XCITIUM COMPLETE

COMPREHENSIVE M(XDR) SECURITY

PROTECTING BUSINESS ECOSYSTEMS AT MACHINE SPEED WHILE CONNECTING AND SECURING THE DOTS BETWEEN ENDPOINTS, CLOUDS & NETWORKS

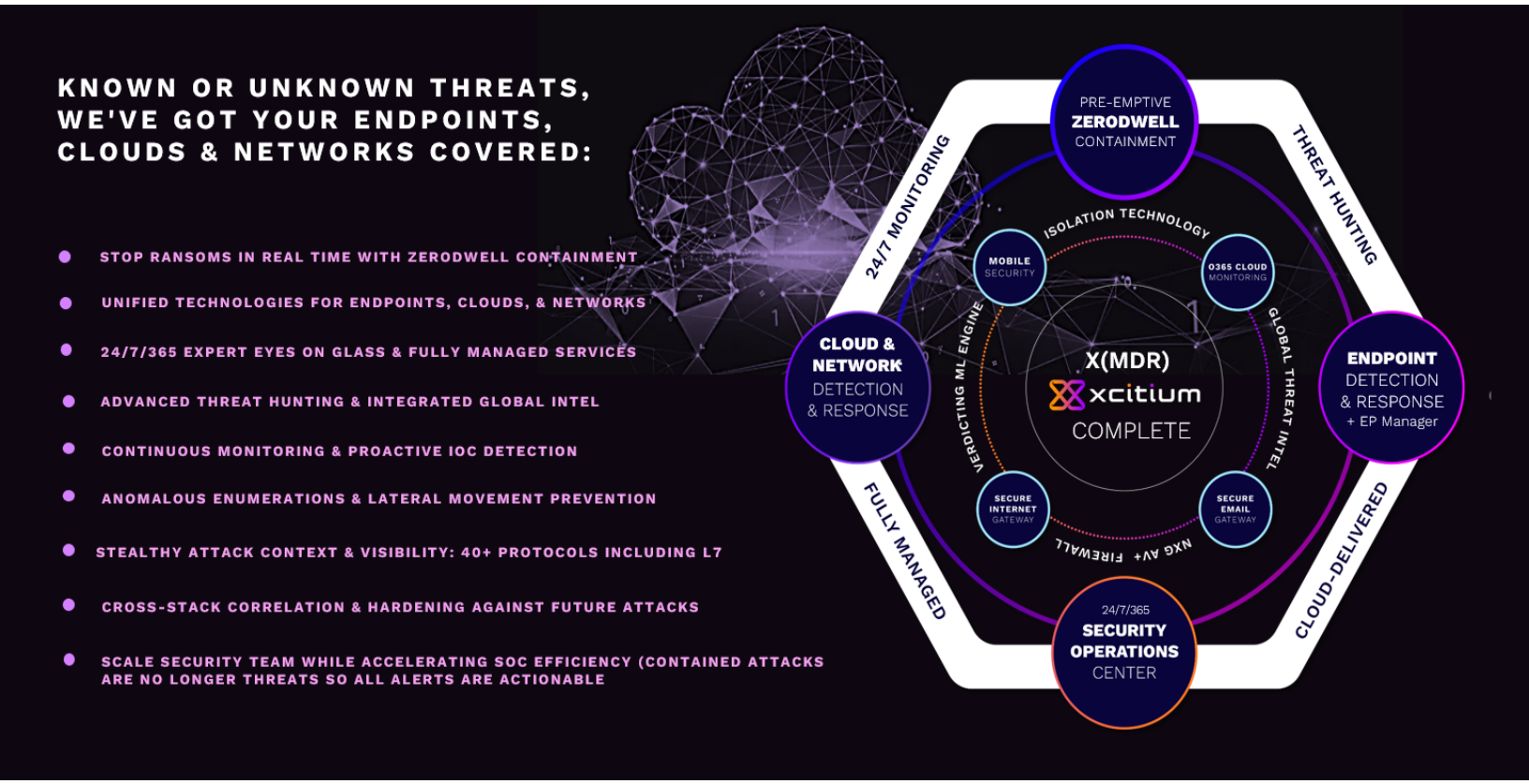
WHAT IS XCITIUM COMPLETE?

Threat landscapes are ever-evolving. Defenders must stay several steps ahead of rapid-fire attackers while continuing to innnovate products, manage business operations, conquer the competition, accommodate remote workers, and provide security to endpoints, networks, and cloud infrastructures.

