SOLUTION BRIEF

# Get Advanced Data Protection with Fortinet FortiProxy

## Executive Summary

**The Fortinet secure web gateway (SWG) solution, FortiProxy, delivers a powerful array of advanced data protection capabilities, designed to safeguard organizations from a variety of web-based threats while ensuring regulatory compliance and secure management of sensitive information.**

**One of the standout features of FortiProxy is its ability to perform deep content inspection, including sophisticated image analysis, optical character recognition (OCR) for text in images, and exact data matching (EDM) for precise data loss prevention (DLP). These capabilities are essential for organizations that handle sensitive information, enforce compliance with strict data protection policies, or wish to filter inappropriate or harmful content.**

## Image Analysis Capabilities

With its integration into existing FortiGate deployments via internet content adaptation protocol (ICAP) as well as a standalone solution, FortiProxy provides a comprehensive and scalable solution to ensure all web traffic, including images and multimedia, is monitored and protected from both security risks and data leakage.

### FortiProxy Highlights

- Advanced protection against threats
- Virtual domains high performance and scalability
- Content caching and WAN optimization

A key advantage of the FortiProxy data protection suite lies in its image analysis capabilities, which go beyond traditional content filtering to classify images based on their visual content. This ensures that inappropriate images, whether containing nudity, weapons, violence, or other categories of concern, are detected and blocked before they reach the network.

FortiProxy also extends its DLP protection by identifying and analyzing text within images using OCR technology, ensuring that sensitive data within visual media is secured. Combined with its EDM-based DLP that leverages predefined datasets, FortiProxy offers a multi-faceted solution that protects both structured, unstructured, and visual data. These features, available as a standalone solution or integrated with FortiGate via ICAP, allow customers to implement granular control over the content that flows through their networks, ensuring comprehensive data protection and compliance across all traffic types.

## Image Analysis for Content Filtering and DLP

FortiProxy image analysis capabilities stand out for their ability to identify, categorize, and enforce image policies, making it a critical part of its broader data protection strategy. Web filtering and DLP solutions have traditionally focused on text-based content, leaving visual media less scrutinized. However, FortiProxy addresses this gap by deploying machine learning (ML) and artificial intelligence (AI) to analyze images in real time, allowing organizations to block unwanted content and prevent data leakage through visual channels.

This feature is particularly useful when dealing with unknown images—user-generated content, obscure media, or new images that haven't been indexed or categorized before. FortiProxy analyzes these images using AI-driven categorization to help security teams enforce policies even when the content hasn't been previously flagged. The system classifies and enforces policies around various types of content, such as:

- **Nudity or explicit material:** Detects and blocks partial or full nudity, pornographic content, or sexually explicit material. This is especially useful in workplaces, educational institutions, or environments that adhere to strict content standards.

- **Weapons and firearms:** Recognizes guns, knives, or other weapons in images, helping institutions like schools, hospitals, and corporate environments block violent or dangerous content.
- **Violence and gore:** Detects images depicting physical violence, blood, or graphic injury, ensuring that sensitive audiences are not exposed to harmful content.
- **Hate symbols or offensive imagery:** Identifies symbols or gestures linked to hate speech or discrimination, which can help protect against harassment or the promotion of harmful ideologies.
- **Drugs and illicit substances:** Blocks imagery related to drug use or paraphernalia, supporting organizational policies that promote safe and compliant environments.

## Content Appropriateness for Unknown Images

FortiProxy advanced analysis is particularly valuable when dealing with "unknown" images that traditional databases haven’t precategorized. It uses ML models to evaluate the visual characteristics of each image, such as shapes, textures, and patterns, allowing it to categorize and block images that exhibit attributes associated with harmful content, even if the image is entirely new or hosted on unfamiliar URLs. Key FortiProxy advanced analysis features include:

- **AI-driven contextual analysis:** This enables FortiProxy to understand isolated visual elements and the context in which they appear. For instance, it differentiates between a firearm shown in an educational context (such as on a museum website) and one depicted in a violent or threatening scenario.
- **Customizable policies:** Organizations can tailor filtering rules according to their specific needs, setting different sensitivity levels for various content categories. For example, a corporate office might block nudity and hate speech but allow access to political or news sites containing images of protests or violent events.

