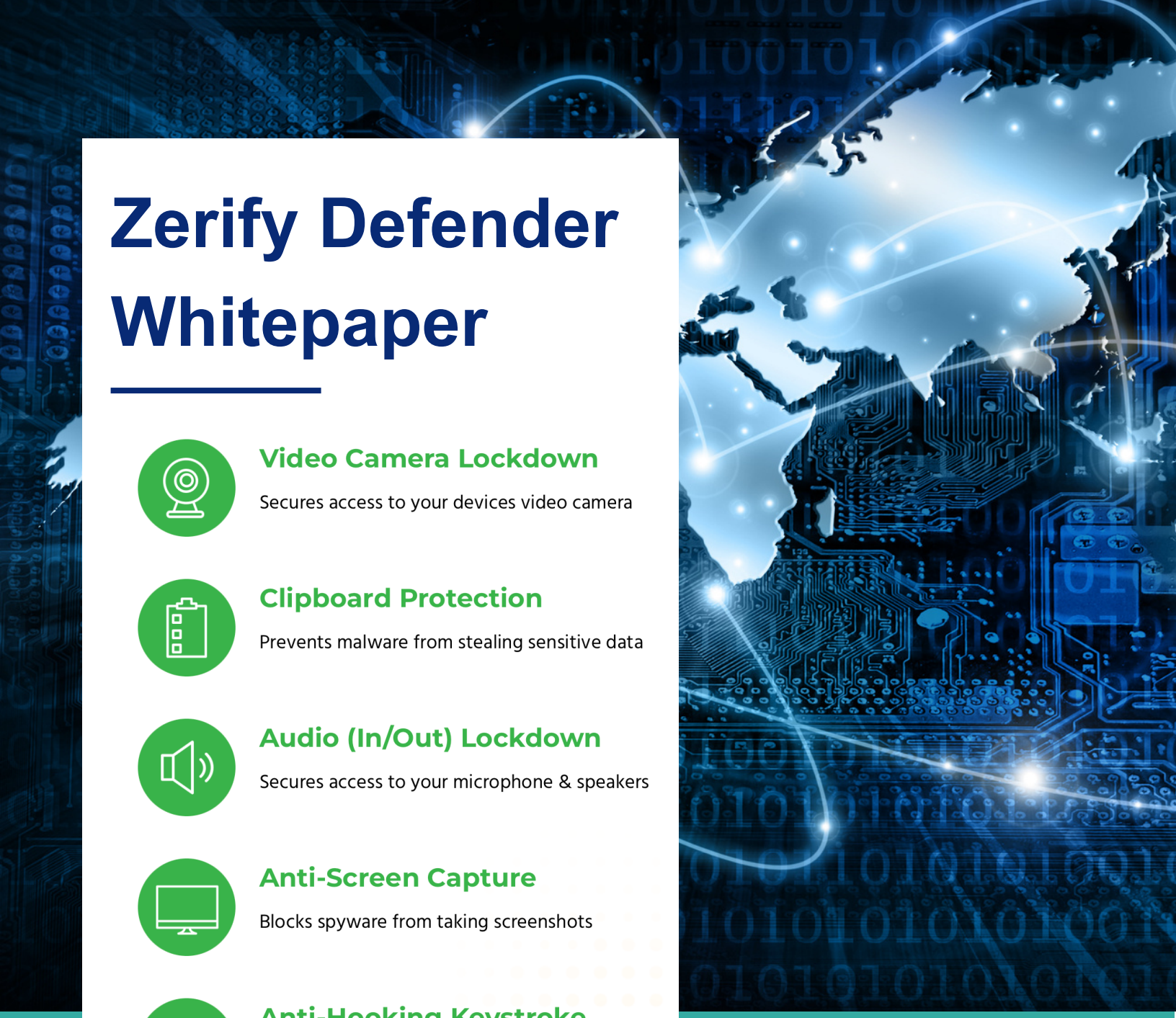


Zerify Defender Whitepaper

Video Camera Lockdown

Secures access to your devices video camera

Clipboard Protection

Prevents malware from stealing sensitive data

Audio (In/Out) Lockdown

Secures access to your microphone & speakers

Anti-Screen Capture

Blocks spyware from taking screenshots

Anti-Hooking Keystroke Protection

Blocks malware from stealing your keystrokes

Zerify™

Table of Contents

Introduction

Cybersecurity is at a crossroads. Even though more money is being spent on cybersecurity (IDC forecasts $219 billion spending on cybersecurity in 2023), the attacks have only increased. This is because hacking has become an industry with specialized players including criminal gangs and nation state players.

