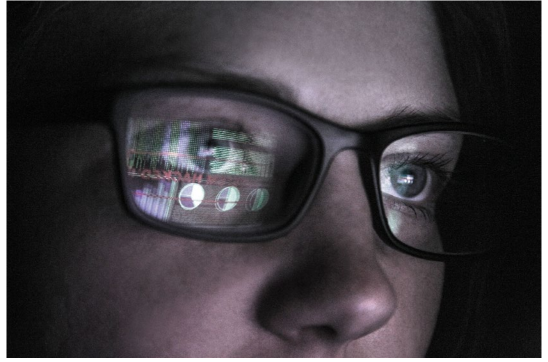
Cytellix Endpoint Detection & Response

CYTELLIX

"In addition, ideal EDR solutions should enable enterprises and smaller organizations to deploy a single solution that also protects against attacks and allows the collection and analysis of log and configuration data."- Gartner, Emerging Technologies: Critical Insights for Endpoint Detection and Response, Author Rustam Malik, 4/20/21 GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.



REAL SECURITY

01
CYBERSECURITY IS A BUSINESS DECISION

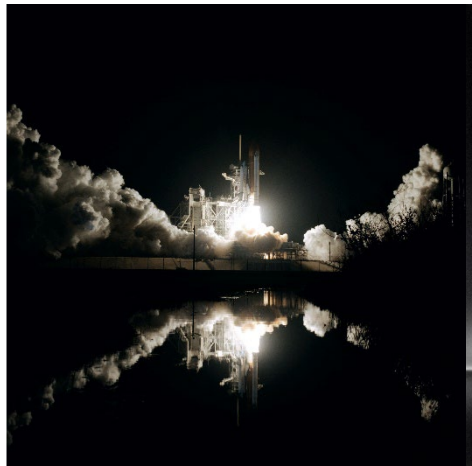
Cybersecurity platforms that leverage EDR and provide visibility of users, devices, applications with near real-time notification and containment capabilities are the basis for company security advancement and business justification.

Cytellix® has over two decades of experience providing cybersecurity for some of the largest networks in the world. We have observed many companies investing in manpower and security tools rather than cost effective solutions with business outcomes. The Cytellix SaaS platform can save 75% of DIY.

To address cybersecurity outcomes as a business decision, Cytellix built and delivers a patented turnkey cybersecurity risk management platform rooted in cyber-frameworks. Overwhelming response from our customers in our SaaS demo's: "*Thank you, I have been looking for a comprehensive platform that does what Cytellix does*".

02
HOW WE'RE DIFFERENT

Cytellix® is a first-of-its kind SaaS platform that brings together practical cybersecurity, cyber-compliance, and risk management under one umbrella. We know your "real security posture" and can provide a new way to manage and deploy cybersecurity capabilities, risk awareness, and compliance with a plan tailored to your specific situation and needs.



03
Endpoint Detection & Response (EDR)

MITRE ATT&CK Framework: Endpoint Detection and Response techniques now align themselves with the MITRE ATT&CK Framework to map detections and possible remediations back to the controls a best practice to mitigate the most advanced attacks. Cytellix uses these techniques in our identify, detect and containment capabilities 24x7x365.

Cytellix Endpoint Detection & Response (C-EDR) is a flexible solution that can be used standalone, enables bring-your-own-license or can be provided turnkey as a complete managed solution with our GRC, MDR, XDR, SOC managed Turnkey Solutions.

Extended Detection & Response (XDR) Extending the EDR capabilities to XDR/MDR with Cytellix correlation of endpoints, user accounts and behaviors into an early detection and containment solution.

Industry Requirements	Cytellix Endpoint Detection & Response (C-EDR)
○ Prevention	√ Signatures, machine-learning, Industry Framework Support (NIST, ISO, GDPR, SEC, PCI), Prevents: Ransomware malware and non-malware attacks,
○ Endpoint Detection Response	√ Always on, real-time event recording; File execution, file modification, network connections, executed binary, registry modifications & memory injections.
○ Simplified Operations	√ Simplified telemetry using common tactics, techniques and procedures
○ Incident response	√ Process kill features, with secure shell for online or offline remote remediation.
○ Data Retention	√ Data retention to meet regulatory obligations and forensic requirements
○ Automated Detection & Threat Intelligence	√ Leverages automated detection techniques using MITRE ATT&CK detections
○ Vulnerability identification on Endpoints	√ Endpoint risk assessment of vulnerabilities used in exploits
○ Platform integration through API's	√ Native integrations with most SIEM's (C-SIEM supported) for more advanced correlation and MDR/XDR requirements

We are Real Security.
We are Cytellix.

Contact our cyber experts
info@cytellix.com to learn more.

04 OUR FLAGSHIP CCWP™, ECOSYSTEM OF SOLUTIONS

Cytellix® Cyber Watch Portal (CCWP)
A patented graphical dashboard presenting GRC, XDR, MDR, EDR and SOAR in an integrated, automated single pane of glass. Delivered as managed Turnkey or Bring-Your-Own-License (BYOL)

Complete Real-time Visibility
Real-time detection, visibility, and awareness into every device and connection—known or unknown—in a dynamic infrastructure to optimize system health and mitigate risk.

Vulnerability Assessments
Patented, Advanced vulnerability identification of infrastructure risks and leverage findings in threat detection and response.

Executive Cytellix Cyber Watch Portal (E-CCWP™)
A patented, hierarchical view of cyber posture at any level of relationship, including parent organization, subordinate organizations, or subsidiaries. Enables monitoring of organizations that may be linked to a supply chain for full visibility of aggregated or single entity cybersecurity posture status.

Cytellix System Information Event Management (C-SIEM™)
Aggregate and analyze every event from any security product end points in real time to support early detection of cyber-attacks, malware, phishing, data breaches, incident response, forensics, and tuned for cybersecurity frameworks meeting regulatory compliance business requirements.

Cytellix Endpoint Detection & Response (C-EDR™)
Endpoint protection and responses of malware and ransomware at every stage of an attack. Advanced capabilities to uncover advanced threats and minimize dwell time. Isolation of infected systems and removal of malicious files to prevent movement. Full integration with CCWP, C-SIEM and GRC/IRM Solutions.

Security Operations Center (SOC)
US-based 24x7x365 monitoring, detection, and response service leverages data from the CCWP and customer provided solutions that can enable immediate mitigation strategies and actions.

Cyber Status
Patented technology that compiles information from the vulnerability's Governance, Risk, and Compliance assessments, data, analytics. Delivered in real-time analysis, including continuous improvement visualization and scorecard.

Cytellix Governance, Risk and Compliance Solutions (C-GRC™/IRM)
An automated and complete physical, logical, and digital assessment utilizing standards-based cybersecurity frameworks for policies, standards, procedures, Plan of Actions & Milestones, and System Security Plans. Capturing risk, data leakage, identifying third-party risks, rating vulnerabilities by severity, applying guidance for policy compliance to industry standard cyber frameworks while leveraging AI/ML automation for immediate reporting and risk scoring.

Threat Hunting and Cyber Analytics
Patent Pending 24x7x365 cyber monitoring and correlated threat intelligence integrated with third-party data streams including enterprise indexed metadata to detect IOC's using AI/ML to provide security intelligence, analysis, and actionable insights for faster remediation.

Cytellix Platform Security Manager (C-PSM™)
Support automated change management workflows, policy management and continuous assessment of network device security enforcement to ensure protection of critical IT assets, optimize performance, manage change, and prioritize risk mitigation.

www.cytellix.com
info@cytellix.com
949-328-6347