plans or policies.*

## System Requirements

**Q:** What operating systems and hardware does HP Proactive Security support?

**A:** HP Proactive Security supports the following Operating Systems. Please note that HP Sure Click Advanced protection is not available on MacOS and Android devices.

Platform	OS Requirements	Hardware Requirements <sup>9</sup>
Windows	Most current generally available Windows 10 OS release, or two previous major releases	HP Sure Click Advanced <sup>10,11</sup> <ul style="list-style-type: none"> <li>Intel Core i3, i5, i7 (or a modern AMD CPU) with Virtualization Technology enabled in the BIOS/UEFI</li> <li>At least 4 GB of RAM (8GB recommended)</li> <li>At least 6 GB of free disk space</li> </ul> HP Sure Sense Advanced <ul style="list-style-type: none"> <li>At least 4 GB of RAM</li> </ul>
MacOS	MacOS 10.12 or higher	HP Sure Click Advanced <ul style="list-style-type: none"> <li>Not Supported on MacOS devices</li> </ul> HP Sure Sense Advanced <ul style="list-style-type: none"> <li>No special hardware requirements on MacOS</li> </ul>
Android	Android v5.0 or higher	HP Sure Click Advanced <ul style="list-style-type: none"> <li>Not Supported on Android devices</li> </ul> HP Sure Sense Advanced <ul style="list-style-type: none"> <li>No special hardware requirements on Android</li> </ul>

To access the company dashboard, security reports and other data hosted on the TechPulse platform, a customer's device also needs to meet the system requirements listed at <https://www.hpdaas.com/requirements>.

<sup>9</sup> Customer can deploy partial technology (HP Sure Sense Advanced or Hp Sure Click Advanced) if system doesn't meet the minimum requirements.

<sup>10</sup> For a complete listing of Windows 10 supported versions, please refer to the [Premium Windows Support Policy](#). Note that Windows 7 and 8.1 are not supported by HP Proactive Security.

<sup>11</sup> HP Sure Click Advanced cannot be installed for Simplified Chinese languages.



## For More Information

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

A: For more information, visit: [www.hp.com/proactive-security](http://www.hp.com/proactive-security).

---

Copyright 2020, 2019 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA7-4572ENW v3 - March 192020