# 

**Technical proposal**

Prepared by: Ziad Haddad

OPSWAT Inc.

A picture containing text, outdoor

Description automatically generatedTable of Contents

United Arab Emirates

This proposal is prepared for:

Emirates Nuclear Energy Corporation (ENEC)

[0](#_Toc150950505)

[Table of Contents 0](#_Toc150950506)

[Executive Summary 2](#_Toc150950507)

[Company Overview 3](#_Toc150950508)

[Industry Leading Cybersecurity Products 3](#_Toc150950509)

[OPSWAT Professional Services and Workforce Development 6](#_Toc150950510)

[Industry Experience 7](#_Toc150950511)

[Recommended Products for ENEC Requirements 8](#_Toc150950512)

[MetaDefender Platform 8](#_Toc150950513)

[MetaDefender ICAP Server 9](#_Toc150950514)

[OPSWAT Central Management 10](#_Toc150950515)

[HLD 11](#_Toc150950516)

[LLD 12](#_Toc150950517)

[OPSWAT Support Plans 13](#_Toc150950518)

Executive Summary

Enterprises are investing more resources than ever in cyber security – and yet there are more and larger breaches every year. Thousands of threat prevention solutions are on the market, but most of them share one crucial flaw: they are based on detection, but detection is never 100% perfect.

Same enterprises face an increasing number of challenges from major attack vectors, including email, BYOD, the Cloud, and web portals. OPSWAT created a platform for preventing and detecting cyber security threats on multiple data channels and devices. The platform is powered by patented technologies and is controlled by a flexible workflow engine to efficiently prevent advanced threats. OPSWAT main use cases include isolated network protection, web and email security, and secure device access.

That's why our advanced threat prevention platform, MetaDefender, is not only based on detection.

MetaDefender uses OPSWAT's unique data sanitization (Content Disarm and Reconstruction) to remove threats from files altogether by reconstructing the files and, in the process, stripping out potentially malicious active content and scripts. MetaDefender complements data sanitization with multi-scanning, vulnerability assessment and data loss prevention (DLP).

MetaDefender is a cyber security platform for preventing and detecting cyber security threats on multiple data channels.

Company Overview

Founded in 2002, OPSWAT is focused on protecting critical infrastructure ([CIP](https://www.opswat.com/critical-infrastructure-protection)). Adhering to Zero Trust philosophy, OPSWAT’s wide range of solutions are designed to eliminate malware and zero-day attacks; provide comprehensive asset discovery and intrusion detection; and provide network security, guarding critical assets against outside threats.

We believe that every file and every device pose a threat, and every network connection needs to be secured. Threats must be addressed at all locations at all times—at entry, at exit, and at rest. Our products focus on threat prevention and process creation for secure data transfer and safe device access. The result is productive systems that minimize risk of compromise.

Over the past 20 years, OPSWAT has experience significant growth and has expanded its portfolio of products and services to meet the needs of our customers. The timeline below illustrates some of the key milestones in OPSWAT’s growth.