## OCR Technology for Text in Images

A key extension of FortiProxy image analysis is its OCR capability, which enables the extraction and analysis of text within images. This feature is especially powerful DLP because sensitive information is often embedded in visual formats, such as scanned documents, screenshots, or photographs. FortiProxy can apply DLP policies to this text, ensuring that confidential or sensitive information is not inadvertently shared or leaked via images. Key FortiProxy features are:

- **Sensitive data detection:** FortiProxy can detect and block images containing sensitive information such as Social Security numbers, account details, passwords, or confidential business data extracted via OCR.
- **Compliance and security:** Organizations in regulated industries (like finance and healthcare) can prevent the unauthorized sharing of personal data or intellectual property hidden within images. OCR also ensures compliance with regulations like GDPR, HIPAA, or PCI-DSS by detecting and blocking sensitive text within visual media.

## EDM-Level DLP with Predefined Datasets

In addition to OCR, FortiProxy also supports EDM to offer even more accurate DLP. EDM uses predefined datasets, such as lists of customers’ PII, credit card numbers, or employee IDs, to ensure that exact matches of this sensitive data are flagged or blocked when they appear in network traffic, whether in text or within images. The benefits include:

- **Structured data protection:** By leveraging these predefined datasets, organizations can create precise DLP policies that specifically protect key data assets, ensuring that no sensitive information is leaked through misconfigured policies or user negligence.
- **Low false positives:** EDM ensures that DLP enforcement is highly accurate, reducing the occurrence of false positives that can frustrate users or hinder productivity. This is particularly important for organizations that handle vast amounts of sensitive structured data.

## Integration with FortiGate via ICAP

When deployed alongside FortiGate firewalls via ICAP, FortiProxy advanced image analysis, OCR, and DLP features can be extended to all network traffic inspected by the firewall. This integration provides a seamless method for combining network-level security with in-depth content inspection. Examples of this include:

- **FortiGate offloading:** FortiGate can send image data and web content to FortiProxy for more advanced inspection, reducing the load on FortiGate processing resources and enabling more granular content inspection at scale.
- **Unified policy enforcement:** Security teams can centrally manage DLP, content filtering, and web security policies, ensuring consistent enforcement across the organization. Whether traffic involves images, multimedia, or text, FortiProxy uniformly applies its powerful filtering and DLP capabilities.
- **Scalability:** The integration ensures that FortiProxy can scale with the network, providing high-performance, real-time analysis and protection, even for large organizations with complex web traffic patterns.

## Regulatory Compliance and Workplace Safety

The combination of FortiProxy image analysis, OCR, and DLP capabilities allows organizations to enforce robust policies that ensure both regulatory compliance and workplace safety. By identifying and blocking inappropriate or harmful content, as well as securing sensitive information, FortiProxy helps organizations:

- **Maintain safe digital environments:** Whether in schools, corporate offices, or public-facing platforms, FortiProxy prevents exposure to inappropriate content, helping create safe, compliant environments for employees, students, or customers.
- **Meet industry regulations:** FortiProxy advanced DLP features help organizations comply with strict regulations by preventing the unauthorized sharing of sensitive or regulated data, both in text and image formats.

## Conclusion

The comprehensive FortiProxy data protection suite, which includes sophisticated image analysis, OCR-based DLP, and EDM-level precision, ensures that organizations can control textual data and visual media flowing through their networks. The solution provides a granular, customizable approach to prevention of content filtering and data loss, blocking harmful or inappropriate images, and protecting sensitive data hidden in structured and unstructured forms.

When integrated with FortiGate via ICAP, FortiProxy extends these protections to all network traffic, ensuring consistent enforcement of policies, reducing risk, and regulatory compliance across the board. FortiProxy is an invaluable tool for organizations focused on securing their digital environments and preventing data leaks.

www.fortinet.com

October 25, 2024 1:53 PM / MKTG-190-0-0-EN