DEFENSESTORM
THE BEST OFFENSE.

DefenseStorm Endpoint Detection and Response (EDR)

As an additional service, DefenseStorm offers EDR which provides an additional layer of cybersecurity protection as a co-managed service. The GRID platform already provides continuous data collection from all systems and solutions, and DefenseStorm EDR builds on that to provide additional capabilities for our TRAC team to help keep you safe and sound. GRID and TRAC continuously analyze all this data looking for threats. Our TRAC team uses a mix of technology and expertise to monitor your event data to provide early identification of threats while using DefenseStorm EDR to rapidly block unwanted applications and/or quarantine machines.

Why DefenseStorm EDR?

- More robust protection against Ransomware related attacks.
- Deployment time in as little as 24 hours from the time your instance is established with the guidance of DefenseStorm's EDR Team.
- Research suggests that EDR tools can take teams as long as 18 months to become proficient in use. DefenseStorm's EDR Team provides a dedicated group of individuals to guide you through installation, setup, and training to potentially drastically increase time to value.
- Through the guidance of DefenseStorm's EDR team, financial institutions have the ability to create custom policies to strengthen your existing security posture to protect against threats not easily visible to other security tools.
- Gives the TRAC team the ability to quarantine machines remotely; rapidly responding to potential cybersecurity threats on your behalf
- TRAC triages the initial alert saving teams minutes to hours of investigation on potential non-threat related incidents to reduce alert fatigue on your existing team while also providing guidance on policy and whitelisting recommendations to keep environments running more smoothly.
- DefenseStorm EDR's features, benefits, and additional capabilities are: Collection, Detection, Containment, and Predictive Modeling.

DEFENSESTORM
THE BEST OFFENSE.

DefenseStorm Endpoint Detectionand Response (EDR)

Collection:

- GRID already provides continuous data collection from all systems and solutions, even when offline
- DefenseStorm EDR provides additional data on potential threats detected from your EDR Cloud Console and puts them all under one pane of glass through GRID.

Detection:

- DefenseStorms EDR provides robust ransomware prevention capabilities. Using behavioral analytics, we can detect and prevent behaviors associated with ransomware. Those behaviors include detecting/preventing access of the main boot record, modification of volume shadow copies, and the encryption of data.
- Additionally, alongside the Carbon Black agent Carbon Black deploys canary/decoy files to track and stop processes attempting to encrypt, modify or delete our files further hardening your systems against Ransomware attempts.
- GRID uses specific EDR based triggers to detect and alert on the above and additional data being sent from your EDR cloud console and is further enhanced by your already in place GRID monitoring and alerting.
- DefenseStorm EDR performs a low-resource consumption one-time scan on installation to take inventory and detect pre-existing malicious items. After this one-time scan our EDR looks at events as they occur in real-time, essentially always scanning for threats.

Containment:

- Policies allow for automatic blocking or quarantining of malware or other unwanted applications
- Allows the TRAC team to remotely quarantine a server or workstation
- Quarantine infected systems to prevent lateral movement while still allowing you to actively investigate, collect, and analyze data from the compromised system while impacting your network or other devices.

DEFENSESTORM
THE BEST OFFENSE.

DefenseStorm Endpoint Detection and Response (EDR)

Predictive Modeling:

- Next Gen Anti-Virus (NGAV) that can complement/replace your existing anti-virus solution
- DefenseStorm EDR continuously analyzes your endpoints for attacker behavior
- Protects against cyber-threats, anomalous behaviors, ile-less malware, or other deeply buried indicators of compromise

Additional Endpoint Capabilities:

- Allow admins to push/download files or remove malicious applications
- Allow for interactive attack chain/process visualization and containment
- Give customer admins command line access to the quarantined device
- Preserve forensic evidence
- Control access to USB devices
- Enforce policies on endpoints even when disconnected from your network