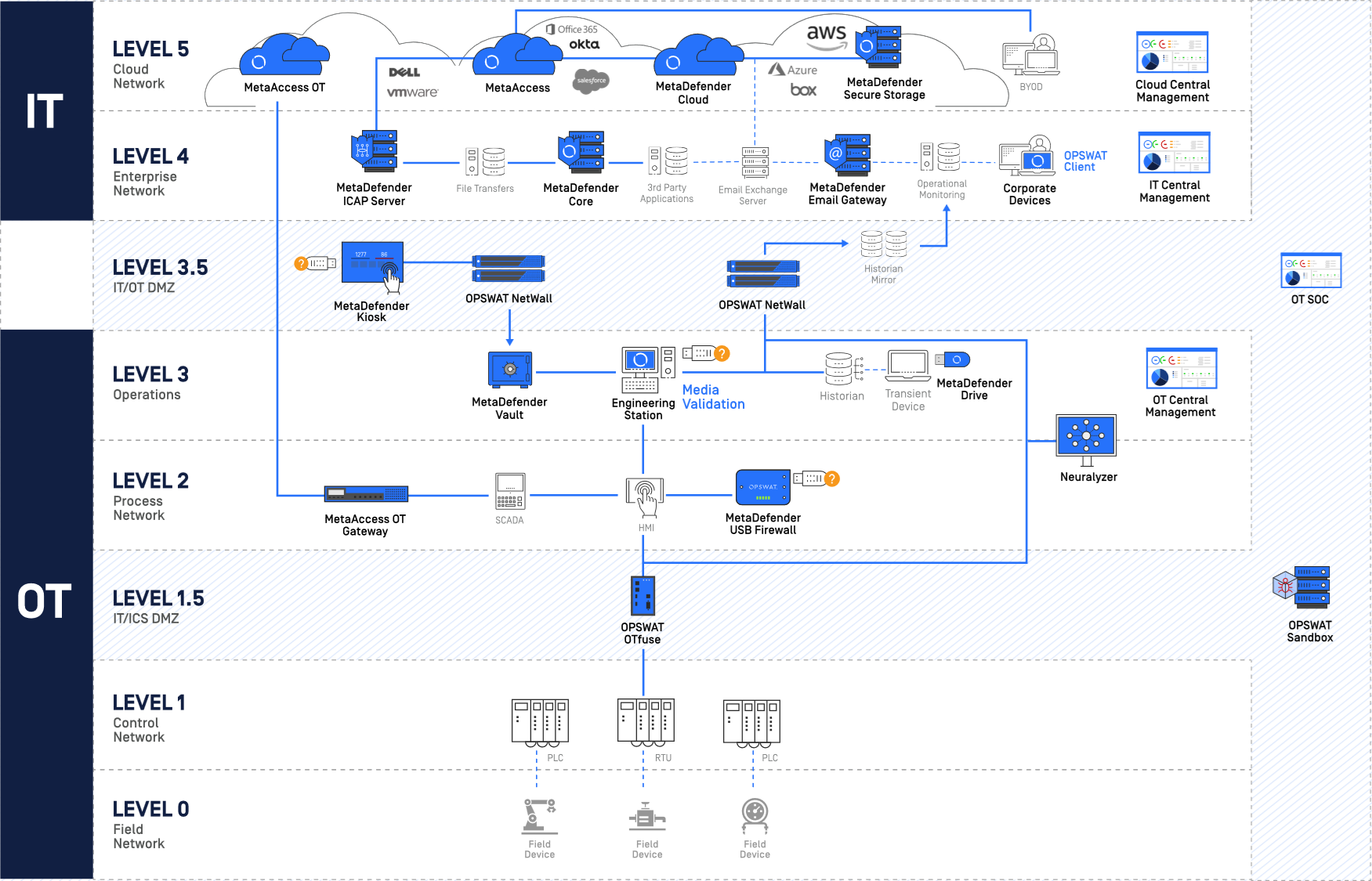
Text

Description automatically generated with low confidence

Supporting over 1500 active customers worldwide, OPSWAT offers a full range of cybersecurity solutions that address the security needs of IT and OT domains as well as securing the communications between IT and OT. The diagram below shows OPSWAT solutions overlaid on the Perdue Model reference architecture.

Industry Leading Cybersecurity Products

To solve the challenges faced by modern industrial and critical infrastructure environments and to shut off major attack vectors, OPSWAT’s product portfolio offers protection against threats at every level of an organization’s infrastructure.



|  |  |
| --- | --- |
| **MetaDefender™ Platform** | **MetaAccess™ Platform** |
| * Enterprises are investing more resources than ever in cybersecurity – and yet there are more and larger breaches every year. Thousands of threat prevention solutions are on the market, but most of them share one crucial flaw: they are based on detection, but detection is never 100% perfect. That's why our advanced threat prevention platform, MetaDefender, is not only based on detection. * MetaDefender uses OPSWAT's unique deep content disarm and reconstruction (Deep CDR) to remove threats from files by reconstructing the files and, in the process, stripping out potentially malicious content and scripts. MetaDefender also offers multiscanning, file-based vulnerability assessment and proactive data loss prevention (Proactive DLP).   [More about MetaDefender](https://www.opswat.com/products/metadefender) | * The move by enterprises to cloud computing, SaaS applications, and bring your own device (BYOD) environments over the last decade has eliminated the traditional network perimeter, making most network access control (NAC) solutions obsolete. * To meet the challenges of modern cloud-based environments and provide administrators with an access control solution for the cloud, we built MetaAccess. * MetaAccess keeps SaaS applications and cloud data safe and secure. It allows access based on device health and compliance to help administrators block risky devices from connecting to sensitive cloud data and SaaS applications.   [More about MetaAccess](https://www.opswat.com/products/metaaccess) |

