CyberProof®
A UST Company

MANAGED ENDPOINT DETECTION & RESPONSE (MEDR)

PROACTIVELY DETECT AND RESPOND TO THREATS AT THE ENDPOINT AND HUNT FOR THOSE ALREADY IN YOUR NETWORK

Cyber attackers are targeting endpoints to compromise users and directly access systems such as cloud workloads, applications and IoT environments. This requires 24x7 monitoring of your endpoints led by skilled analysts on-hand to actively hunt, investigate and contain validated threats before they impact your business.

WE'LL CHASE THE ALERTS AND HELP REMEDIATE THE INCIDENTS

Challenge - Managing endpoint alerts can be overwhelming if you don't know what to do with the volume of in-depth information, such as process data, registry keys and memory activity.

Our Solution - We'll take care of alerts 24x7, triaging and investigating them under the context of a single incident. We'll then collaborate with you via real-time ChatOps in our service platform to remediate the incident.

HUNT FOR THREATS THAT HAVE SLIPPED THROUGH THE CRACKS

Challenge - Attackers will find a way to get through, but SOC analysts don't have the time or often the training to hunt across large datasets and identify previously unknown attacker activity.

Our Solution - Our dedicated Threat Hunting team supports our SOC analysts by proactively searching for adversaries that slipped past your endpoint security controls. They go beyond basic methods such as retro-hunting on known IOCs to include incident-based, intelligence-based, and behavioral analysis procedures.

REDUCE DWELL TIME AND REALIZE VALUE QUICKLY

Challenge - As your infrastructure changes and attacker techniques evolve, so must your endpoint security policies, detection rules and response procedures. But time spent on this means less time detecting and responding to daily threats.

Our Solution - We use our curated library of detection and response use cases, continuously updated by our EDR engineers, threat intelligence analysts and incident responders, to reduce dwell time quickly and continuously tune detection rules, policies, incident playbooks and reporting.

WHAT'S INCLUDED?

- **CyberProof Defense Center (CDC) Platform -** acts as the single interface for SOC activities with real-time ChatOps for collaborating with our analysts. Our virtual analyst, SeeMo, provides timely insights and automates repetitive tasks such as alert triage, enrichment and investigations
- **Behavioral Analysis and Automation -** to correlate and enrich data from across all endpoints in real-time, associating multiple alerts to a single incident and speeding up detection and response
- **24x7 Security Monitoring -** round-the-clock security alert monitoring, enrichment and triage
- **Managed Response -** incident investigation, issue prioritization and customized response activities such as threat containment, remediation and assistance with recovery
- **Agile Use Case Management -** continuously optimized threat detection rules, playbooks, enrichment integrations, automated responses and reporting
- **Leading EDR technology -** support for all leading EDR technologies and the ability to design, deploy, configure and manage legacy and greenfield deployments