"What is needed is a new paradigm to tackle this growing menace"

Cybersecurity begins at the endpoint. Malware detection is not 100%. Some malware will evade detection. This is the Security Gap. What is required is a strategy to protect the endpoint in the event anti-virus software is not successful in detecting the malware.

Zerify Defender takes a different approach. Rather than trying to detect malware it protects the key data that the malware is after – keystrokes, screen shots, clipboard and media. This way, even if the malware escapes detection by anti-virus software, the important data is still protected.

Most data breaches are caused by keyloggers which grab user credentials when they are entered into websites and during network logon. Some of the malware also capture the screen (especially financial malware) and modify the clipboard. With the rise in remote work and video conferencing, the camera, microphone and audio output are increasingly becoming the target of hackers.

By locking down the keystrokes, screen, clipboard, camera, microphone and audio output, Zerify Defender protects the critical data of an endpoint in the event anti-virus software fails to detect malware.

Keystroke Protection

Keyloggers are a component of malware that grab keystrokes. They are the #1 reason behind most data breaches. Hackers use keyloggers to capture user credentials and other PII entered into websites and VPN clients. Once they have the user credentials, they can commit identity theft, steal funds, burrow deeper into the corporate network and cause mayhem. The current defense of trying to detect them does not always work due to zero-day exploits and novel methods of evading anti-virus software.

How keyloggers work

When a keystroke is entered on the keyboard, it is read by a piece of software called the keyboard driver. The driver encodes the keystroke into a message and sends it in the message queue until it is displayed in the program that has the focus.

The malware can grab the keystroke by placing a hook in the message queue at various points and read the keystroke. Several Windows API (such as GetKeyState, GetAsyncKeyState, GetKeyboardState, JournalRecordHook, LowLevelHook, etc) exist to facilitate this.

How Zerify Defender protects against keyloggers

When a keystroke is entered, Zerify Defender grabs the keystroke at the lowest level possible and encrypts it. It then generates a fake key, which appears as a number ranging from 0 to 9. It monitors the message queue for keystrokes and retrieves the encrypted key and displays it in the application that has the focus.

Zerify Defender secures all windows applications as well as the login screen.

Screen Capture Protection

Many malware variants, especially financial crimeware, have a screen capture module. This allows them to take screen shots of data of interest. Typically, this module is activated when the user navigates to a specific URL, such as a bank website. If a virtual keyboard is used to prevent keyloggers, the hacker can take screen shots of the password/pin being entered by the user.

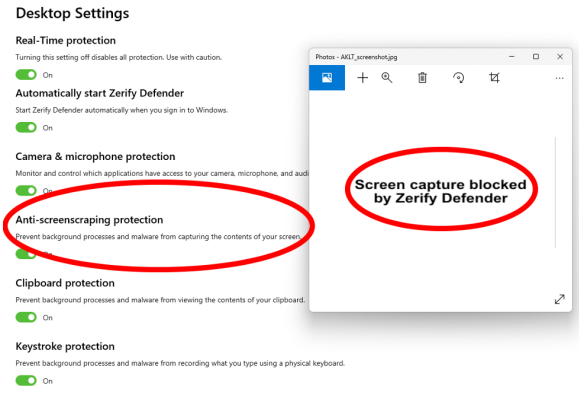
How screen capture works

The screen can be captured in two ways – (1) simulating the print screen keystroke programmatically, or (2) hooking into the windows display buffer or calling certain windows functions. The screen shot can be triggered by a keystroke event, mouse click or at certain intervals.

How Zerify Defender protects against screen capture

To secure against the print screen key capture, Zerify Defender monitors the keystrokes for indication of the print screen keypress event. It then prevents the keystroke from invoking the print function and presents a security screen to the user.

To defend against malware that access the windows display buffer or call windows screen capture API, Zerify Defender hooks into the pertinent API calls and determines if the process is authorized to capture the screen. If not, it displays a security screen.