**Our Cybersecurity Philosophy: Trust no file. Trust no device.**

Our philosophy drives our products and defines our mission. We believe that all files and devices are malicious until they are confirmed otherwise. For that reason, we, “Trust no file. Trust no device.”

This philosophy is a cybersecurity approach that emphasizes the importance of assuming all files and devices as potential threats, regardless of their source or reputation. This philosophy helps to proactively safeguard digital assets and reduce the risk of cyberattacks and is rooted in the following key principles:

Assume All Files Are Malicious

Treat every file, whether it is from a known or unknown source, as potentially harmful until proven otherwise. This approach encourages the use of robust security measures, such as multi-scanning, content disarm and reconstruction (CDR), and data sanitization, to verify and neutralize threats.

Assume All Devices Are Compromised

Consider every device connecting to the network, including personal and company-owned devices, as potentially infected or compromised. Implement stringent access controls, endpoint security solutions, and continuous monitoring to detect and respond to threats.

Zero Trust

Embrace a “Zero Trust” approach, which involves continuous verification and validation of users, devices, and applications in a network. This model requires the implementation of security measures such as multi-factor authentication (MFA), least-privilege access, and micro-segmentation.

Defense In Depth

Adopt a multi-layered security strategy that uses various tools and technologies to provide protection at different levels, including network, endpoint, application, and data. This approach ensures that even if one layer of defense is breached, other layers remain intact to minimize the impact of an attack.

OPSWAT Professional Services and Workforce Development

OPSWAT backs our solutions with excellent support and professional services. OPSWAT resources are strategically located across the global. We offer a full range of support and professional services to ensure our customer’s complete satisfaction. OPSWAT installed base of products are protected with global 24x7 support to rapidly address issues and we provide professional services to expedite product implementation and training. We also provide cybersecurity training for our customers through OPSWAT Academy, which helps build our customers security expertise.

**OPSWAT Academy**

There's no better way to learn the cybersecurity that protects our way of life than with OPSWAT Academy, because when it comes to critical infrastructure protection training and certification, we wrote the book.

Text, letter

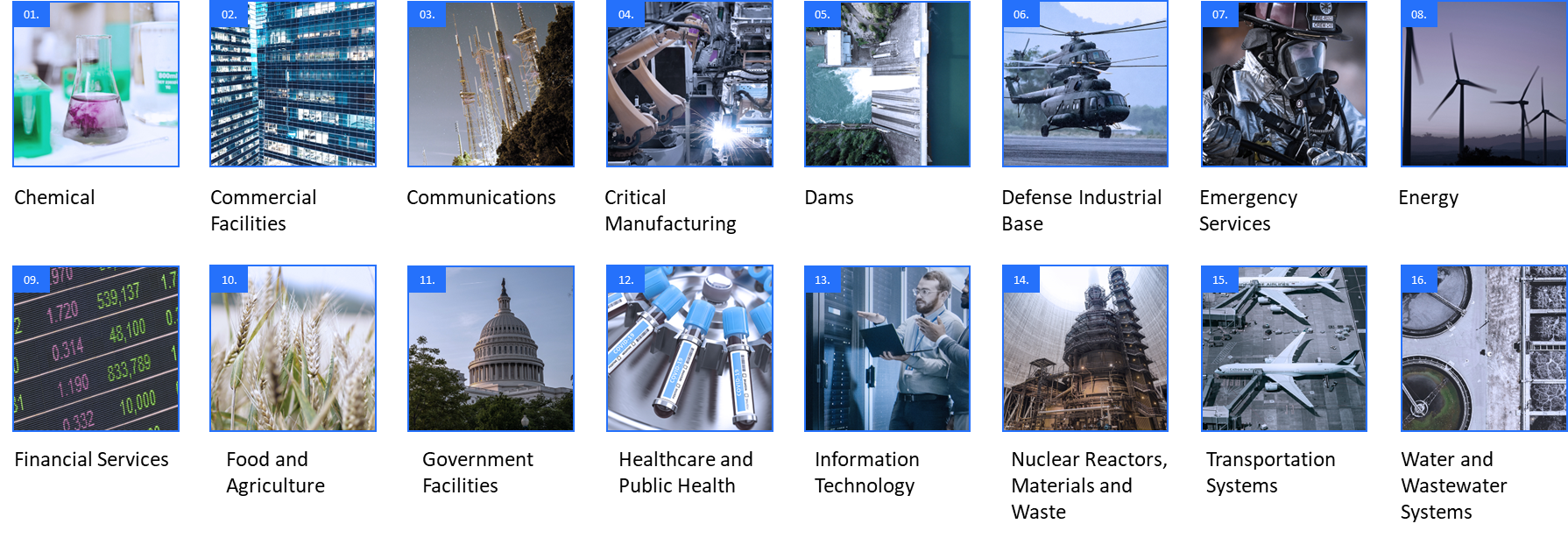
Description automatically generatedGraphical user interface