CYBERPROOF DEFENSE CENTER (CDC) PLATFORM

SINGLE INTERFACE view of SOC activities

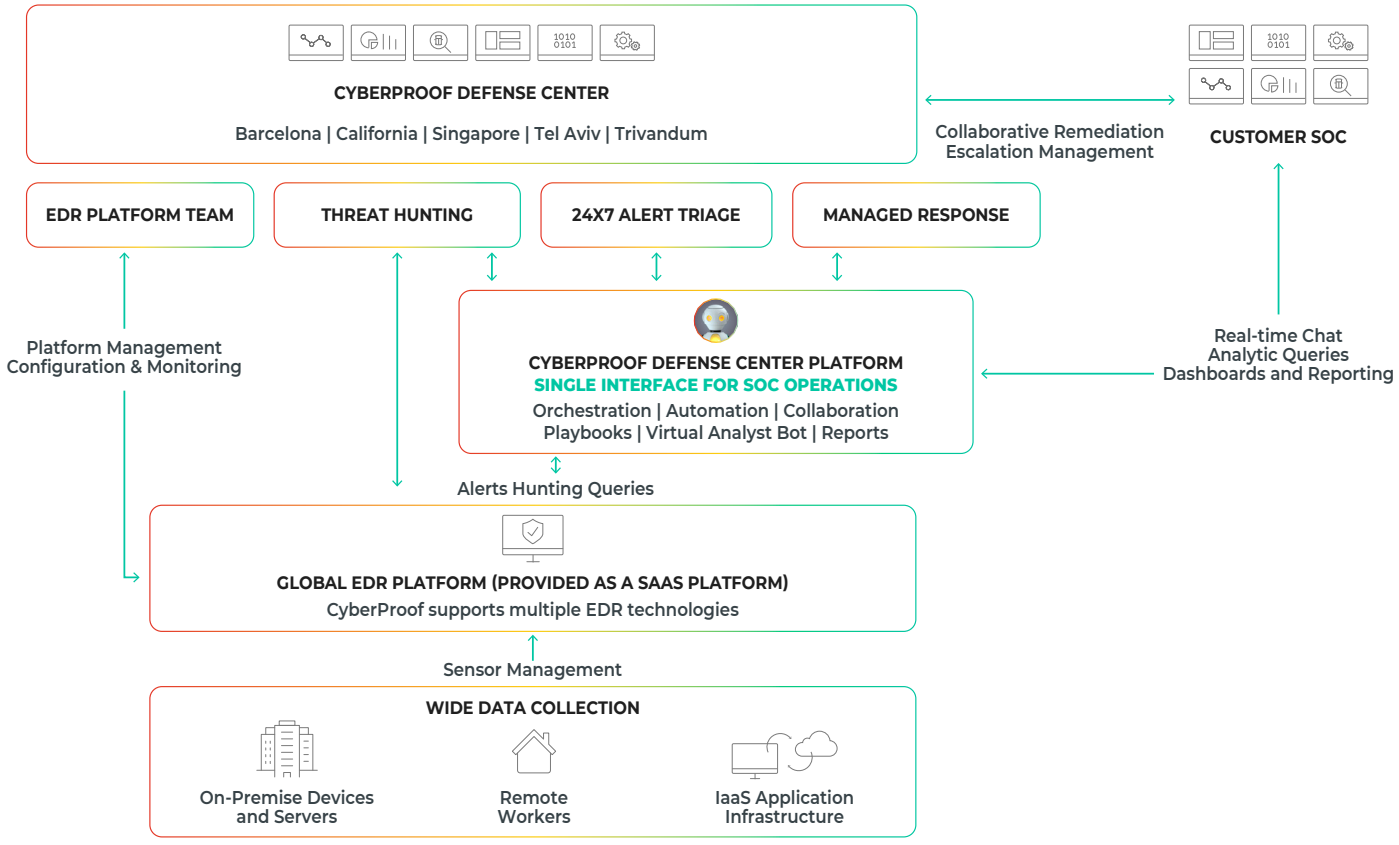
CUSTOMIZED REPORTING to measure tailored KPIs and summarize EDR incident handling

ORCHESTRATION to integrate with various sources and technologies

SEEMO, OUR VIRTUAL ANALYST automates previously manual analyst tasks and provides wider context to alerts

CHATOPS COLLBORATION to communicate with stakeholders and our teams in real-time

SERVICE ARCHITECTURE



WHY CYBERPROOF?

Independently Recognized Leader – MDR Award Winner and Recognized as 'Leader' by Forrester in the Midsize Managed Security Services Market

SeeMo, Your Virtual Analyst Bot – SeeMo acts as a virtual member of your team to automate L1+L2 SOC activities and significantly reduce human effort

CDC Platform Provides Transparency and Collaboration – Our platform provides a collaborative environment with real-time ChatOps to coordinate between internal and external teams and maintain complete transparency into security operations

Bring Your Own EDR Technology or Leverage Our Partnerships – We can integrate with your existing EDR technology investments or provide you with our recommendations based on your unique requirements

Dedicated Threat Hunting – Our dedicated Threat Hunting team use advanced techniques to uncover threats that may have been missed

Continuous Improvement – We use our curated library of threat detection and response content to continuously configure and tune customized detection rules and policies to your endpoints - improving your security posture

ABOUT CYBERPROOF

CyberProof is a security services company that helps organizations to intelligently manage incident detection and response. Our advanced cyber defense platform enables operational efficiency with complete transparency to dramatically reduce the cost and time needed to respond to security threats and minimize business impact. SeeMo, our virtual analyst, together with our experts and your team automates and accelerates cyber operations by learning and adapting from endless sources of data and responds to requests by providing context and actionable information. This allows our nation-state cyber experts to prioritize the most urgent incidents and proactively identify and respond to potential threats. We collaborate with our global clients, academia and the tech ecosystem to continuously advance the art of cyber defense.
For more information, see: www.cyberproof.com

LOCATIONS

Barcelona | California | London | Paris | Singapore | Tel Aviv | Trivandrum