Plume Security's

RansomStop

TECHNICAL BRIEF

# Data-Centric Ransomware Defense for Critical Infrastructure

## How Remote Encryption Attacks Evade Traditional Security

Traditional cybersecurity relies on **endpoint-based detection and response (EDR) and anti-virus (AV) technologies that attempt to identify and block malware during execution. However, modern ransomware attackers have evolved sophisticated evasion techniques that bypass these foundational defenses.

## The Critical Gap

Traditional endpoint security requires visibility into malware execution on the endpoint itself. But remote encryption attacks operate diffe ently. Attackers infiltrate systems through compromised credentials, RDP vulnerabilities, or VPN access, then execute encryption remotely **without** malware executing on the target endpoints. This means EDR and AV tools never "see" the attack occurring.

## Attack Vectors That Evade Endpoint Security

Ransomware attackers leverage multiple pathways to encrypt data while remaining invisible to traditional defenses:

### Remote Desktop Protocol (RDP) Exploitation

Attackers exploit weak passwords, misconfigured RDP settings, or unpatched vulnerabilities to gain remote access. Once authenticated, they can execute encryption commands without triggering endpoint security tools that typically monitor for malware execution on local systems.

### Compromised Credentials

Legitimate user credentials (stolen via phishing or data breaches) allow attackers to authenticate and access file servers as trusted users. Endpoint security tools cannot distinguish between legitimate administrative activity and malicious encryption.

RansomStop

**Phishing & Email-Based Initial Access**

While phishing may install initial reconnaissance tools, attackers establish remote access channels (RDP, VPN, web shells) before deploying ransomware, keeping their encryption operations remote and invisible to endpoint agents.

**“Living Off The Land" (LOTL) Attacks**

Attackers use legitimate Windows system tools (PowerShell, WMI, robocopy) to execute encryption. Because these are valid operating system utilities, EDR tools struggle to differentiate malicious use from legitimate administrative activity.

**The Data Shows the Problem is Real**

According to Sophos 2024 research, 59% of organizations experienced ransomware attacks in the last year.

Of those attacks:

- **70% successfully encrypted data** despite EDR/AV deployment
- **57% successfully compromised backups**, making recovery impossible
- The median recovery cost exceeded $1.7 million

**Attackers** only need to get encryption right **ONCE**.

**DEFENDERS must get detection right Every Single Time.**

## Why RansomStop Takes a Different Approach

As AV and EDR tools improve, attackers shift tactics to methods these tools cannot detect. Rather than trying to detect malware execution (the cat-and-mouse game), **RansomStop** monitors **data itself for malicious interactions**. This approach is fundamentally more difficult to evade because **data either gets encrypted or it doesn't**, regardless of attack origin or technique.

***The Core Principle...***

Instead of asking ***"Is malware executing?"***

**RansomStop** asks "***Is data being encrypted in abnormal ways?***"

RansomStop

# SOLUTION ARCHITECTURE & INTEGRATION

## Data-Centric Detection Methodology

**RansomStop** continuously analyzes data characteristics to identify ransomware activity with forensic precision:

**Detection Signals Analyzed**

1. **File Format Changes**: Monitors whether files are being converted to encryption-specific formats (e.g., new file extensions, binary data replacing readable text)
2. **File Content Analysis**: Detects when file contents shift from recognizable data patterns (documents, databases, images) to encrypted random-looking binary data, a hallmark of ransomware activity.
3. **File Name Patterns**: Identifies systematic renaming of files or bulk pattern changes consistent with ransomware behavior.
4. **Access Pattern Anomalies**: Detects abnormal user access patterns (e.g., sudden bulk file modifications from accounts that typically read-only access, access during unusual hours, or modification velocities inconsistent with normal operations)

### Detection is Nearly Impossible to Evade

Encryption creates observable data transformation. Whether attackers use remote encryption, LOTL techniques, or sophisticated evasion methods, the encrypted data presents the same telltale signatures **RansomStop** monitors.

### Automated Response: Seconds, Not Hours

Upon detection of malicious activity, **RansomStop** immediately executes automated containment protocols:

- **Suspended Compromised Account**: The user account conducting the malicious activity is immediately suspended, preventing further access
- **Blocked Attacker IP Address**: The IP address originating the encryption activity is blocked at the network level

- **Malicious Process Termination**: Any processes associated with the malicious activity are stopped
- **Complete Response in Seconds:** All actions occur automatically without human intervention, halting the attack before significant data destruction

**Speed is critical:** Modern ransomware encrypts thousands of files per second. Manual response delays measured in minutes can mean thousands of additional compromised files.

