QuellSecure

A RANSOMWARE CONTAINMENT ANALOGY:

There Are Only So Many Ways to Cook an Egg. Same for Encryption.

QuellSecure is designed to fight ransomware at the final step of an attack, when files are being maliciously encrypted to disrupt operations. Once the attack has begun, the results are obvious to the patented algorithm that powers QuellSecure's Active Containment™.

There are more ways to breach a network than to encrypt files. All file writes go through the OS file system driver — a chokepoint with a limited command set. Ransomware can vary its approach, but **it can only cook the egg so many ways.**

Cooking Eggs

WRITE DELIVERY METHODS

All file writes go through the operating system's file system driver, which has a limited number of ways to write bytes to locations in storage. The write commands can be invoked in different ways, and the malicious encryption can be disguised or optimized; **these are just different ways to cook eggs.** Two examples are:

1. **Direct Overwrite**
   Optimized for speed, not stealth. Writes to small files in full and the first few MBs of large files to maximize damage quickly.

2. **Memory-Mapped Writes**
   Writes to a temporary in-memory copy, relying on the OS to flush to disk. Slower but harder to catch early — gets further before triggering standard detection.

EVASION VARIATIONS: STILL JUST OMELETTES

These next three techniques have unlimited variations and are all applied slightly differently by various ransomware groups, but fundamentally aren't very different. If you add ham and cheese to an omelette, **it's still an omelette.**

1. Ransomware will partially encrypt files, mixing encrypted and unencrypted data to evade simple detection and move faster.

2. Ransomware mixes move, write, and delete operations to obfuscate destruction.

3. Ransomware uses specialized or custom encryption algorithms that are optimized to avoid different detection methods.

If QuellSecure can see bytes being written to files, our algorithm detects it regardless of the attack.

THE QUELLSECURE ADVANTAGE

All Ransomware Looks the Same To Us

Beyond the obvious benefit of easier and more efficient detection, QuellSecure's design comes with another critical benefit. To continue the egg analogy, it doesn't really matter who is cooking the eggs if you're aware of all the ways they can do it. From QuellSecure's perspective, all ransomware looks the same to our Active Containment™.

Truly novel encryption delivery is extremely rare.

With Active Containment™, the ransomware of yesterday is no different than today's or tomorrow's. Variant novelty doesn't matter if you're watching the chokepoint.

0-day
VARIANTS COVERED

∞
KNOWN VARIANTS COVERED

~7
FILES ENCRYPTED BEFORE CONTAINMENT