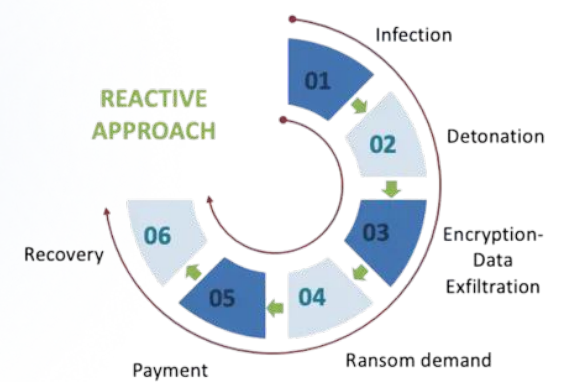


RansomSnare 2.0TM

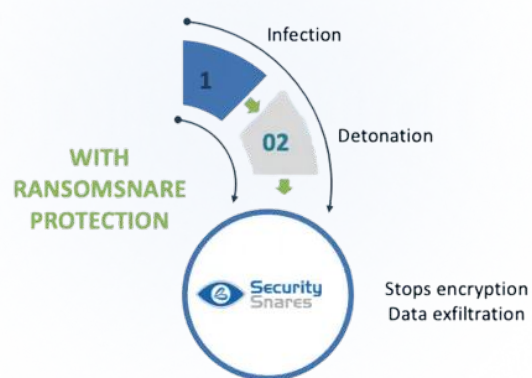
Ransomware threats are evolving rapidly, making it increasingly difficult for traditional endpoint security and anti-malware tools to keep pace. Endpoint detection and Response (EDR) alone are no longer enough—especially with today’s mobile workforce.

RansomSnare 2.0 provides a critical layer of defense against all forms of ransomware and extortion. Every ransomware attack relies on encrypting files or exfiltrating data. **RansomSnare 2.0** stops these attacks immediately by terminating malicious processes at the first attempt to encrypt or transfer data.

Ransomware Problem



Solving the Ransomware Problem



RansomSnare 2.0, powered by a lightweight mathematical algorithm, operates with minimal resource impact and avoids the performance issues common to behavior-based detection. Unlike solutions that depend on signatures, behavioral models, or machine learning, **RansomSnare 2.0** has successfully blocked every ransomware strain and variant for over five years—without requiring updates. With **RansomSnare 2.0**, you eliminate the need to recover from backups, downtime, and ransom payments.

How It Works

When ransomware infects your endpoint or server, it attempts to encrypt files and exfiltrate data from your environment. When ransomware tries to encrypt the first file or exfiltrate data, **RansomSnare** terminates the malicious process(es) and alerts the security team without disrupting systems or users. Because the process is immediately suspended, the security team can analyze the event and respond at their own pace. This approach eliminates the typical fire drill response.

Stop ransomware from working by terminating the malicious process as it attempts to encrypt and exfiltrate data.

Proprietary Detection Algorithm



Watch all files on the endpoint



Detect any attempt to encrypt a file



Classify the process (trusted or untrusted)



Terminate process if untrusted

Ransomware adversaries have significantly improved their techniques, rendering traditional endpoint protection ineffective against zero-day ransomware.

SecuritySnares offers complete protection against all ransomware threats:

File Share Protection (SMB)

The SMB/file share protection feature prevents ransomware from encrypting shared data by enforcing conditional write access. Unlike traditional EDR solutions, which detect and respond after malicious activity begins, this system stops encryption at the storage layer itself.

Malicious Script Protection

The Script Control feature prevents malicious or unauthorized scripting activity from encrypting or damaging corporate data. By monitoring the execution of scripting engines such as PowerShell, Python, and Bash, SecuritySnares identifies and blocks encryption behavior originating from unapproved interpreters.

Integrations

The SecuritySnares management console aggregates alerting information, agent status, agent configuration, and monitoring across the entire organization. The data can be managed in the console or integrated with your Security Information and Event Management (SIEM) tool, SOAR, Ticketing System, or MDR provider.

Data Exfiltration Prevention

The Data Exfiltration Prevention feature protects against unauthorized data theft by identifying and blocking the tools and techniques used by attackers during staging and exfiltration. Using real-time cyber intelligence, the system detects when known or suspicious exfiltration tools are invoked and automatically stops data transfer attempts.

Wiper Protection

Wiper attacks pose a significant threat, leading to irreversible data loss and devastating business disruption. RansomSnare 2.0 protects against the malicious deletion and/or corruption of sensitive data. RansomSnare ensures you never pay a ransom or recover from backup.

EVENTSSTART & END TIMESHOST NAMEACTION TAKENPROCESS PATHPROCESSPARENT PROCESS

14

11/17/2025, 2:55:20 AM
12/5/2025, 2:29:36 AM

WIN-PO3D8HUFAQ1

Killed

C:\Users\Administ...

babaxz.exe

MDS: 7500d43bcf0ee...

SHA256: 17722a2b266...

babaxz.exe

MDS: 7500d43bcf0ee...

SHA256: 17722a2b266...

Process ID: 2856

Process File Path: C:\Users\Administrator\Desktop\ransomware\babaxz.exe

Process MD5: 7500d43bcf0eed51952e112e0aae5d82

Process SHA256: 17722a2b266576261cfbccda0f6ac8aa2d86059ece1624afd11b586465b58165

Parent Process ID: 7748

Parent Process File Path: C:\Users\Administrator\Desktop\ransomware\babaxz.exe

Parent Process MD5: 7500d43bcf0eed51952e112e0aae5d82

Parent Process SHA256: 17722a2b266576261cfbccda0f6ac8aa2d86059ece1624afd11b586465b58165

Attempted File Encryption: C:\Users\Administrator\Documents\file_05_914aa06f.bin

IP Address: 51.79.67.99

Mac Address: FA163E41A0F2

AI Threat Analysis

High Confidence

The process name 'babaxz.exe' and its file path located in a directory labeled 'ransomwar...

Attempted Execution Times (Local Machine Time):

1. 12/5/2025, 2:29:36 AM

2. 12/5/2025, 2:29:35 AM

3. 11/20/2025, 6:31:03 AM

4. 11/20/2025, 6:31:03 AM

5. 11/20/2025, 6:31:02 AM

6. 11/20/2025, 6:31:02 AM

7. 11/17/2025, 8:15:43 AM

8. 11/17/2025, 8:15:43 AM

Allow

Dismiss Alert

Download Quarantined Process

Minimum Requirements

Processor

1 GHz

RAM

512 MB

Storage

60 MB

Platform Support

Windows 10 and later

Server 2016 and later

Coming Soon

Linux (RHEL and Debian variants)

MacOS

About Us

SecuritySnares is a leading ransomware-prevention company known for its mathematically powered RansomSnare platform, which provides real-time protection against all ransomware threats, supplementing traditional endpoint protection with a single, lightweight agent for comprehensive threat prevention. Founded by cybersecurity experts and executives frustrated with advanced endpoint protection technologies, SecuritySnare's mission is to protect organizations from the ever-evolving threat of ransomware and provide solutions designed to stop damage from the highest cybersecurity risks businesses face.