Clipboard Protection

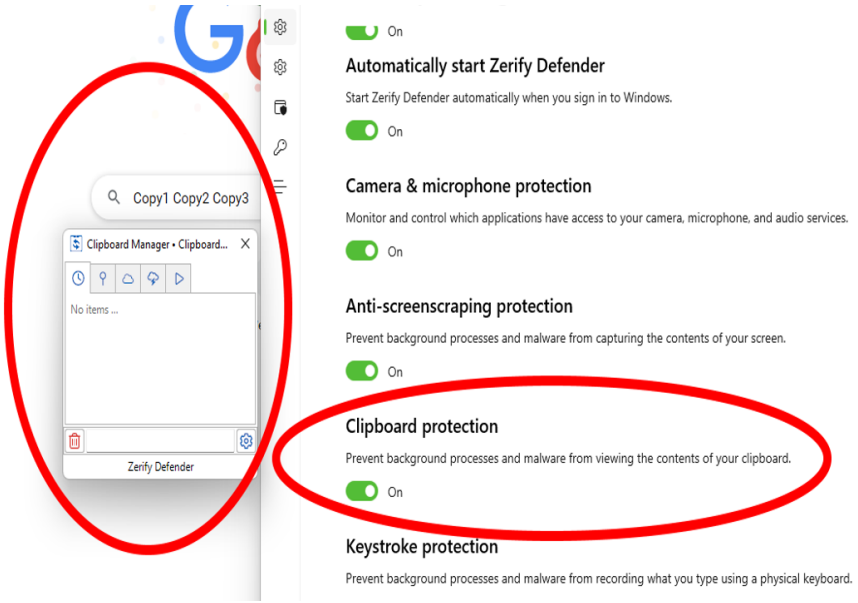
Generally speaking, whenever you copy an item (such as image or text), it is temporarily stored in the clipboard buffer until you paste that item somewhere else. This is a functionality used very commonly, and the hacker is fully aware of this, especially when it comes to confidential information and data. However, this is a security issue that is still extremely overlooked.

How clipboard capture works

Clipboard capture works by accessing the contents of the copy buffer. In some cases, the clipboard contents can be modified. The capture is typically triggered by keystroke events.

How Zerify Defender protects against screen capture

To defend against malware that access the windows copy buffer, Zerify Defender hooks into the pertinent API calls and determines if the process is authorized to access the copy buffer.



Media Protection

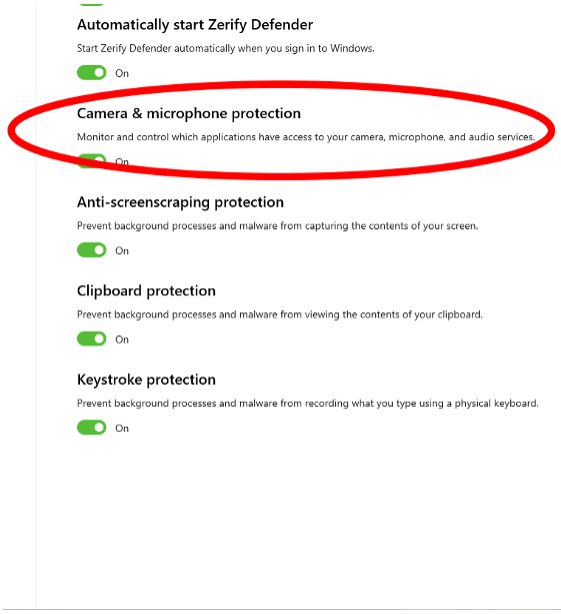
With the advent of remote work and the rise in video conferencing, protecting access to the camera, microphone and audio output has become important. Recording the video conference is fairly easy for an attacker and thus the new way of doing business is at risk.

