RansomStop

Frequently Asked Questions

General

What is RansomStop vs Plume Security?

A: RansomStop is an anti-ransomware solution created by Plume Security, Inc.

RansomStop

Methodology

How does RansomStop work?

A: RansomStop monitors file activity and file access, contents and metadata to determine if there is malicious encryption activity.

In the event of malicious encryption activity, RansomStop identifies the compromised user account, access keys, IP address and/or process id, and stops the activity in real time.

How does RansomStop avoid false positives?

A: Because we are looking at outcomes to data, and not intentions of executables or processes, it is much more certain. I.e. if the file isn't getting encrypted, it isn't ransomware.

Malicious encryption looks very different from traditional encryption. If you've ever done incident response for a ransomware attack, it looks obvious. Plume Security has distilled that information into a layer of signals to determine if the encryption is malicious in nature, or a normal part of operations.

Installation

What platforms are supported?

A:

- RansomStop can be installed on any supported Windows Server version (2016 or newer), and some older versions.
- RansomStop can be installed on Synology DSM 7.x, both virtual and hardware based.
- RansomStop supports all AWS S3 in any region.
- RansomStop supports all Google Drive instances.

How do I install RansomStop?

A: Install is simple and can be done in a few minutes on any platform.

- Windows. An executable installer is provided.

RansomStop

- Synology. A Synology SPK file is provided for Synology DSM.
- AWS S3. RansomStop uses pre-configured CloudFormation scripts to install into AWS Elastic Cluster Service (ECS).
- Google Drive. RansomStop uses local scripts to execute Google CLI commands to install into Google Cloud Run.

Integrations

Can I forward alerts to another tool?

A: Aside from viewing alerts in the RansomStop Admin Portal, you can also configure alerts to automatically be forwarded in real time to other tools to ease processes and workflows. RansomStop currently supports syslog, email and Slack, and we are adding new integrations all the time.

Security

Where does data analysis happen?

A: All data analysis happens in the customer environment and is not processed or stored in Plume Security's infrastructure.

What data does Plume Security have access to, process, or store?

A: Plume Security SaaS receives metadata from analysis, including Alerts (filename, location, username, IP, etc), summarized statistics (number of files read, modified, deleted, by user/IP/timeframe), Policy configuration, and high level logs from the RansomStop service(s).

Plume Security (systems, services, and employees) does not have access to, process or store any file contents outside of the customer environment.

How is data encrypted?

A: All node-to-node communications use AES-256 to encrypt all data in transit.

RansomStop

All API calls to RansomStop SaaS platform use HTTPS with TLS 1.2 or better.

All data stored in RansomStop SaaS platform is encrypted at rest with AES-256 encryption.

Other

Where can I see a demo?

A: We have demos available on our YouTube channel (https://www.youtube.com/@ransomstop), or feel free to contact us at sales@ransomstop.com for a personal demo.