DEFENSESTORM
THE BEST OFFENSE.

DefenseStorm Endpoint Detection and Response (EDR)

Continuous analysis of endpoints to protect against threat actors.

Financial institutions need to stay ahead of threat actors, and protecting the endpoints is a must for comprehensive protection of your data and customers' information. With EDR protection, you can stay stop the advancement of attacks, have better threat visibility, and protect your organization against new and emerging ransomware attacks.

Why DefenseStorm EDR?

DefenseStorm offers two EDR options, Carbon Black or CrowdStrike, to provide an additional layer of cybersecurity protection as a co-managed service. Combined with GRID Active Threat Surveillance and supported by our CTS Ops (Cyber Threat Surveillance Operations) Team to better monitor, mitigate and minimize threats, DefenseStorm continuously analyze all endpoint data looking for threats.

Our CTS Ops 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.

DefenseStorm EDR is integrated with GRID Active, our intelligent data platform and GRID Active Threat Surveillance, which consolidates cybersecurity data for real-time visibility into your cyber risk and includes capabilities focused on the following: Collection, Detection, Containment, and Predictive Modeling.

COLLECTION

- GRID Active 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.

Endpoint Detection and Response

FEATURES

- **Robust protection against Ransomware related attacks.**
- **Fast deployment with guidance from the DefenseStorm EDR Team.**
- **Strengthen your security posture with custom policy creation.**
- **Rapidly respond to threats with remote machine quarantine capabilities.**
- **Focus on threats that matter through CTS Ops team triage of alerts.**

BENEFITS

- **Stops current and future ransomware variants.**
- **Become more proficient in understanding threats and strengthen protection.**
- **Protection against threats not easily visible to other security tool through integrated platform.**
- **Rapidly respond to threats and stop the advancement of the attack.**
- **Reduce alert fatigue and keep environments running more smoothly.**

DEFENSESTORM
THE BEST OFFENSE.

DefenseStorm Endpoint Detection and Response (EDR)

Additional data on potential threats is detected and integrated through GRID Active.

DETECTION

DefenseStorm's EDR provides robust ransomware prevention capabilities through use of behavioral analytics, to detect and prevent behaviors associated with ransomware.

- Combined with the Carbon Black agent canary/ decoy files are deployed to track and stop processes attempting to encrypt, modify or delete files to further harden your systems against Ransomware attempts.
- Enhanced monitoring and alerting through GRID Active.
- DefenseStorm EDR performs a low-resource consumption one-time scan on installation to take inventory and detect pre-existing malicious items and continues to scan for threats in real time.

CONTAINMENT

- Established policies allow for automatic blocking or quarantining of malware.
- Prevent lateral movement.
- Actively investigate, collect and analyze data from compromised system without impacting the network or other devices.

PREDICTIVE MODELING

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

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. Included with Carbon Black and at an additional cost with CrowdStrike.
- Enforce policies on endpoints even when disconnected from your network
- CrowdStrike allows end-users and administrators to perform on-demand scans