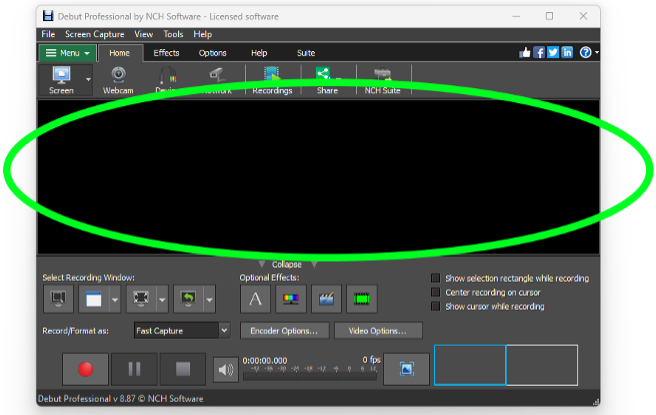
How media capture works

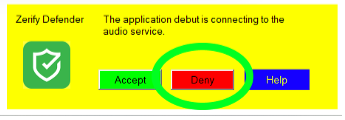
Media capture works by enumerating the media devices and calling specific API to record the media stream.

How Zerify Defender protects against media capture

To defend against malware that accesses the media stream, Zerify Defender hooks into the media stack and checks every media access request. The user is notified of the access request allowing them to grant/deny access.





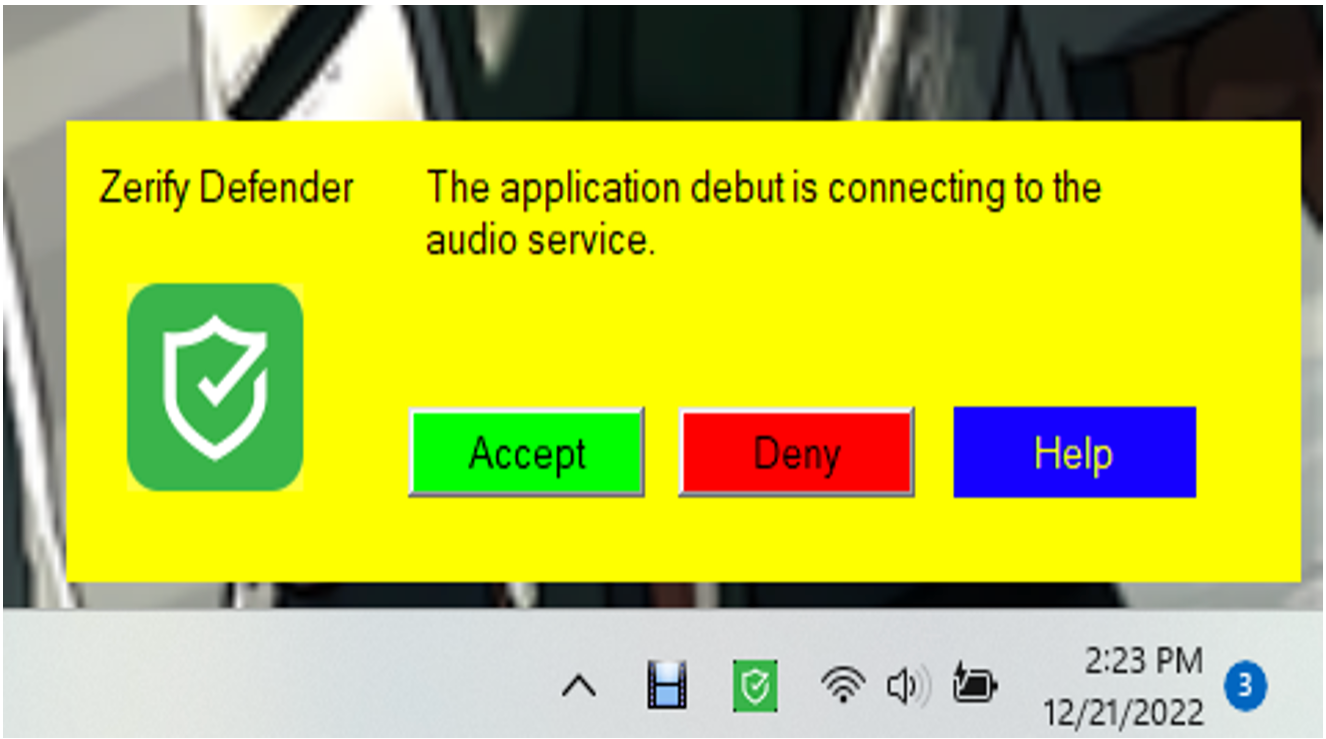


NIST 800-171

Any organization that processes or stores sensitive, unclassified information on behalf of the US government is required to be compliant with the National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171) cybersecurity standards. NIST 800-171 specifically focuses on the protection of Controlled Unclassified Information (CUI) and seeks to ensure that such sensitive government information located on contractors' networks is both secure and protected.