Description automatically generatedGraphical user interface

Description automatically generated

Industry Experience

OPSWAT’s system deployment experience extends to every critical infrastrcuture market and we enjoy leadership positions in Global Power Generation and Distribution, Government and the Defense Industrial Base, Financial Services and Oil and Gas production facilities.



Recommended Products for ENEC Requirements

## MetaDefender Platform

Graphical user interface

Description automatically generated

OPSWAT’s advanced threat prevention solution, MetaDefender Core enables the integration of advanced malware prevention and detection capabilities into existing IT solutions and infrastructure to better handle common attack vectors: securing web portals from malicious file upload attacks, augmenting cybersecurity products, and developing advanced malware analysis systems. The patented, industry-leading technologies that power MetaDefender Core include:

**Deep CDR**

Deep Content Disarm and Reconstruction (Deep CDR) prevents known and unknown file-based threats, protecting against malware and zero-day attacks. Deep CDR regenerates safe, usable files and supports hundreds of file types, including PDFs, archives, and file formats that support archives.CDR disarms active embedded threats, sanitizes, and reconstructs every file to prevent zero-day attacks and advanced evasive malware.

**Multiscanning**

Conduct simultaneous analysis with 30+ leading anti-malware engines to detect nearly 100% of known threats.

**Proactive Data Loss Prevention (Proactive DLP)**

Check for sensitive and confidential file content to prevent data leakage and meet regulatory compliance.

**Threat Intelligence**

Provide enriched intelligence on threats on billions of hashes, IPs and domains.

**Next Generation Sandbox**

Deliver adaptive threat analyses.

