

# FileWall™



Eliminate Malware Threats from  
email attachments

19 Hamalacha ST. Rosh Haayin  
48630 Israel



972-3-9026080



info@odix.com



www.odi-x.com



# Contents

**2**

The Challenge

**3**

FileWall for  
Exchange online

**4**

FileWall – Solution  
Components

**5**

FileWall  
Technology

**6**

FileWall Admin  
Console

**7**

Easy  
Implementation

**8**

User Reviews

**9**

About odix

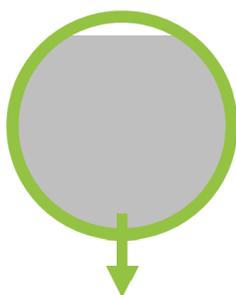
# The Challenge

94% of malware is delivered via email

According to recent research, spear phishing emails with malware attachments are the most common vectors for deployment of Advanced Persistent Threat (APT) attacks. These meticulously crafted emails bait the user into opening attached files, with the understanding that the file will run inside the organization's network.

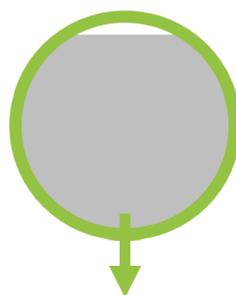
At this widespread method of spreading malware is not new, most organizations implement a secured email gateway in an attempt to block suspicious traffic. However, it is virtually impossible for such detection-based solutions to keep up with and detect the thousands of sophisticated malware variations that emerge daily. As a result, organizations remain vulnerable to one of the most popular channels for attacks. Today, an estimated 94% of malware is delivered via email. 90% of malware hidden in files use common types such as PDF, Office and archive. [source: Verizon business 2019 Data Breach Investigations Report]. Moreover, 34% of hacks involves internal actors.

**Cyber threats ; watch your email, your files, your colleagues**



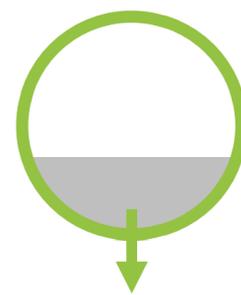
**94%**

of malware delivered via email



**90%**

of file based attacks use Office, PDF and archives



**34%**

involved internal actors behind the attacks

Source: Verizon business (2019 Data Breach Investigations Report), Mimecast threat intelligence report

# FileWall for Exchange online

The only Microsoft 365 native app for CDR malware prevention

FileWall is a native Microsoft 365 application providing the ultimate security layer against file-based attacks. FileWall is based on odix's patented algorithm for eliminating malware hidden in files. Instead of trying to detect a known malware and block the file for the user, FileWall service disarms malware and provides a sanitized file for safe usage. FileWall provides an effective malware prevention solution against both known and unknown malware attacks and handles all incoming email traffic including internal emails. The product is designed to run in conjunction with existing Microsoft security solutions such as EOP and ATP, ensuring no harm or change to any of Microsoft sender related security capabilities.

FileWall service has been available officially for online purchase via the Microsoft marketplaces since September 14, 2020 for SMBs. FileWall introduces a new paradigm for SMBs, enabling them to consume an enterprise-grade security solution that they can activate instantly and affordably.

## **Cutting edge technology - no malware bypass:**

FileWall supports the sanitization of even the most complex files, including archives, password-protected files, nested files, and more. This is made possible due to odix's unique analytical capabilities, which enable a highly granular examination of the files.

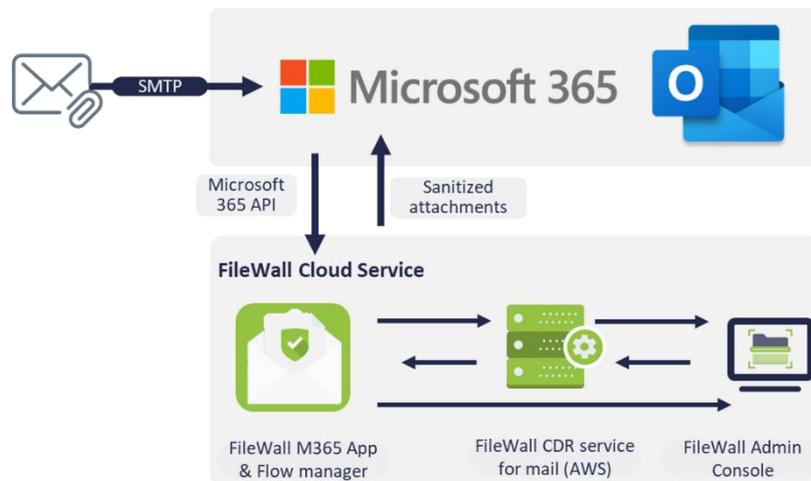
A Complementary solution to Microsoft EOP & ATP, FileWall provides disarming malware from commonly used files offering seamless deployment and high performance.

