Agger: Service Description

The Big Picture: How Agger Stops Ransomware

Agger stops ransomware by turning every computer into a minefield for attackers.
It quietly places harmless bait files and system objects that legitimate programs never touch but ransomware inevitably will. The moment a process interacts with one of these traps, Agger kills it before encryption can begin.

At the same time, Agger continuously monitors how every process interacts with the file system.
If a program starts rapidly renaming files, rewriting large volumes of data, or showing other tell-tale signs of active encryption, Agger shuts it down immediately.

Because Agger evaluates behaviour instead of signatures, cloud intel, or AI predictions, it can block completely new zero-day ransomware even if no one has ever seen the strain before. Kernel-level self-protection ensures attackers cannot disable or interfere with Agger during an intrusion.

This combination means Agger blocks attacks earlier, stops threats that other tools miss, operates fully offline, and avoids the slowdowns caused by scanning engines or AI models.

Why Agger Is Different

Traditional EDR and anti-ransomware tools look for known threats through:

- Signatures
- Cloud lookups
- Machine learning models
- Behaviour classification tuned for general malware

These methods only stop ransomware they have seen or been trained on.
Agger takes a completely different approach.

Agger doesn't care **who** the ransomware claims to be.
It cares **what it's doing**.

Ransomware cannot encrypt files without revealing its behaviour.
Agger detects those actions the moment they begin.

No cloud lookups.
No signature updates.
No model drift.

No dependency on threat feeds.
No performance impact from heavy scanning.

Just deterministic disruption of encryption behaviour.

Layered Detection Model

1. Deception: Instant, High-Confidence Detection

Agger reshapes each endpoint into hostile terrain for ransomware by planting system-specific decoys, runtime lures, fake recovery artefacts, and bait objects.

These traps are invisible to the user but unavoidable for ransomware.
If anything touches a decoy, Agger immediately terminates the process.

The unique layout per endpoint prevents attackers from testing or bypassing traps.

---

2. Core Behaviour Engine: Zero-Day Safe by Design

Agger's kernel minifilter observes real-time file-system behaviour at a granular level. It detects patterns that only encryption or destructive activity produce:

- High-entropy writes
- Rapid rename or deletion bursts
- Large-scale rewrites
- Extension changes
- Abnormal relocations
- Behavioural "distance" between operations

This is why Agger remains effective even against brand-new, morphed, or custom-built ransomware families.

---

3. Scutum Anti-Tamper: Protection That Cannot Be Disabled

Agger includes kernel-level self-protection that blocks attempts to:

- Kill its processes
- Suspend or unload its components
- Disable protected EDR or backup agents

These events act as an early warning, often surfacing an attacker long before they launch ransomware.

Proven Against Modern Threats

Agger has been tested against most major ransomware and wiper families since 2017, as well as a continuous stream of in-house zero-day samples.

Because Agger focuses on behaviour:

- Obfuscation does not matter
- New variants work against themselves
- Fileless strains still reveal activity
- Tamper attempts trigger alerts
- Zero-days are blocked with no tuning required

Agger is purpose-built as the last line of defence for stopping destructive behaviour.

Data Privacy: 100% Local Analysis

Agger performs all analysis on the endpoint.
No files ever leave the device. Ever.

It works:

- Fully offline after initial activation
- On-prem or in any private cloud region
- Without cloud scanning or threat lookups
- In sensitive and highly regulated environments

This architecture eliminates data sovereignty issues entirely.

Enterprise Performance: Light, Fast, Invisible

Across production environments, Agger averages:

- ~90 MB RAM
- ~0.55 percent CPU

It runs two user-land and two kernel components, engineered for minimal overhead even during heavy file-system activity.

Deployment: Simple, Fast, Zero Friction

Agger requires no special infrastructure.

Deploy via:

- SCCM
- BigFix
- Any enterprise software platform

Supports GUI and command-line installation.
Onboarding typically completes within minutes per device.

Plays Nicely With Your Existing Stack

Agger is not a traditional AV or EDR, so it avoids the conflicts that come from:

- API hooking
- Kernel callbacks
- File scanning on drop
- Behaviour classification engines

It operates as a complementary layer and integrates cleanly alongside:

- CrowdStrike
- Microsoft Defender for Endpoint
- SentinelOne
- Backup/restore platforms
- SIEM/SOAR pipelines (via event APIs)

Agger strengthens the security stack without overlap.

Response Workflow: Fast, Clear, Configurable

When Agger detects ransomware behaviour, it can:

- Kill

- Kill + quarantine
- Capture memory / system state for forensics
- Report all details to the SOC (process tree, paths, triggers, timestamps)

This lets defenders contain threats in milliseconds and conduct accurate post-incident analysis.

Updates: No Threat Feeds, No Daily Maintenance

Agger requires:

- No signatures
- No cloud intelligence
- No ML retraining
- No continuous tuning

Only occasional engine improvements and feature updates.

Reporting & Forensics

Agger provides detailed telemetry for every event, including:

- Full process tree
- Violating paths
- Behavioural and deception triggers
- Exact timestamps
- All associated activity

These records support compliance, audit, and deep forensic reconstruction.

Legacy Support

Agger continues to support Windows 2000 through Windows 7 SP1.
On these systems, the deception engine provides strong protection even without modern OS capabilities.