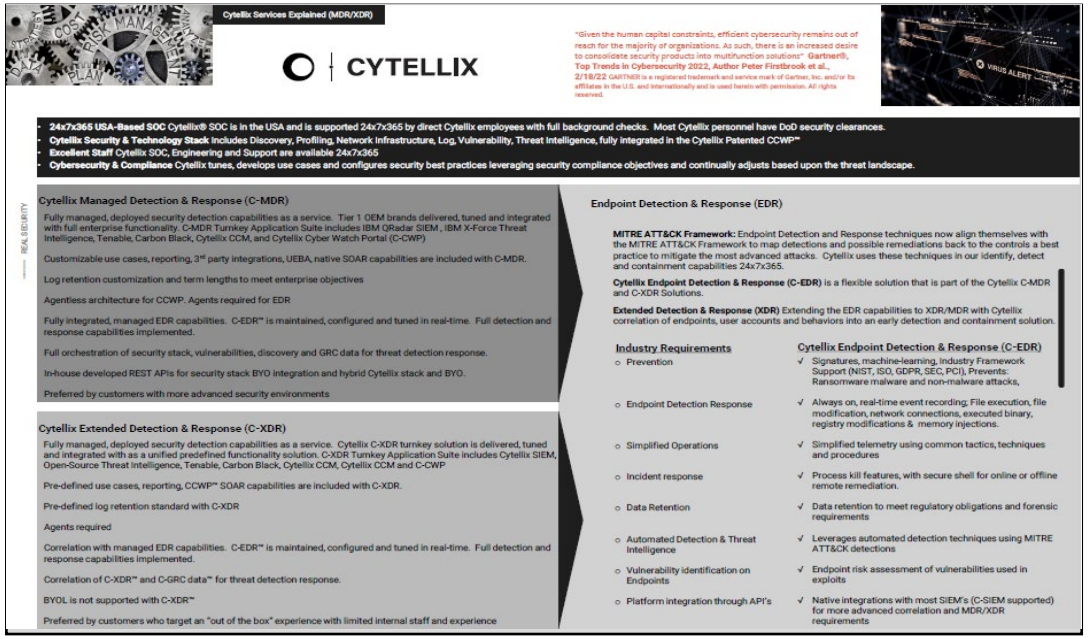
CYTELLIX

Cytellix Services Explained (MDR/XDR)



carahsoft

For more information, contact Carahsoft or our reseller partners:
Cytellix@carahsoft.com | 866-662-2724

CYTELLIX

Thank you for downloading this Cytellix brief. Carahsoft is the trusted provider for Cytellix Cybersecurity solutions.

To learn how to take the next step toward acquiring Cytellix's solutions, please check out the following resources and information:

For additional resources:
Carah.io/CytellixResources

For additional Cytellix solutions:
carah.io/CytellixSolutions

To purchase, check out the contract vehicles available for procurement:
carah.io/CytellixContracts

For upcoming events:
carah.io/CytellixEvents

For additional Cyber solutions:
carah.io/Cybersecurity

To set up a meeting:
Cytellix@carahsoft.com or 888-662-2724

Cytellix Services Explained (MDR/XDR)

CYTELLIX

"Given the human capital constraints, efficient cybersecurity remains out of reach for the majority of organizations. As such, there is an increased desire to consolidate security products into multifunction solutions" **Gartner®, Top Trends in Cybersecurity 2022, Author Peter Firstbrook et al., 2/18/22** 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.

- **24x7x365 USA-Based SOC** Cytellix® SOC is in the USA and is supported 24x7x365 by direct Cytellix employees with full background checks. Most Cytellix personnel have DoD security clearances.
- **Cytellix Security & Technology Stack** Includes Discovery, Profiling, Network Infrastructure, Log, Vulnerability, Threat Intelligence, fully integrated in the Cytellix Patented CCWP™
- **Excellent Staff** Cytellix SOC, Engineering and Support are available 24x7x365
- **Cybersecurity & Compliance** Cytellix tunes, develops use cases and configures security best practices leveraging security compliance objectives and continually adjusts based upon the threat landscape.

REAL SECURITY

Cytellix Managed Detection & Response (C-MDR)

Fully managed, deployed security detection capabilities as a service. Tier 1 OEM brands delivered, tuned and integrated with full enterprise functionality. C-MDR Turnkey Application Suite includes IBM QRadar SIEM , IBM X-Force Threat Intelligence, Tenable, Carbon Black, Cytellix CCM, and Cytellix Cyber Watch Portal (C-CWP)

Customizable use cases, reporting, 3rd party integrations, UEBA, native SOAR capabilities are included with C-MDR.

Log retention customization and term lengths to meet enterprise objectives

Agentless architecture for CCWP. Agents required for EDR

Fully integrated, managed EDR capabilities. C-EDR™ is maintained, configured and tuned in real-time. Full detection and response capabilities implemented.

Full orchestration of security stack, vulnerabilities, discovery and GRC data for threat detection response.

In-house developed REST APIs for security stack BYO integration and hybrid Cytellix stack and BYO.

Preferred by customers with more advanced security environments

Cytellix Extended Detection & Response (C-XDR)

Fully managed, deployed security detection capabilities as a service. Cytellix C-XDR turnkey solution is delivered, tuned and integrated with as a unified predefined functionality solution. C-XDR Turnkey Application Suite includes Cytellix SIEM, Open-Source Threat Intelligence, Tenable, Carbon Black, Cytellix CCM, Cytellix CCM and C-CWP

Pre-defined use cases, reporting, CCWP™ SOAR capabilities are included with C-XDR.

Pre-defined log retention standard with C-XDR

Agents required

Correlation with managed EDR capabilities. C-EDR™ is maintained, configured and tuned in real-time. Full detection and response capabilities implemented.

Correlation of C-XDR™ and C-GRC data™ for threat detection response.

BYOL is not supported with C-XDR™

Preferred by customers who target an "out of the box" experience with limited internal staff and experience

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 is part of the Cytellix C-MDR and C-XDR 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.

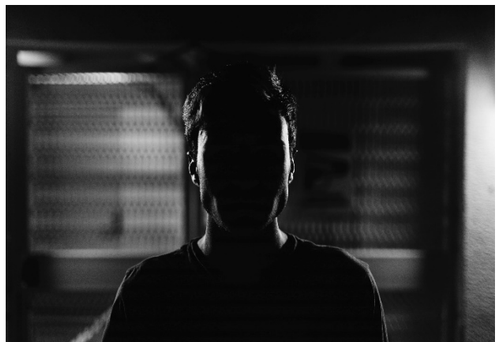
Vulnerability Assessments
Patented, Advanced vulnerability identification of infrastructure risks and leverage findings in threat detection and response.

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.

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



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.