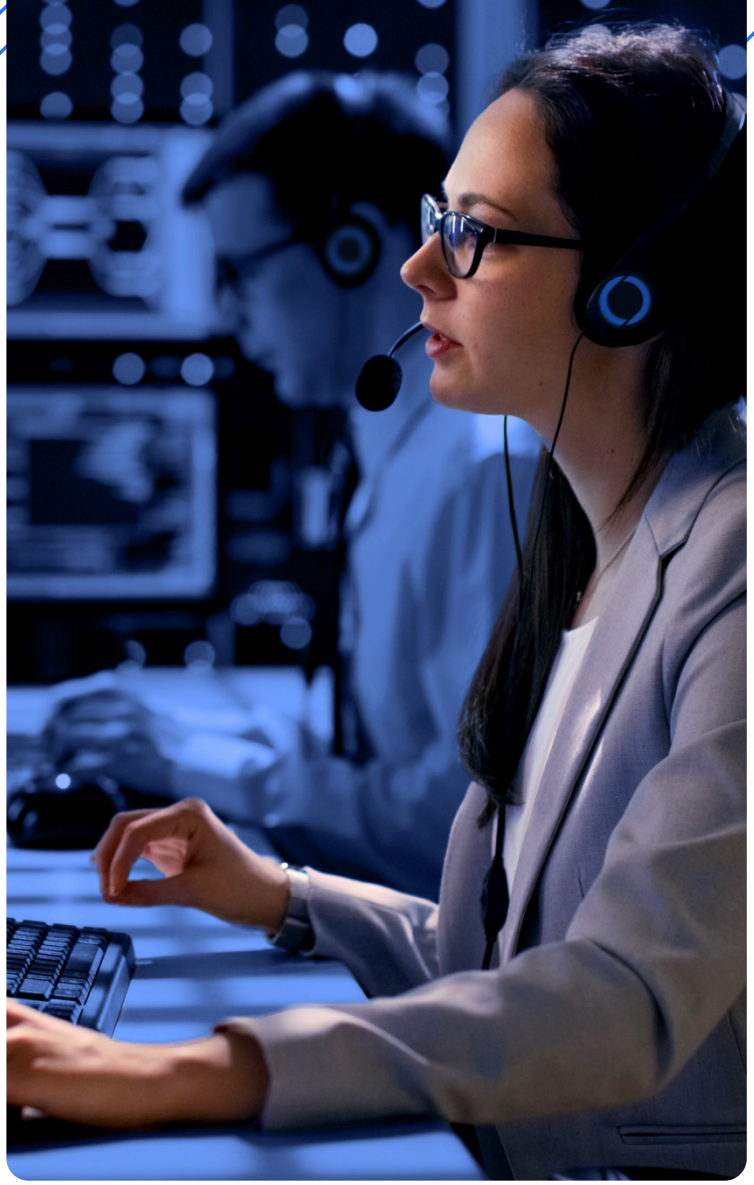
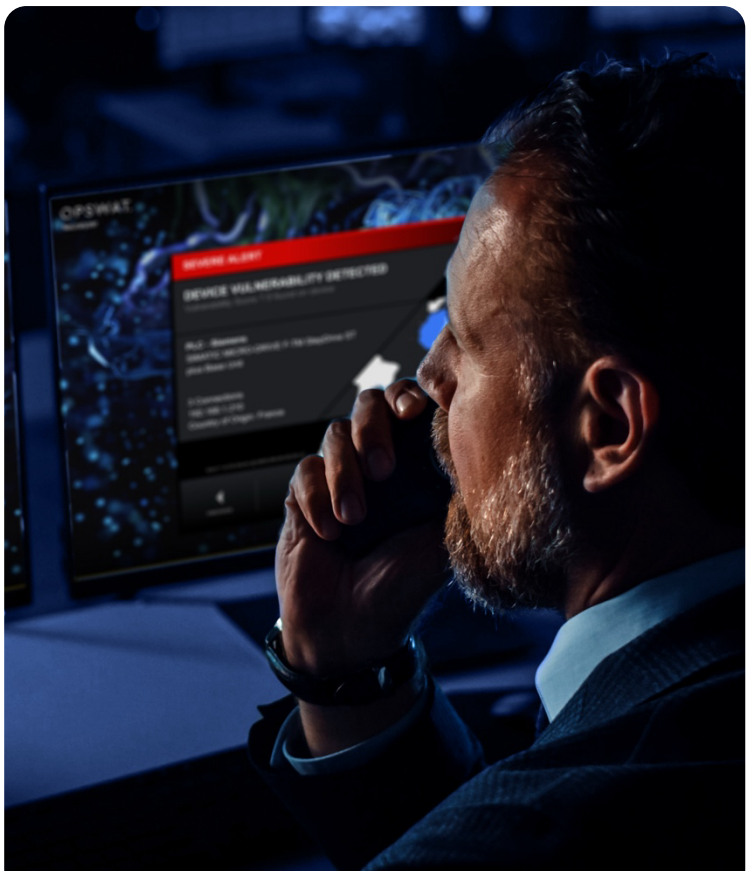
OPSWAT.