Meanwhile, ransomware attacks are on the rise, data breaches and IP theft is rampant and continuous, and defeated SOC teams industry wide are dealing with alert and staff fatigue at unprecedented levels. With massive increases in the volume and variety of attacks, everyone is asking whether today's detection-first cybersecurity approaches actually work. Who needs yet another M(XDR) detection product?

ENTERPRISES NEED XCITIUM COMPLETE M(XDR) BECAUSE WE NEVER TRUST, ALWAYS VERIFY

Xcitium's COMPLETE M(XDR) is an impotant paradigm shift. It is a uniquely differentiated MXDR service for endpoints, clouds, and networks that includes machine-speed ZeroDwell Containment across all the data points and vectors traversed by bad actors. MXDR extends across endpoints to continuously monitor, manage, and connect the dots across your entire technology stack. Our Kernel-level ZeroDwell virtualization is a pre-emptive prevention technology that precedes detection and response by containing Unknowns and potential attacks at runtime. This zero trust approach protects endpoints proactively while setting the groundwork for MXDR as a critical next step for offensively protecting, monitoring, securing, hardening and responding to known and unknown objects and future threats, including the deployment of advanced threat hunting at every level of your digital ecosystem —all from a single, unified platform. With automated containment as the innovative zero trust technology that distinguishes Xcitium from the glut of detection-first vendors in the marketplace, you receive only actionable alerts that accelerate the security team's ability to provide active responses via 24x7x365 managed SOC operations, because contained attacks are no longer threats.



XCITIUM COMPLETE M(XDR) ADVANTAGES

XCITIUM COMPLETE M(XDR) is a comprehensive service that combines the capabilities of Xcitium's patented ZeroDwell Containment technology + all of the holistic, multi-layered capabilities of Xcitium Managed MDR + Xcitium M(XDR)'s advanced visibility, context, corrrelation, and **security ecosystem and data lake integration** woven together by automated AI and advanced machine learning capabilities. The key to any managed-XDR system is integraiton across an organization's security technology stack..

Xcitium MXDR's comprehensive integration and extensive visibility&context produces uniquely differentiated advantages:

- A siingle platform providing deep insight into stealth attacks that aid and accelerate the SOC team's abiility to step ahead of threat actors and harden against future attacks.
- Zero malware and ransomware dwell time, courtesy of Xcitium ZeroDwell Containment techology (this means contained attacks cannot dwell in, move laterally, or cause damage as a result of Xcitium's default virtualization of all unknowns at runtime).
- Rapid attack mitigation and vulnerability management, backed by advanced AI and ML with out-of-the-box security stack prevention and attack correlations. that lead to tremendously improved ROII for your business.
- Straightforward configuration, deploy,ment, and maintenance so you don't need additional staff to manage your security operations; we do all the heavy lifting for you.

M(XDR) INTEGRATIONS

GLOBAL THREAT INTL

ENDPOINTS

NETWORKS

CLOUDS

INTERNET | EMAIL GWs

APPLICATIONS

ZERO TRUST

M(XDR) SOLUTIONS

- 24/7/365 Eyes on Glass Alerting
- Weekly/Monthly Reporting
- Profile & Policy Management
- Pro-Active Threat Hunting & GLobal Threat Intel
- ZeroDwell Containment for Endpoints, Cloud & Network
- Human-Led Expert Incident Response / Forensics
- Live Remediation Support
- Monthly Security Meetings
- Security Ecosystem Integration
- Convergence of network security services & Zero Trust
- Network Monitoring:
  - NetworkLogTrafficVisibility (NTBA)
  - Intrusion Detection (IDS)
  - Additional Log Ingestion
  - Windows Event Logs
  - Firewall Logs
  - Linux Server Logs
  - Custom Data Sources
- Cloud Monitoring:
  - O365
  - Azure AD
  - AWS CloudTrail

M(XDR) USE CASES

IMMEDIATE TIME TO VALUE & REDUCED TCO

OPERATIONAL EASE WITH RICH, BUILT-IN INTEGRATIONS ACROSS THE ENTIRE SECURITY TECH STACK PROVIDING DEEP VISIBILITY, REAL TIME CONTEXT, AND AUTOMATED CONTAINMENT, DETECTION AND RESPONSE. ONLY ACTIONABLE ALERTS/ NO ALERT FATIGUE. FULLY INTEGRATED PLATFORM MEANS SIGNIFICANT REDUCTION IN TOTAL COST OF OWNERSHIP.

IR & PROACTIVE THREAT HUNTING

24/7/365 EYES ON GLASS ALERTING AND INCIDENT RESPONSE + FORENSIC ANALYSIS. PROACTIVE THREAT HUNTING QUERIES AND BUILT-IN SIEM FOR LOG INGESTION. PROFILE & POLICY MANAGEMENT AND LIVE REMEDIATION SUPPORT.