# FileWall -Solution Components

Providing Malware-Free files for safe usage

FileWall provides deep file inspection for disarming malware of any kind - regardless if it's known or unknown. Based on odix's unique patented algorithm, FileWall supports nested files attacks and complex file scenarios.

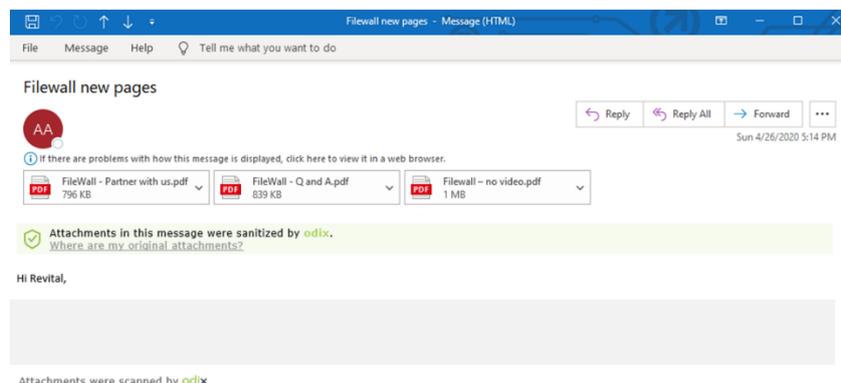
FileWall solution architecture is illustrated in the following diagram:



As a native Microsoft 365 app, FileWall is integrated seamlessly via Microsoft APIs.

Equipped with a powerful, smart admin console, FileWall offers total visibility and control of the file sanitization process including Content Disarm and Reconstruction (CDR) and the company's security policy.

Once its service is activated, FileWall will process all email messages with attachments and notify users within their email messages, as shown below.



# FileWall Technology

Providing Malware-Free files for safe usage

**FileWall** is powered by odix's field-proven **True Content Disarm and Reconstruction (TrueCDR™)** core technology. This patented technology scans, disarms and rebuilds files into clean versions that can be safely used by users. odix TrueCDR™ technology removes both known and unknown malicious code from a wide range of file types, while encapsulating three functional phases within various security processes.



## STEP 1

**Policy enforcement** –FileWall initially checks if the company policy allows the file to be processed. The policy enforcement can be determined by file type, user, file characteristics and even by dynamic content within the file.



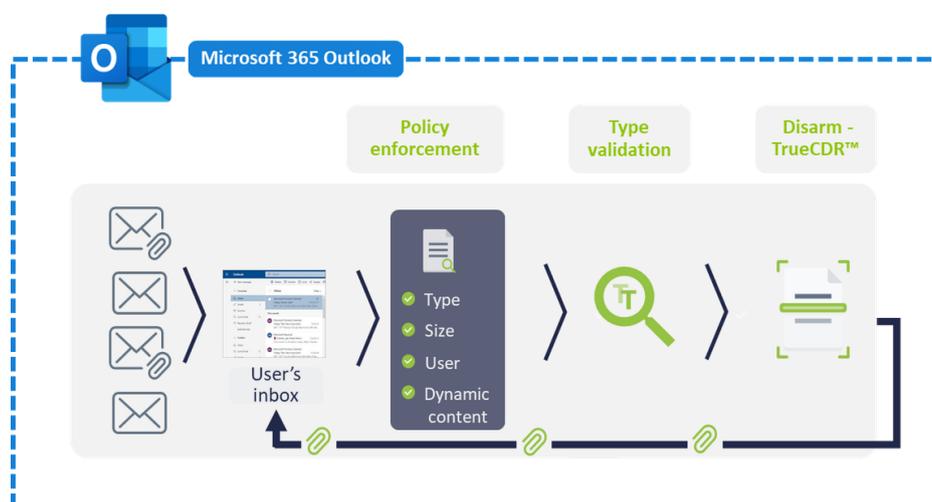
## STEP 2

**Smart True Type check** –FileWall conducts a smart True Type check, including file type validation, file structure validation, matching of file type and file shape to suffix, and additional validation checks of the file itself.