SUPPORT PROCESS AND ESCALATION PROTOCOLS



OPSWAT SUPPORT

Introduction

Navigating the intricacies of modern cybersecurity solutions demands a responsive and reliable support system powered by a team of experts. That's why we've meticulously designed a comprehensive support process to ensure that our customers receive prompt assistance and resolution to any challenge they encounter. OPSWAT's support process is built upon a foundation of expertise, efficiency, and empathy. Our team of dedicated support professionals possesses unrivaled knowledge of our products, coupled with a commitment to delivering exceptional customer service.

Whether it is troubleshooting technical issues, providing product guidance, or assisting with implementation, our support team is equipped with the tools and expertise to deliver tailored solutions that meet the unique needs of each client

Table of Contents

01 Support Communication Channels

02 OPSWAT Support Team

03 Initial Triage and Assessment

04 Severity Definitions

05 Incident Management Service Level Agreements (SLAs)

06 Service Level Agreement Tables

07 Requesting Issue Escalation

08 Support Escalation Workflow

09 Requesting Support for Specific Planned Activities

10 Root Cause Analysis Feedback

11 On-Site Support

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

01 Support Communication Channels

OPSWAT Support offers a diverse range of assistance options, including:

Case Management	Support requests via tickets through My OPSWAT
Chat	Via AI chatbot and live agent chat on My OPSWAT
Phone	For premium customers, with dedicated support phone numbers located in multiple countries, including Australia, France, Hungary, Israel, Japan, Romania, Spain, UAE, UK, and USA

Additionally, we provide self-service support through a chatbot, robust knowledge center, and active community forums. These resources empower users to find solutions independently while our expert team remains readily available for personalized assistance when needed.

See opswat.com/support for details

Note:
Using any of our support communication channels results in a support transaction record filed our case management system, which lets us properly track all of our customers' issues. For this reason, we do not accept email as a support communication channel.

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

02 OPSWAT Support Team

At OPSWAT, our strategically located support offices across Asia, Europe, and America are designed to provide exceptional, round-the-clock global support through an efficient follow-the-sun model. Here's how our approach ensures seamless customer experiences:

Regional Focus and Expertise:

Each region is managed by a dedicated Director of Support, responsible for overseeing operations and addressing customer queries and concerns originating within their respective areas. Teams are staffed with experts who understand the unique requirements and nuances of their regional customers.

Follow-the-Sun Support Model:

Our global offices operate on a follow-the-sun model, ensuring that customer inquiries are handled promptly, regardless of the time zone. Each regional team takes full ownership during their shift, providing dedicated support tailored to the region's needs.

Seamless Knowledge Transfer:

Ample overlap time between shifts ensures smooth transitions and uninterrupted service. Critical knowledge transfer processes are in place to maintain continuity and efficiency in issue resolution as operations shift from one region to another.

Unified Global Tiered Support Framework:

Our support model is structured into three tiers, ensuring sufficient issue resolution and seamless collaboration across regional teams. Each tier provides a defined level of expertise and escalation delivering consistent service quality and a cohesive customer experience worldwide.

Customer-Centric Communication:

Our Support leadership welcomes direct communication from customers, particularly when it can expedite issue resolution or enhance satisfaction.

We value customer feedback and are committed to resolving concerns effectively and efficiently.

