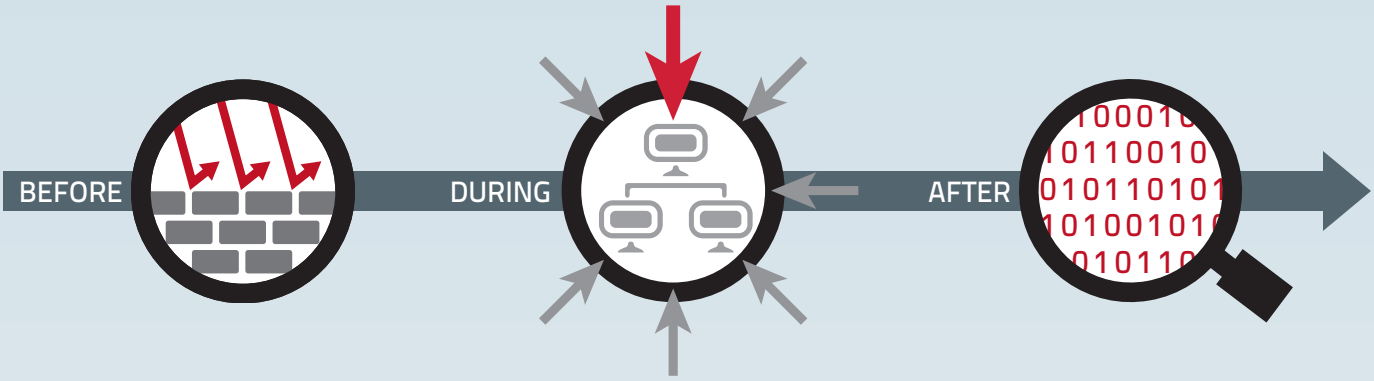
Cybersecurity: Ready or not?



Your challenge: Attack frequency and sophistication are changing. You need to protect your network, devices and data.

Your need: Cost effective threat remediation. A security solution that is scalable, smart and supports standard policies and controls.

Your solution: EventTracker – a combination of our award winning SIEM product plus expert services. Our threat centric approach reduces complexity while delivering superior visibility and control, while saving you time and reducing costs. With EventTracker you get advanced threat protection across threat continuum – before, during and after attacks.

Before an attack

Discover. Enforce. Harden.

You need to know your network in order to defend it. Discover the vulnerabilities in your devices and applications. Apply secure configuration to reduce your attack surface.

EventTracker Vulnerability Assessment Service helps avoid attacks by identifying vulnerable systems and versions, and by providing detailed recommendations on remediation.

EventTracker Configuration Assessment compares your existing configuration against baselines from Microsoft, DISA, or the USGCB. Secure configuration is an economical method to reduce attack surface.

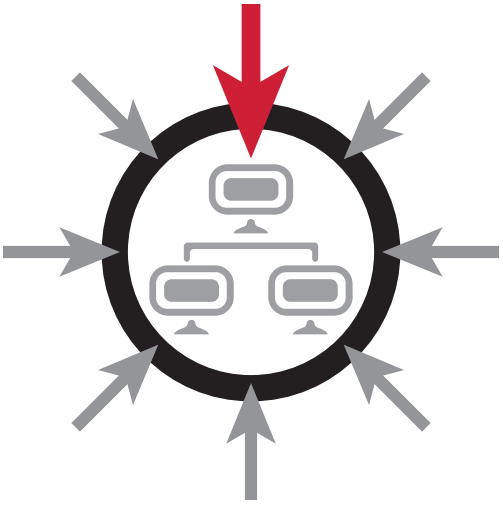
EventTracker | 8815 Centre Park Drive, Columbia MD 21045

www.eventtracker.com

EventTracker
Logging In Depth

During an attack

Detect. Block. Defend.



Today's threatscape includes advanced malware and zero-day attacks. You need quickly deployed, low resource, accurate threat detection to continuously identify malicious activity on your network.

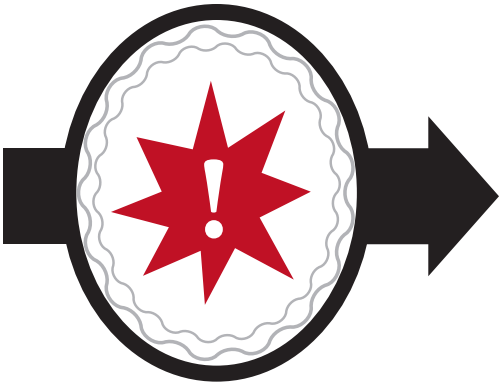
EventTracker integration with top-of-the-line threat intelligence feeds quickly detects and alerts on unknown processes or low reputation endpoints interacting with assets inside the enterprise network. Rapidly refined internal whitelisting is used to reduce false positives. Correlation of unknown processes interacting with low reputation sites delivers pinpoint alerts.

EventTracker Endpoint Protection detects insertion/removal of unauthorized mass storage devices including USB sticks and writable CD/DVDs. Log all activity or block access per policy.

Risk prioritized alerts – when properly tuned provide excellent, low noise notification of ongoing attacks.

After an attack

Scope. Contain. Remediate.



Perfect protection is not practical. Therefore monitoring is necessary to determine the scope of the damage, contain the event, remediate, and return operations back to normal.

Explore log data with fast indexed search and endless refine. Drill by log source, time, smart tokens, and patterns in description or a combination to quickly get to the bottom. Export data to the datamart for deep dives.

Built in Incident Handlers Handbook based on a model from SANS. Quickly record all actions taken and results from forensic analysis in a central location. Send results via email and/or export to Excel.