## Architecture & Deployment Model

**RansomStop** uses a **containerized analyzer architecture** designed for deployment flexibility and data sovereignty

## Core Components

### Containerized Analyzers

- Lightweight containers deployed on-premises or in customer-controlled cloud environments
- Process event streams from protected systems in real-time
- Generate policy-based alerts when malicious activity is detected
- Data never leaves customer infrastructure (no cloud data transmission)

### Windows Server Integration

- Lightweight agent forwards Windows event logs to the on-premises analyzer
- Agent designed specifically for file event export (minimal performance impact)
- Compatible with other endpoint agents (non-interfering architecture)
- Awaits automated response instructions upon attack detection

### NAS Appliance Integration

- Built-in syslog service forwards file events to analyzer and responder service
- No additional agents or appliances required for NAS devices like Synology

RansomStop

### Cloud & SaaS Protection (Agentless)

- Analyzer containers deployed in customer's cloud environment (AWS, Azure, GCP)
- Uses native cloud APIs to monitor file access and changes in:
- Google Drive
- Microsoft 365 SharePoint/OneDrive
- Cloud object storage buckets
- Any SaaS storage platform with API access
- **Agentless deployment**: Zero performance impact, no client software

### Key Architectural Advantages

- **Data Sovereignty**: All data analysis occurs within customer infrastructure; customer retains complete control
- **On-Prem or Cloud Flexible**: Deploy analyzers on-premises or in customer-owned cloud accounts
- **Minimal Performance Footprint**: Lightweight agent design ensures no interference with business operations
- **Non-Intrusive**: Compatible with existing endpoint security tools; no conflicts or performance issues

## Integration With Existing Security Infrastructure

**RansomStop** integrates seamlessly into mature security operations environments.

### Management & Policy Configuration:

- **SaaS Admin Portal**: Centralized policy management, alert configuration, and rule tuning
- **No Specialized Skills Required**: Straightforward interface designed for IT operations teams without advanced cybersecurity expertise
- **Rapid Deployment:** Typical installation requires only minutes per storage location

### Security Operations Integration

- **SIEM Integration**: Alerts can be forwarded to Security Information & Event Management systems for centralized logging and correlation
- **SOAR Integration**: Alerts can trigger automated playbooks in Security Orchestration, Automation & Response platforms
- **Managed Service Provider (MSP) Integration**: Alerts can be forwarded to external MSPs for 24/7 monitoring and response
- **Alert Visibility**: Real-time alerts viewable in both RansomStop Admin Portal and integrated security platforms

RansomStop

## Deployment Footprint

**RansomStop** protects business-critical data stores with a **targeted, efficient footprint:**

- File Servers
- SQL Servers
- Application Servers
- SharePoint Environments
- Web Servers
- Cloud Object Storage
- NAS Appliances
- Hypervisors

Rather than protecting every endpoint (resource-intensive and incomplete), **RansomStop** laser-focuses on the data repositories that drive business operations, enabling faster deployment and reducing false positive noise in security monitoring.

## Operational Benefits

### Set-It-and-Forget-It Simplicity

- Installation takes minutes per storage location
- No continuous endpoint agent management required
- Responds automatically without human intervention
- Works 24/7 without requiring specialized cybersecurity expertise

### Resource Efficiency for IT Teams

Unlike endpoint products requiring continuous monitoring, updating, and configuration management across hundreds or thousands of devices, **RansomStop's** targeted deployment on critical data stores significantly reduces IT team burden while providing superior protection for the assets that matter most.

## Summary

**RansomStop** addresses the fundamental gap in traditional ransomware defense: **attackers who bypass endpoint security and encrypt data remotely**. By monitoring data itself for encryption-specific changes rather than attempting to detect malware execution, **RansomStop** provides nearly impossible-to-evade protection. Rapid automated response in seconds ensures attacks are contained before significant damage occurs. The flexible, containerized architecture integrates seamlessly with existing security infrastructure while maintaining complete data sovereignty, critical for government and critical infrastructure operators.