By combining regional expertise, a robust operational model, and a customer-first approach, OPSWAT continues to deliver world-class support that meets and exceeds customer expectations.

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

Note
For customers with support entitlements that restrict access to specific geographic regions, only support personnel within the designated region will have visibility and provide coverage. Support teams and managers outside of that region will not be involved or have access to these cases.

Support Leadership Team

Role	Name	Email	Location
Senior Vice President of Customer Experience	Dan Lanir	supportescalation_svp@opswat.com	San Francisco, California, USA
Vice President of Global Technical Services	Nith Mehta	supportescalation_vp@opswat.com	Bangalore, India
Senior Support Duty Manager Europe, Middle East, Africa	Razvan Chilu	supportescalation_emea@opswat.com	Timisoara, Romania
Support Duty Manager America	Tien Tran	supportescalation_amer@opswat.com	Tampa, FL, USA
Support Duty Manager Asia, Pacific, Japan	Dung Nguyen	supportescalation_apj@opswat.com	Ho Chi Minh City, Vietnam

Note
Up-to-date contact information for your regional Support Duty Manager and your CSM or TAM (if applicable) is available to you in your My OPSWAT portal -> Support Services page.

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

03 Initial Triage and Assessment

When a customer submits a support request—or when one is created following a chat or phone call—our team conducts an initial triage to ensure prompt and effective resolution. The speed of response is determined by several key factors:

Issue Complexity:

The intricacy of the problem, including technical depth and diagnostic requirements, is assessed to determine the appropriate level of expertise needed.

Severity Level:

Issues are evaluated based on their impact on the customer's operations, ranging from minor inconveniences to critical business disruptions. The Severity levels are described in Section 3 of this document.

Prioritization:

Cases are prioritized to ensure that the most urgent and impactful issues are addressed first.

Resource Allocation:

Based on the nature of the issue, the appropriate support resources are assigned. This may include collaboration with specialized teams such as Cloud Ops, DevOps, Engineering, or Sales.

Support Entitlement:

The customer's support plan and entitlements influence how the case will be managed and the specific SLAs applied.

SLA-Driven Response Times:

The results of the assessment guide the expected response times, ensuring alignment with the customer's service-level agreement (SLA).

This structured approach ensures that every support request is addressed efficiently, with the right resources and response time tailored to the customer's needs.

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

04 Severity Definitions

OPSWAT's support SLAs are based on severity of the issue, using a scale from 1 to 4 based on the following criteria:

Severity Level	
1	An existing network or environment is down or there is a critical impact to your business operation. OPSWAT will commit resources during OPSWAT business hours and use reasonably diligent efforts to provide a workaround and/or resolve the situation.
2	Operation of your existing network or environment is severely degraded or significant aspects of your business operations are negatively impacted by unacceptable network or environment performance. OPSWAT will commit resources during OPSWAT business hours and use reasonably diligent efforts to provide a workaround and/or resolve the situation.
3	Although most business operations remain functional and/or a security application or security application state is not properly detected and/or remediated and is negatively affecting most of your personnel. OPSWAT will commit resources during OPSWAT business hours to restore service to satisfactory levels.
4	You require information or assistance on software capabilities, installation, or configuration and/or a security application or security application state is not properly detected and/or remediated. OPSWAT will provide resources during OPSWAT business hours to provide information or assistance as requested.

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

05 Incident Management Service Level Agreements (SLAs)

OPSWAT provides SLAs for three critical phases of an incident case:

First Response	We commit to acknowledging receipt of the escalation within a specified timeframe, ensuring that customers receive prompt acknowledgment of their requests.
Ongoing Diagnosis Update	We aim to complete a thorough diagnosis of the issue, providing customers with clear insights into the root cause of the problem and potential solutions. During this phase, we provide regular updates within a specified timeframe to keep customers informed of progress.
Fix Release	Once a solution is identified and implemented, we commit to releasing the fix within an agreed-upon timeframe, minimizing downtime and disruptions for our customers.

The actual SLA timeframes on each of these phases are dependent on the severity of the incident issue as well as the support entitlement of the customer. Tables with specific time frames are provided in the last section of this document.

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

06 Service Level Agreement Tables

SLAs are based on the support entitlement of the customer as well as the severity of the incident issue.