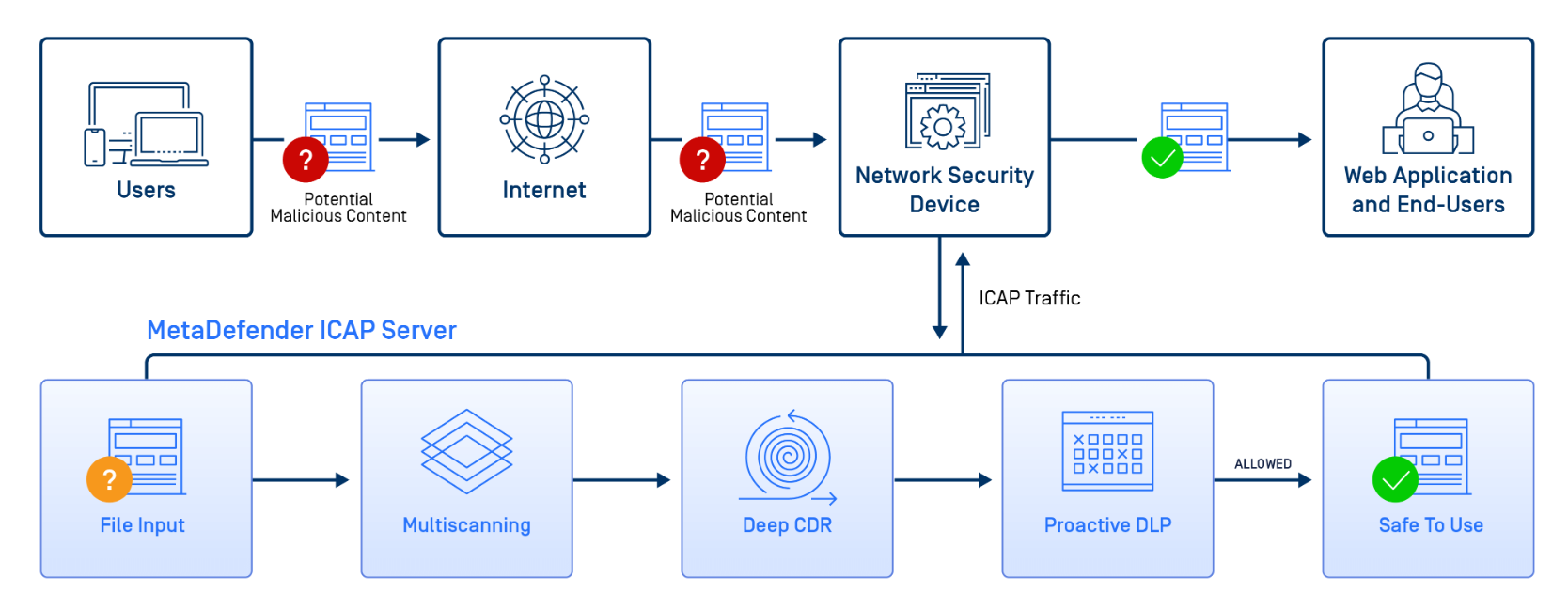
**File-Based Vulnerability**

Scan and analyze binaries and installers to detect vulnerabilities before exposure.

OPSWAT Solutions Overview

### MetaDefender ICAP Server

MetaDefender ICAP Server is a plug-and-play solution to protect your network against malicious internet content. MetaDefender ICAP Server uses the Internet Content Adaptation Protocol (ICAP) to integrate with network appliances to protect against advanced threats in network traffic and storage devices, using industry-leading theat prevention technologies.



MetaDefender ICAP Server can be used with any ICAP-enabled network appliance, including application delivery controllers, network gateways, forward and reverse proxies, attached storage devices, and next-generation firewalls.