GLOBAL THREAT INTELLIGENCE

XCITIUM VERDICT CLOUD INTEGRATION WITH OPEN-SOURCE FEEDS THAT LEVERAGE INTERNAL INTELLIGENCE PLUS 300+ BEHAVIORAL ALERTS. DETAILED KILL-CHAIN REPORTS & EMERGING THREAT REPORTING WITH WEEKLY / MONTHLY SUMMARIES.

STREAMLINED EFFICIENCY

INCREASED SOC PRODUCTIVITY – ONE PLATFORM & ONE WORFKFLOW. AUTOMATED FORENSIC COLLECTION AND BLOCKING ACTIVITY IN REAL-TIME. ATTACK ISOLATION AT ENDPOINT, NETWORK & CLOUD WITH KERNEL-LEVEL API VIRTUALIZATION. ENDPOINT MANAGEMENT WITH REMOTE ACCESS. MOBILE DEVICE MANAGEMENT AND INTEGRATION.

ZERO BREACHES. ZERO TRUST. ZERO DOWNTIME. ZERO DAMAGE.

WHY YOU NEED XCITIUM MXDR

01. **Containment-Powered Protection:** Security has never been a process of setting and forgetting. Now, attack intensity is increasing worldwide. It is more important than ever to protect first with ZeroDwell Containment, and then stay well ahead of attackers with managed detection, continuous monitoring, and expert attacker response strategies now that you are no longer burdened by alert fatigue.

02. **Evolving Threat Landscape:** Threats and attacks are continuously evolving and becoming more advanced, strategic and persistent. Ransomware attacks such as Nvidia and Toyota are just a few examples of notably-sized organizations that have suffered breaches. Without ZeroDwell Containment, organizations, regardless of size, are highly likely to experience a breach, and it is a matter of when, not if, it will happen.

03. **Limited Person-Power:** There are no shortcuts that can be taken to ensure an elevated level of dedicated security measures. You know your business and your customer better than anyone. Similarly, an MDR provider also knows its strengths in this line of business. With a lack of dedicated security expertise within your organization, partnering with an experienced XMDR provider is a must-have, not a nice to have.

04. **Time and Cost:** When deciding to develop and build an internal team for holistic security, or a committed team for incident response or threat hunting, the time and cost required can be prohibitive. By allowing you to focus on your business needs, Xcitium's dedicated XMDR solution allows you to focus your efforts entirely on analyzing events, conducting investigations, and observing round-the-clock monitoring.

05. **Critical business value:** With ZeroDwell protection coupled with a comprehensive, integrated XMDR solution that includes continuous monitoring and vulnerabilities guidance, organizations are able to conduct business at a level of comfort and security because their employees, IP, and infrastructure are managed expertly, and this posture helps to boost business productivity.

06. **Enrich attack forensics with integrated threat intelligence:** Xcitium Complete integrates threat intelligence with containment, telemetry, and proprietary detection sources to empower security teams with context-rich data and Indicators of Compromise (Ioc), including IP addresses, hashes, revealed vulnerabilities, and at-risk domains. This accelerates proactive forensics and triage capabilities.

BUSINESS REWARDS

- Proactive protection for endpoints, networks and clouds using Xcitium's ZeroDwell Containment automated virtualization technology to isolate all unknowns and reduce the attack surface.

- Real-time monitoring, alerting, aggregating and reporting of suspicious activity and telemetry sensor data for endpoints, networks, and clouds.. Gain real time automated ML and AI-built context and correlations.

- Security event alert management

- Endpoint management

- Incident response management and investigation to proactively reveal advanced attacks and stealth strategies.

- Dedicated Xcitium SOC IR expert analysts for accelerated analysis, forensics, and hardening against future threats.

- Managed proactive threat hunting capabilities to expose and pinpoint threats and attacker profiles.

- Advanced analytics highlighting file, user, application, and endpoint data.

- 24 x 7 SOC support through numerous geographical centers

ABOUT US

Xcitium, formerly known as Comodo Security Solutions, is used by more than 3,000 organizational customers & partners around the globe. Xcitium was founded with one simple goal – to put an end to cyber breaches. Our patented ZeroDwell technology uses Kernel-levle API Virtualization to isolate and remove threats like zero-day malware & ransomware before they cause any damage to any endpoints. ZeroDwell is the cornerstone of Xcitium's endpoint suite which includes pre-emptive endpoint containment, endpoint detection & response (EDR), and managed detection & response (MDR). Since inception, Xcitium has a track record of zero breaches when fully configured.

CONTACT

sales@xcitium.com • support@xcitium.com