

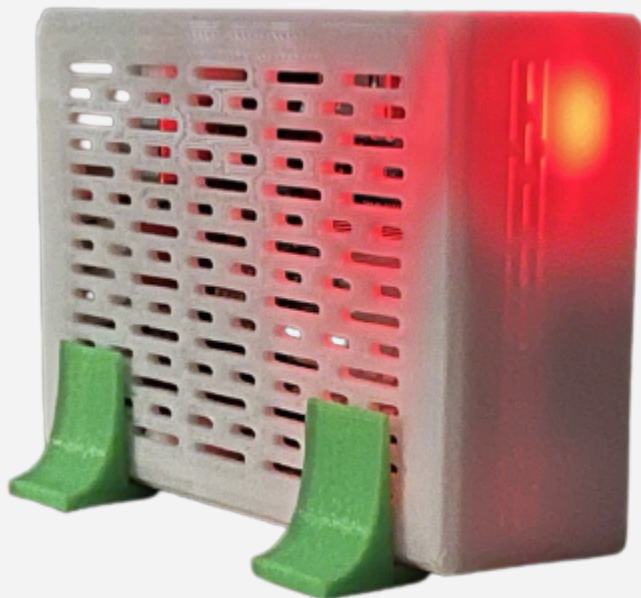
<https://cwg.systems>

# CWD Canary

## Automated Threat Detection and Alert System

---

CWD Canary Appliance Rev. 1.0



### Product Overview

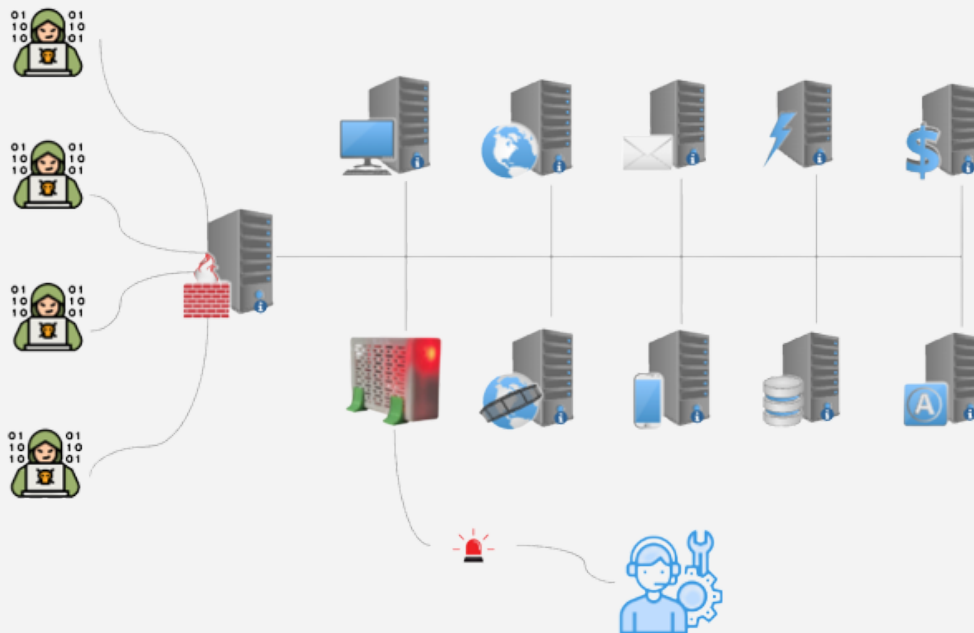
CWD Canary is a threat monitoring, detection, alert, and honeypot system for local networks. Canary will not only alert the network admin of attack attempts, but contain the attacker so that no damage can be done to the network. A large network that requires large-scale monitoring can take advantage of Canary to alert network admins of potential attacks before they can accomplish anything damaging.

Government and large corporation networks will benefit greatly with reduced effort on behalf of their staff to detect and eliminate threats to the network and its systems. All with a small device that notifies admins continually of any potential issues.

## What is a Canary


The Canary device can 'mimic' nearly any device from a Cisco switch to a Windows file server, mainframes, and workstations. Utilizing this technology, the Canary becomes a 'honeypot' luring attackers to attempt to take advantage of the mimic device. Attacker becomes lured in by the bait of an easily compromised system, and attempts to exploit it. While this is going on the Canary keeps track of the exploit attempts and documents them in a file for observation by network admins. Simultaneously, the device alerts the network admins to the attack attempt.

The notification is sent via email to network administrators who then become aware of the attack attempt, and can mitigate the situation effectively. Easily finding and understanding the attack attempt so that it may be resolved quickly and seamlessly. Information about the attacker, type of attack, and methods are all included in the notification details.



## Be Secure

With the help of the Canary, defending large networks becomes very simple and straightforward. The attacker's methodology and primary attack vectors and targets become



clear, and a plan can then be easily designed to thwart said attacks. Multiple Canary appliances can be deployed across multiple subnets on a large scale network.

- **Detailed Attack Reports and Targets**

With the reports generated by Canary, your network administrators will be fully aware of your network's weaknesses and primary targets. This allows them to provide much better defense of these targets and prevent the attack vectors.

- **Quick Notification and Action**

Canary's immediate notifications provide instant details to your administrators with everything they need to know to ensure the attack causes no damage to critical infrastructure.

Never fall prey to attackers again, keep a close eye on your network automatically, and be fully aware of what is going on within your network in a completely automated fashion.