**MetaDefender ICAP Benefits**

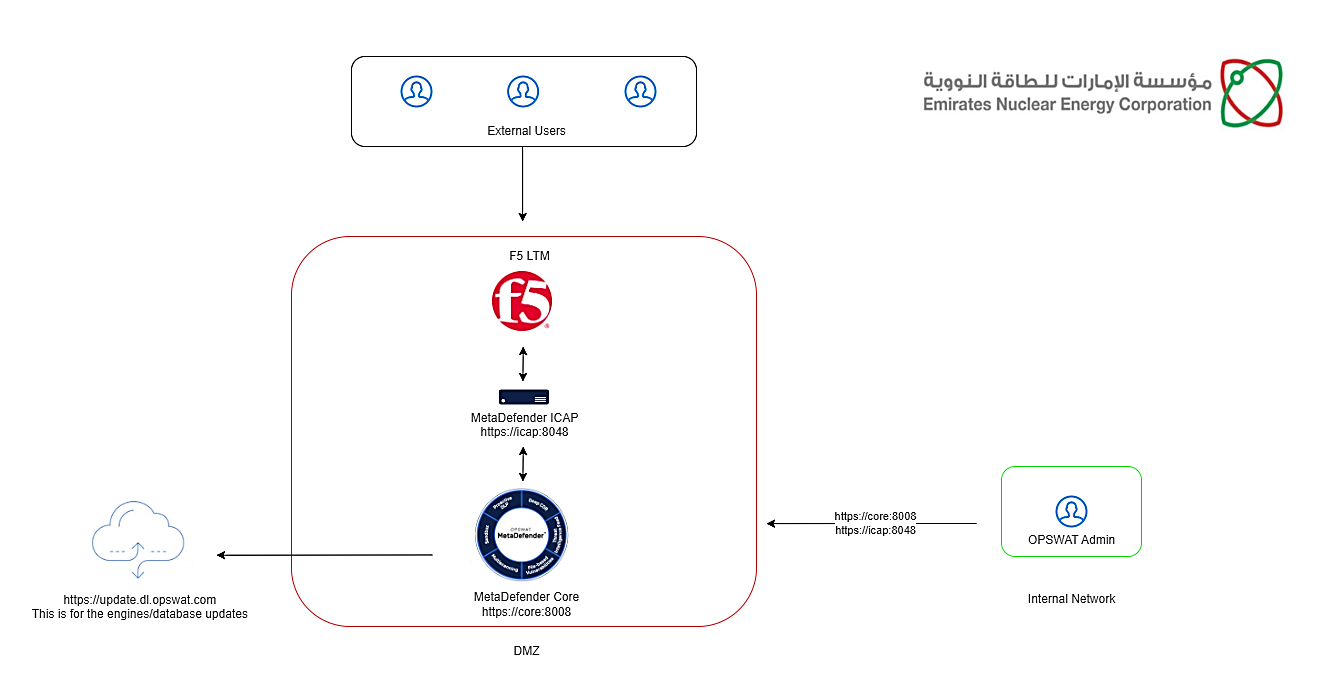
* Real-time comprehensive threat detection and prevention for your network
* Protection from malicious file uploads at the gateway of your network
* Protection against zero-day and advanced targeted attacks
* Detection of file-based vulnerabilities before they are installed
* No more sensitive data entering or leaving your organization without your discretion
* Custom policies, workflow, and analysis rules to meet your unique security needs
* Simple integration with any ICAP-enabled devices

HLD

A screen shot of a computer

Description automatically generated

LLD



OPSWAT Support Plans

OPSWAT offers different technical support plans to best meet your organizations needs

|  | **Silver** | **Gold** | **Platinum** | **US In-Country Platinum** |
| --- | --- | --- | --- | --- |
| **Support Hours** | | | | |
| **Support via OPSWAT Portal Case Management System** | **7AM to 7PM** On Business Days | **24 hours**  On business Days | **24 x 7 x 365** | **24 x 7 x 365** |
| **Support via Chat** | **7AM to 7PM**  On Business Days | **24 hours**  On Business Days | **24 hours**  On Business Days | **8 AM to 9 PM ET**  On Business Days |
| **Support via Phone** |  | **24 hours**  On Business Days | **24 x 7 x 365** | **24 x 7 x 365**  **For Blocker Cases** |
| **Incident Response Times** | | | | |
| **First Response Times for Blocker Severity Issues** | Within 4 hours\* | Within 2 hours\* | Within 1 hour | Within 1 hour |
| **First Response Times for Lower Severity Issues** | Within 3 business days | Within 2 business days | Within 1 business day | Within 1 business day |
| **Customer Success Management** | | | | |
| **Assigned Customer Success Manager** |  |  | A blue circle with a white tick in it  Description automatically generated | A blue circle with a white tick in it  Description automatically generated |
| **Quarterly Conference Call Reviews** |  |  | A blue circle with a white tick in it  Description automatically generated | A blue circle with a white tick in it  Description automatically generated |
| **Yearly Roadmap Review with the Product Team** |  |  | A blue circle with a white tick in it  Description automatically generated | A blue circle with a white tick in it  Description automatically generated |
| **Quarterly Summary Reports** |  |  | A blue circle with a white tick in it  Description automatically generated | A blue circle with a white tick in it  Description automatically generated |

During the hours covered in the that support plan (\*)  
See our Hardware and Appliance Warranty section at the following [link](https://www.opswat.com/support#:~:text=above%20USD%202%2C500.-,OPSWAT%20Hardware%20and%20Appliance%20Warranty%20Plan,-OPSWAT%27s%20Hardware%20and)