Platinum and Emerald Support

Security Level	First Response	Ongoing Diagnosis Update	Fix Release
1	1 hour	2 hours unless otherwise agreed	Once every 2 hours. until hotfix is released unless customer accepts the next estimated release date without need for further status updates
2	1 hour	1 business days unless otherwise agreed until fix is identified and estimated release date is provided	Within 1 business day of determination that: • a fix version release has been rescheduled, or • a fix needs to be removed from the originally assigned release
3	4 hours	1 business days unless otherwise agreed until fix is identified and estimated release date is provided	Within 2 business days of determination that: • a fix version release has been rescheduled, or • a fix needs to be removed from the originally assigned release
4	4 hours	1 business days unless otherwise agreed until fix is identified and estimated release date is provided	Within 3 business days of determination that: • a fix version release has been rescheduled, or • a fix needs to be removed from the originally assigned release

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

Gold Support

Security Level	First Response	Ongoing Responses During Diagnostics Phase	Ongoing Responses During Solution Release Phase
1	2 hours during OPSWAT business hours	8 hours unless otherwise agreed	Once every 1 business day until hotfix is released unless the customer accepts the next estimated release date without need for further status updates
2	2 hours	8 hours unless otherwise agreed until fix is identified and estimated release date is provided	Within 2 business days of determination that: • a fix version release has been rescheduled; or • a fix needs to be removed from the originally assigned release
3	8 hours	1 business days unless otherwise agreed until fix is identified and estimated release date is provided	Within 2 business days of determination that: • a fix version release has been rescheduled; or • a fix needs to be removed from the originally assigned release
4	8 hours	1 business days unless otherwise agreed until fix is identified and estimated release date is provided	Within 3 business days of determination that: • a fix version release has been rescheduled; or • a fix needs to be removed from the originally assigned release

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

Silver Support

Security Level	First Response	Ongoing Responses During Diagnostics Phase	Ongoing Responses During Solution Release Phase
1	4 hours during OPSWAT business hours	12 business hours unless otherwise agreed	Once every 1 business day until hotfix is released unless the customer accepts the next estimated release date without need for further status updates
2	4 hours	12 business hours unless otherwise agreed until fix is identified and estimated release date is provided	Within 2 business days of determination that: • a fix version release has been rescheduled; or • a fix needs to be removed from the originally assigned release
3	1 business day	1 business days unless otherwise agreed until fix is identified and estimated release date is provided	Within 2 business days of determination that: • a fix version release has been rescheduled; or • a fix needs to be removed from the originally assigned release
4	1 business day	1 business day unless otherwise agreed until fix is identified and estimated release date is provided	Within 3 business days of determination that: • a fix version release has been rescheduled; or • a fix needs to be removed from the originally assigned release

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

07 Requesting Issue Escalation

We recognize that some issues may require additional attention and resources beyond initial support interactions. To ensure timely resolution and customer satisfaction, we have established a robust support escalation process designed to efficiently address complex or critical issues that may arise.

The following list describes steps our customers should take to request escalation:

1. Customers can update their case with specific escalation requests, such as a request to have a video conference, change the severity level of the case, speak to a Duty Manager or Director of support, etc.

2. Customers can simply press the `Escalate to Management` button on their case and then optionally provide additional information in the text window that pops up. A Customer Experience Coordinator or a Duty Manager will respond within two business hours.

3. Customers that have phone support as part of their support entitlement (e.g. Emerald, Platinum, Gold) can call an OPSWAT Support line with specific escalation requests, including having a Duty Manager or Director of Support reach out to them. The Duty Manager will respond within two business hours.

4. If the above escalation steps have still not proven sufficient, customers can contact our regional support leaders as well as our Vice President of Technical Services and Senior Vice President of Customer Experience. (See OPSWAT Support Team below). The person you contact will respond within two business hours.

For each step above, the escalation point person will contact the customer, provide their contact information, discuss action plan and next steps with the customer, discuss which other parties need to be involved (e.g. does an OPSWAT Engineer need to get directly involved), and take ownership of the issue until the issue is resolved or the customer is comfortable with the progress of the issue.

