FileMan
INFORMATION MANAGEMENT

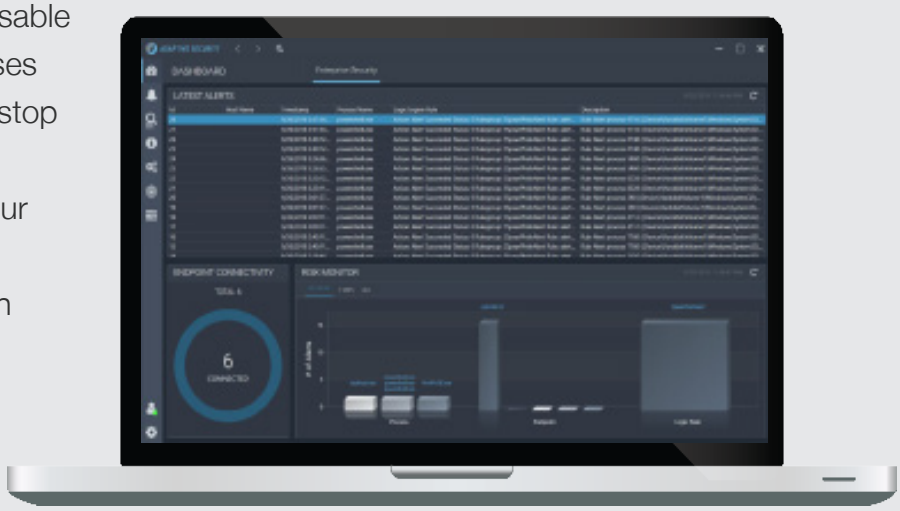
ADAPTIVE SECURITY

Visibility into your environment is crucial to your organisation's security. When you can find the critical data at the right time, you have a wealth of information to inform your next steps: Is my organisation compromised? Has someone taken critical data out of my organiation? How was someone able to access our environment? Is something about to happen?

FileMan Adaptive Security provides the visibility, adaptability and control you've been missing with traditional endpoint products.

THE FILEMAN ADVANTAGE

- **Compress response time.** Shorten the feedback loop by answering root cause questions in seconds. Use a uni ied view of live and historical endpoint activity across the enterprise to quickly anticipate and respond to threats.
- **Quickly adapt to changing threats.** Our programmable intelligent agent can respond automatically based on behaviours.
- **Stop threats in real time.** A customisable logic engine on the endpoint recognises and acts on threats at chip speed to stop threats in real time.
- **Get intelligent endpoint visibility.** Our lightweight agent (3.5 MB) provides real-time visibility at the kernel level on desktops, laptops, and servers.



FILEMAN
INFORMATION MANAGEMENT

ADAPTIVE SECURITY

STOP WASTING TIME

By leveraging endpoint analytics, FileMan Adaptive Security reduces the time it takes to detect an impending or ongoing attack. This approach accelerates recovery time; makes it easier to adapt to changing environments, regulations, and attack vectors; and ultimately stops incidents in their tracks. Stop wasting time wading through endless piles of data hunting for elusive threats. Detect and block threats in real time; investigate within minutes; strike back against attackers; and automate response actions to stop data exfiltration and lateral movement. Take back control. Sound good? We think so.

BUCK THE ENDPOINT STATUS QUO

FileMan Adaptive Security has perfected the art of continuous monitoring and response to isolate the important (and often small) signals from the noise and identify uncharacteristic behaviours. How? FileMan Adaptive Security relies on two fundamental and unique elements to drive the protect-detect-respond-remediate process:

- The Digital Behaviour Recorder™ continuously monitors and records key digital behaviours including sessions, processes, images, registry, DNS queries, network flow data, files, removable media, printing activity, and keylogs.
- The logic engine provides customisable logic on the endpoint, enabling it to recognise and act on threats in real time.

WHAT YOU CAN DO WITH FILEMAN ADAPTIVE SECURITY

FileMan Adaptive Security offers a wide portfolio of capabilities, but our customers love the ability to:

- Isolate infected endpoints from the rest of the enterprise
- Immediately distinguish between legitimate and harmful user or application behavior
- Stop ransomware and spearphishing attempts before they execute
- Detect and repel active attackers in real time
- Detect malware
- Uncover root cause in minutes
- Maintain the system's viability—even after being compromised
- Push out remediation across the enterprise
- Mislead adversaries by turning endpoints into decoy targets
- Replace existing antivirus agents with integrated Windows Defender Antivirus
- Meet Federal Information Processing Standards (FIPS) 140-2 Level 1 requirements