## STEP 3

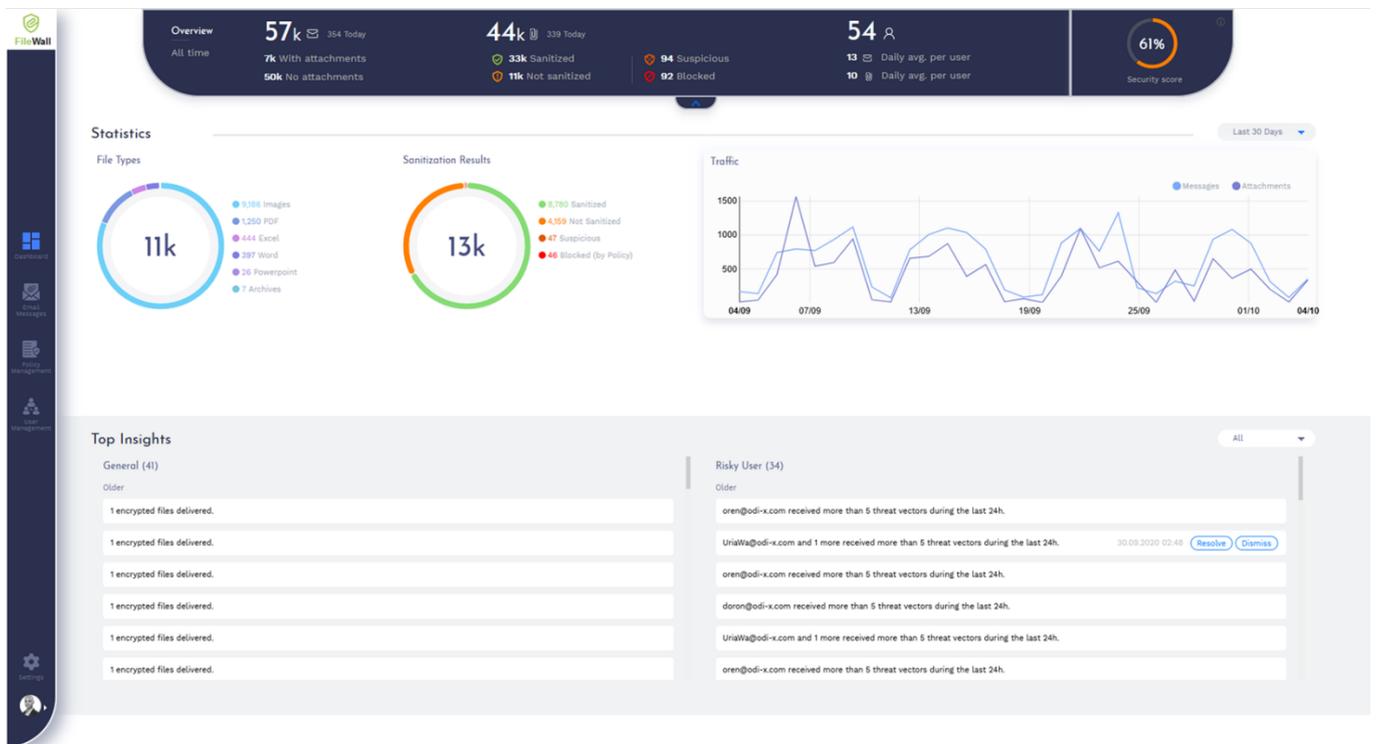
**TrueCDR** –FileWall applies multiple advanced algorithms to each file. These algorithms perform complex operations precisely tailored to each file type. They, identify and immediately destroy known and unknown hidden malware –without changing the structure of the files.



# FileWall Admin Console

The **Management Server** enables configuration and reporting. It performs several functions including:

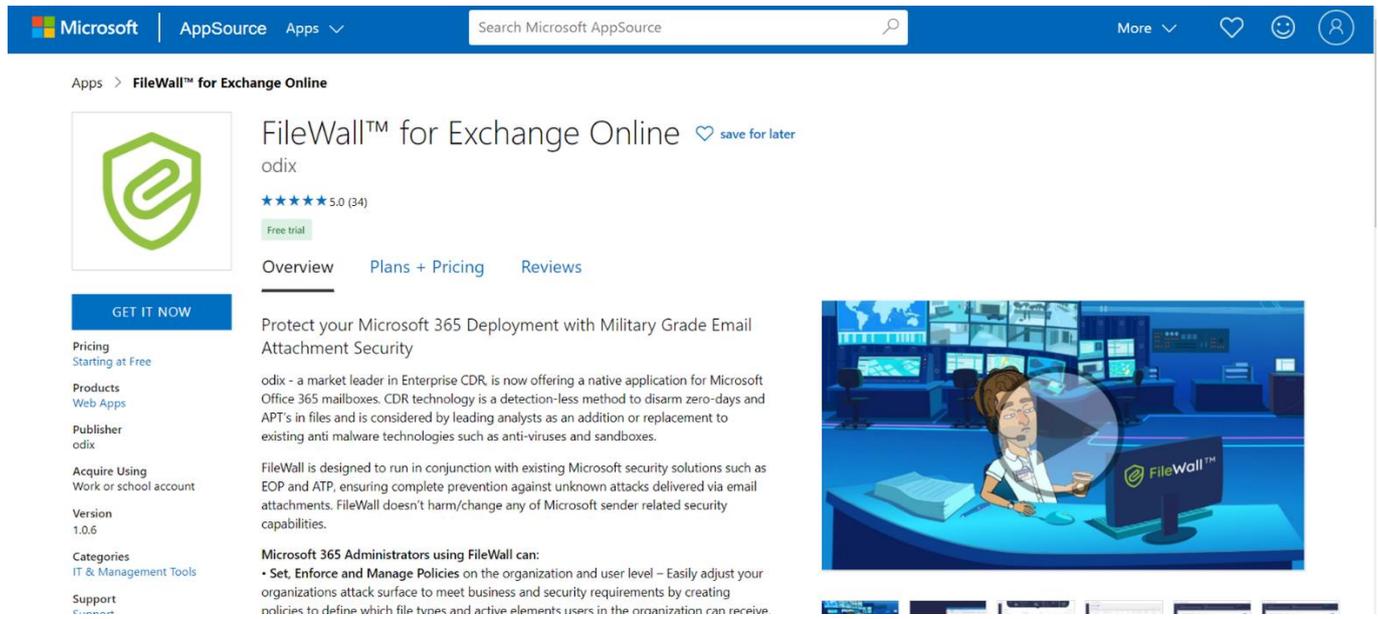
- **Comprehensive dashboard** – presents updated insights about the processes files, risky users and more.
- **User Profiles** – establishes user profiles for the sanitization including:
  - Rules regarding which files are allowed to be sanitized and/or prohibited.
  - Permitted sanitizing volumes for a single file and a collection of files.
- **Log Data** – the admin console stores log data of the system processes.
- **Admin sign in** – using the same credentials, the Microsoft 365 administrator can log into the admin console.



