Implementation Services

Expert-led deployment of OPSWAT solutions — engineered to maximize time-to-value, minimize deployment risk, and ensure your critical infrastructure protection is operational from day one.

The Challenge

Selecting Deploying enterprise-grade security platforms across complex environments — especially OT and critical infrastructure — is rarely straightforward. Misconfigured policies, incomplete integrations, and gaps in stakeholder alignment can leave deployments under-utilized for months after go-live, eroding the value of the underlying product investment. In-house teams frequently have the skills but lack the bandwidth or product-specific depth to execute a structured rollout. OPSWAT Implementation Services closes that gap by embedding OPSWAT-certified engineers who own the technical execution end-to-end, ensuring your platform reaches production state quickly and predictably.

What is OPSWAT Implementation Services?

OPSWAT Implementation Services is an expert-led engagement that designs, deploys, and operationalizes your OPSWAT solutions — delivered onsite or remotely to match the operational profile of your environment. Our engineers handle architecture, configuration, integration, validation, and knowledge transfer, ensuring the platform is production-ready, fully aligned with your security objectives, and confidently adopted by the teams that depend on it.

What's Included

Every Implementation Services engagement delivers a structured set of technical and operational deliverables:

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

- Deployment of OPSWAT hardware and software components, sized and architected for your environment
- Configuration of policies, threat detection rules, and remediation actions aligned to your security objectives
- Integration with third-party IT tools, Active Directory, SIEM, and API-driven workflows
- Testing, validation, and user acceptance testing with key stakeholders
- Knowledge transfer sessions and deployment architecture documentation
- Structured project delivery with formal sign-off at each phase gate
- Post-deployment fine-tuning and operational handover to your internal teams

Service Packages

Choose the engagement model that matches your environment, security posture, and access constraints. Both packages are delivered by OPSWAT- Professional Services engineers following the same structured methodology - and every engagement concludes with final design documentation and a formal operational handover to your internal teams.

Implementation Services — Onsite

Engineer-led deployment delivered directly at your facility, ideal for air-gapped environments, OT and critical infrastructure sites, and complex network topologies.

- Onsite OPSWAT stack deployment (hardware, firmware, software), network configuration, and physical integrationHands-on collaboration with on-premise stakeholders and security operations teams
- Direct integration with air-gapped and OT environments, supported by MetaDefender data diodes where required
- Onsite testing, validation, and user acceptance walkthroughs
- In-person workshops, runbook walkthroughs, and operational handover
- Final design documentation delivered at engagement close

Implementation Services — Remote

Fully remote engagement for IT-accessible environments where deployment can be executed without onsite presence — streamlined for distributed teams and standardized rollouts.

- Remote deployment via Teams or other Video Conf tools
- Architecture design, policy configuration, and integration with your existing security stack
- Integration with Active Directory, SIEM, and API workflows
- Virtual validation testing and stakeholder review sessions
- Virtual workshops and documented knowledge transfer

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

Why OPSWAT-Led Implementation?

Stop absorbing deployment risk into your in-house teams. OPSWAT-certified Professional Services engineers bring product-native expertise, structured methodology, and proven playbooks — transforming a complex security rollout into a predictable, milestone-driven engagement.

Product-Native Expertise

Engineers trained, certified, and aligned to OPSWAT product roadmaps deliver configurations that reflect vendor best practices from day one — not a generalist interpretation of the documentation.

Faster Time-to-Value

Structured project delivery with parallel workstreams compresses deployment timelines and accelerates your path to operational coverage of your critical assets.

Risk-Managed Rollout

Proven deployment patterns reduce the likelihood of misconfiguration, integration gaps, and post-launch surprises that erode security ROI, drain team productivity and trigger costly rework.

Documented and Sustainable

Every engagement leaves behind architecture documentation, operational runbooks, and trained stakeholders — equipping your team to confidently operate the platform after handover.

Pillars of Implementation Services

Every engagement progresses through five documented phases, grouped under Initiation, Execution, and Closure, with formal stakeholder sign-off at each gate.

1. Assessment & Planning (Initiation)

Identify customer use cases, evaluate IT/security infrastructure compatibility, define deployment architecture, assess compliance needs, and develop a tailored implementation roadmap.

2. Installation & Configuration (Execution)

Deploy OPSWAT hardware and software, configure policies, threat detection, and remediation actions, implement authentication and access controls, and validate network and endpoint connectivity.

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

3. Integration & Customization (Execution)

Integrate with other OPSWAT products and third-party IT tools, connect Active Directory and identity providers, and build out API-driven workflows.

4. Testing & Validation (Execution)

Functional testing of policy enforcement and threat detection, user acceptance testing with stakeholders, performance optimization, and validation of compliance and regulatory standards.

5. Knowledge Transfer (Closure)

Document the deployment architecture, capture key findings and recommendations, train stakeholders to operate and troubleshoot the product, and align them with OPSWAT ongoing support.

Get Started

To scope an OPSWAT Implementation Services engagement for your environment, contact your OPSWAT representative or visit: www.opswat.com

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.