Clarity

EDR

Endpoint Detection and Response

FULLY MANAGED ENDPOINT PROTECTION

Clarity provides fully managed endpoint protection backed by our 24/7 U.S. based SOC. We are able to automatically isolate and prevent attacks, drive centralized hunting and detection, and enable interactive response. Our SOC + Endpoint Protection (EDR) helps to extend our monitoring of the cloud, network, and devices by providing an additional layer of security for endpoints. With this layer of protection, we offer you the peace of mind you need, so you can rest easy.

UNIFIED PROTECTION, DETECTION, AND GUIDED REMEDIATION

Enhanced Visibility

Clarity monitors your environment with kernel-level data collection and purpose-built dashboards. In turn, you get to your threat intelligence data quicker.

Magnified Detection

We generate useful alerts by continuously correlating host activity with other environmental data. Clarity's platform is customized for you by preparing for threats unique to your industry or environment.

Rapid Response

When your security is on the line, you can't afford to react slow. Our analysts are empowered with detailed data from across your endpoints allowing them to respond to threats quickly.

PREVENT RANSOMWARE & MALWARE, WHILE DETECTING ADVANCED THREATS

Prevent

Secure Windows, macOS, and Linux systems. Stop ransomware before data is encrypted, and block malware. Disrupt advanced threats with behavior-based prevention. Leverage integrated threat intelligence from Recorded Future and Anomali.

Correlate

Collect data from every major OS — including cloud workloads — all the way down to the kernel and glean host insights.

Respond

Empowers our analysts with rich host data, relevant threat intelligence, interactive visualizations for investigations. Accelerate remediation with remote response actions like host isolation. Connect workflows with Clarity's orchestration tools.