# Easy Implementation

No integration required

FileWall is available for direct purchase at the Microsoft marketplaces. In addition, Microsoft CSPs can bundle the service from their Microsoft partner account portal.



The screenshot shows the Microsoft AppSource interface for the application 'FileWall™ for Exchange Online' by 'odix'. The page features a blue header with the Microsoft logo, 'AppSource' branding, a search bar, and navigation icons. The main content area includes the application's logo (a green shield with a white 'e'), a 'GET IT NOW' button, and a sidebar with metadata such as 'Pricing: Starting at Free', 'Products: Web Apps', 'Publisher: odix', 'Acquire Using: Work or school account', 'Version: 1.0.6', and 'Categories: IT & Management Tools'. The main text describes the application as 'Military Grade Email Attachment Security' and provides details about its CDR technology and integration with Microsoft security solutions. A 'Free trial' badge is visible. A 'save for later' link is also present. On the right, there is an illustration of a person at a computer workstation with a 'FileWall™' logo on the monitor. Below the illustration are several small thumbnail images.

# User Reviews

FileWall user experience by Microsoft MVPs

odix highly appreciates the FileWall user's community feedback in the Microsoft AppSource and other platforms. We are looking forward to expanding the FileWall cybersecurity coverage for hundreds of millions of users within the broader Microsoft 365 community.



**Mohamed Elsherif**

Oct 15, 2020

## It is the best for protection

FileWall helped us to resolve our email security issues. Although we used many security tools before but File Wall beats them all, its the best to provide the required security to protect your business save your budget. The tool was able to achieve the highest level of satisfaction for both the IT employees and the company's employees



**Emanuel Ceciu**

Oct 7, 2020

## Great security add-on for Exchange Online

FileWall is a great security add-on for Exchange online. It was super easy to configure it and the user/admin interface is super intuitive. It catches a number of attachments which passed through EOP without problems. In today's environments where a lot of malware is coming via email and users are opening all messages and clicking



**Sanjay Kumar**

Aug 18, 2020

## FileWall is a must have security add-on for all EOP users

FileWall is a necessary security layer along with basic EOP. I configured Filewall and it was very easy to deploy and manage. I was surprised that the it captured lot of infected attachments and SPAM emails which EOP did not capture.



**Oluwaseyi Davies**

Jul 26, 2020

## Great solution to protect Microsoft 365 mailboxes from being compromised

FileWall is quick and simple to implement, a great security supplement for Microsoft 365 tenant. FileWall is easy to configure and navigate even by a non tech savvy and as such posses all the qualities like: efficiency, functionality, adaptability, maintainability, and usability.

# | About odix

**odix** develops and markets advanced anti-malware tools based on its **True Content Disarm and Reconstruct (CDR)** technology for preventative cybersecurity in enterprises of all sizes. odix's technology prevents the malware infiltration to organizational networks by removing all malicious code from a wide range of file types. Uniquely, odix protects files from unknown attacks, where legacy solutions fall short.

odix solutions are trusted by enterprises in diverse sectors including industrial, finance, insurance, and government.

odix operates from its headquarters in Israel and from regional offices in the U.S.A. and Europe.

For more information visit odix website  
<https://odi-x.com>