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

08 Support Escalation Workflow

Throughout the escalation process, we continuously monitor the status of the issue and gather feedback from the customer to ensure their needs are being met effectively. Regular communication and updates are provided to keep the customer informed and engaged.

	Customer Action	OPSWAT Response to Customer	OPSWAT Internal Action
Case Creation Cases get created in My OPSWAT and are converted from phone calls and chat	**Start** Create incident case	Case owner reviews priority, begins issue resolution related work	Sales and CSM/TAMs are informed customer has opened a case
Escalation Path OPSWAT's goal is for our customers to get their desired outcome without needing to continue escalating along the ladder. OPSWAT's Support Engineers are trained to react to an escalation at each rung of the ladder with that goal in mind. However, if a customer feels they are not getting the support they need, we encourage them to continue to escalate so that we can take the appropriate corrective action.	**1st Escalation** Escalate via a case update with details of the escalation request. Specify if the severity level needs to be updated	Case Owner updates the case with customer's requests, informs support manager, reaches out to customer to get additional information and elevate case handling **SLA:** same as SLA on the severity of the case	Escalation to other groups working on issues (e.g.: Cloud Ops, Dev Ops, Engineering, Product). Alert to regional Support Duty Manager and CSM/TAM if applicable
	2nd Escalation From within the case, click on the `Escalate to Management` button	CX Coordinator or Duty Manager contacts customer to get info needed to properly elevate case handling, informs case owner, informs Support Duty Managers. They take ownership of the case until customer is comfortable with progress **SLA:** 2 hours	Escalation to other groups working on issue (e.g.: Cloud Ops, Dev Ops, Engineering, Product). Alert to all Support Duty Managers and CSM/TAM if applicable
	3rd Escalation Call the OPSWAT support phone line to request the on-shift Support Duty Manager	Duty Manager works with the customer to elevate case handling and determine how previous escalations failed them. Support Leadership team take ownership of the case until customer is comfortable with progress. **SLA:** same as SLA on the severity of the case	Escalation to leaders of other groups working on issue (examples above). Alert to all Support Duty Managers, CSM/TAM if applicable, Services VP, Regional Sales Manager
	4th Escalation Email the Support Leadership team to request further escalation	Duty Manager, Services VP, and CSM/TAM work with customer to get adjust case handling, provide root cause analysis of why issue needed to be escalated four times. **SLA:** 2 hours.	Escalation to leaders of other groups working on issue (examples above). Alert to all Duty Managers, SVP of CX, Sales VP, Chief Product Officer

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01

09 Requesting Support for Specific Planned Activities

OPSWAT Support is dedicated to accommodating our customers for their scheduled activities, such as installations or upgrades scheduled for a specified maintenance window.

To ensure the right level of support during the planned activity, the customer should log a support case with OPSWAT as early as possible and provide information on the time of the activity, the purpose of the activity, pertinent considerations and constraints, plus any specific user contact information, required video sharing application (e.g. Teams, Zoom, Google Meeting, etc.). An OPSWAT Support agent will confirm the request and ensure readiness from the OPSWAT Support team.

10 Root Cause Analysis Feedback

OPSWAT is dedicated to resolving Severity 1 issues promptly and thoroughly. Upon customer request, OPSWAT can provide a root cause analysis document, typically within one week of the resolution of the issue. This document will be based on our internal root cause analysis, which we perform to identify underlying causes, provide actionable feedback, and implement necessary improvements swiftly. By prioritizing timely and effective solutions, we ensure minimal disruption and maximum satisfaction for our customers.

11 On-Site Support

For customers unable to receive remote support, OPSWAT offers on-site support services for additional fees and charges. With pre-approval from the customer, our expert technicians can provide personalized assistance directly at the customer's location. This ensures a seamless support experience and timely resolution of issues, meeting the unique needs of every customer with professionalism and efficiency.

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaDefender, MetaScan, MetaAccess, the OPSWAT Logo, Trust no File. Trust No Device., OPSWAT Academy, Protecting the World's Critical Infrastructure, Deep CDR, InQuest, the InQuest Logo, DFI, RetroHunt, Deep File Inspection, and Join the Hunt are trademarks of OPSWAT Inc. Third party trademarks are the property of their respective owners. Rev. 2025-01