NIST SP 800-171 requirement 3.13. 12 and CMMC practice SC. 2.178 require that you "Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device."

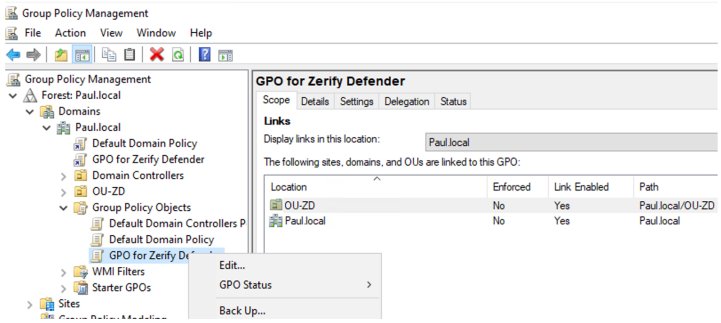
This pertains to notifying the user when their camera or microphone is accessed. Zerify Defender addresses this requirement by notifying the user when their camera or microphone is accessed and allows them to prohibit their use.



Enterprise Deployment

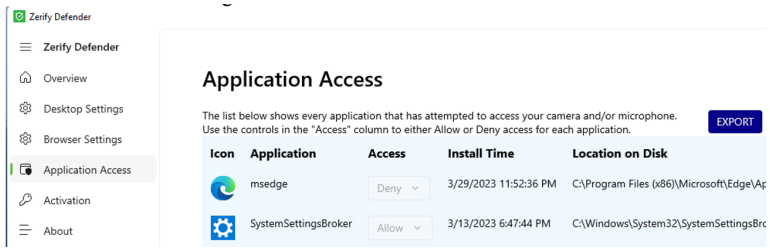
Installation

Zerify Defender can be installed via Active Directory Group Policy. This enables enterprise admins to manage the installation without any user intervention.



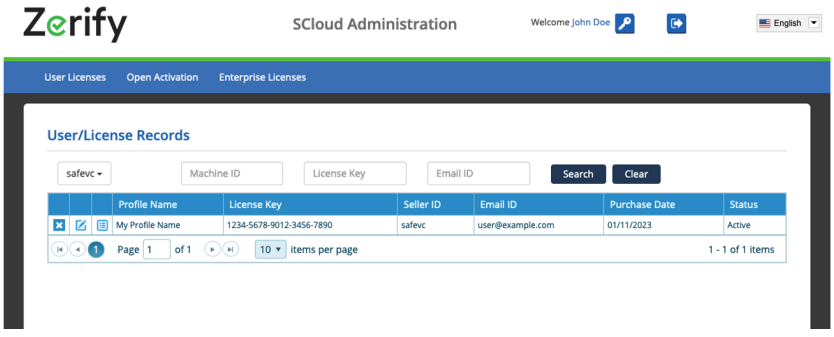
Whitelisting

If there are trusted apps that the enterprise does not need to be flagged, a policy can setup in Active Directory to have them whitelisted.



License Administration

The Zerify SCloud Administration portal allows you to manage enterprise licenses for Zerify Defender, users' accounts associated with those licenses, and the users' devices activated on each license.



Conclusion

Zerify Defender is a proactive cyber security solution that secures your endpoint. By locking down the keystrokes, screen, clipboard, camera, microphone and audio output, Zerify Defender protects the critical data of an endpoint in the event anti-virus software fails to detect malware.

"Zerify Defender is a useful tool for preventing many malicious forms of access to external devices and services. Defender has several intended purposes to provide protection. All the protection methods offer protection against intrusive or malicious software. While threat actors will continue to push the boundary of malicious access, Zerify Defender greatly improves the user's defense against stealthy attempts to retrieve sensitive information. Proof Labs finds very thorough protection when considered for the use case of companies hoping to achieve and prove security with controls described in NIST SP 800-171. Defender takes many steps to protect against malicious access. Zerify Defender software has addressed the spirit and has exceeded the standard of NIST SP 800-171 for protecting collaborative computing devices." **Dick Wilkinson, Co-founder Proof Labs**