
# XCITIUM MANAGED

WORRY-FREE MANAGED SECURITY
MDR SERVICE

# WHAT IS XCITIUM MANAGED?

Leading analyst firm Gartner defines Managed Detection and Response (MDR) as the process of providing real-time detection, analysis, investigations, and active response, all delivered remotely through a security operations center (SOC) on a 24x7x365 basis. When set up with precision, insights, and experience, MDR is a dynamic extension of your wider security posture.

**BUT NOT ALL MANAGED DETECTION AND RESPONSE SERVICES ARE BUILT THE SAME.** Xcitium's MANAGED product is a uniquely differentiated MDR service that provides a variety of supplementary benefits, including ZeroDwell Containment. Its Kernel-level 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 MDR as a critical next step for organizations with limited or almost no resources dedicated to offensively protecting, monitoring, securing, and responding to known and unknown objects (including advanced threat hunting).

### COMPLETE BREACH PREVENTION AND THREAT MANAGEMENT

Breach protection with patented ZeroDwell Containment technology is the world's only active breach prevention strategy employing true Zero Trust virtualization to stop ransomware, malware, and cyber-attacks from causing damage to your endpoints or business. This means you get pre-emptive protection of your endpoints and systems without having to rely on detection as the first line of defense, which is what everyone else does, and which is why breaches persist worldwide and attacks are accelerating. Xcitium Managed, however, focuses on threat hunting, attack engineering, environment monitoring, and vulnerability hardening, unburdened by alert fatigue and false positives. Only actionable alerts are raised by Xcitium products.

### REAL-TIME VISIBILITY, BEHAVIORAL ANALYSIS, AND FORENSICS

In-built endpoint detection and response-level forensics offer continuous visibility and insight into the applications and processes running in your environment. And Xcitium MDR services enable rapid detection and analysis of attacker enumerations and future threats before you become vulnerable, helping you gain a full understanding of the means, methods and root causes associated with suspicious and evolving malware.

## FOUR PILLARS OF XCITIUM MANAGED (MDR)

**HUNTING-ON-THE-GO.** Xcitium's dedicated team of highly-skilled security specialists hunt continuously for anomalies, suspicious activity, threat actor profiles and methodologies, and potential threats across your organization's endpoints, network, and cloud environments.

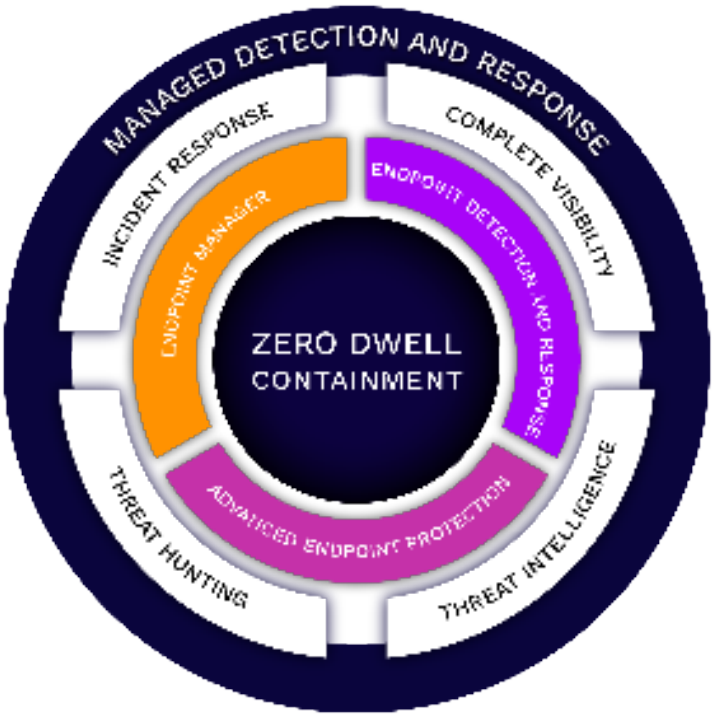
**INCIDENT RESPONSE.** Our MDR services leverage a team of expert forensic analysts working wiith real-time global intel from the Xcitium Threat Labs to respond to contained attacks and security policy violations by conducting in-depth investigations. You receive a detailed timeline of reports with analyses of artifacts such as MFT$, Windows Event Logs, Registry, Web History, etc so you can harden and defend against future attacks.

**FULL VISIBILITY WITH REAL-TIME ALERTING.** Routed to our state-of-the-art Xcitium Platform, triaged events, alerts, and harmful behavior from containment analysis are visualized, correlated, and addressed rapidly.

**UNIFICATION OF THREAT INTELLIGENCE.** We double-down on numerous internal and external threat intelligence feeds, providing wide coverage of global threat data that contributes to halts and alerts on Indicators of Compromise (IoC).

# HOW XCITIUM MANAGED [MDR] SERVICES WORK

This illustration highlights the tightly integrated nature of Xcitium MDR, combining appropriate technology, experts, and processes to provide comprehensive MDR advantages to mid-market enterprises at EDR-level prices.




**DEPLOY**

Become efficient and operational in hours from deployment of lightweight agents.

**DETECT**

Hunt and track down high priority threats, payloads, and signatures across the organization

**TRIAGE**

Tailor endpoint security rules and logic to understand and monitor risk severity and attack profiles while ZeroDwell Containment is preventing damage in real-time simultaneously.

**REMEDIATE**

Patented virtualized containment stops the damage, but our security experts need to clean up and match any loose issues to harden your endpoints, manage attack profiles, and prevent future attacks.

**REPORT**

Receive a detailed breakdown of every incident for compliance on a regular cadence to understand your environment and your new and enhanced managed security.

## WHY YOU NEED XCITIUM MDR

01. **Zero 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 MDR 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 MDR 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 MDR 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.

## BUSINESS BENEFITS

- Real-time monitoring and alerting for suspicious activity
- Proactive Endpoint Protection using our ZeroDwell Containment with Automated virtualization technology to isolate all unknowns and reduce the attack surface
- Real-time aggregation and correlation of telemetry sensor data for endpoints
- Security event / alert management
- Endpoint management
- Incident response management and investigation
- Leverage Xcitium's dedicated SOC IR analysts for responding to threats
- Managed advanced threat hunting capabilities to expose and pinpoint threats and attacker profiles
- Advanced analytics highlighting file, user, and endpoint data
- 24 x 7 SOC support through numerous geographical centers

## XCITIUM MANAGED ADVANTAGES

Xcitium MDR services provide a holistic, multi-layered approach to endpoint security that includes patented isolation technology to contain unknown files before they can do any harm. Our virtualization solution fully controls access to system resources -- preventing Unknowns and intruders from writing to the hard disk, com interface, and registry – which attackers need for file executions, persistence. and doing harm. This protection is significant for small to medium sized businesses which are attacked by the same threats as large enterprise but cannot afford access to the same defensive tools as these enterprise.For this reason, Xcitium's enterprise class security, with patented breach containment, is offered as fully managed MDR at EDR pricing.

## MANAGED MDR SERVICES: CAPABILITIES

### COMPLETE VISIBILITY

ZERODWELL CONTAINMENT | ENDPOINT DETECTION & RESPONSE TELEMETRY COLLECTION | NETWORK TRAFFIC VISIBILITY | 3RD PARTY DATA SOURCE INGESTION | ANOMALOUS BEHAVIOR & TRENDS | IDENTIFY ROOT CAUSE

### REAL TIME RESPONSE

AUTOMATE FORENSIC COLLECTION | BLOCK ACTIVITY IN REAL-TIME | ISOLATE ENDPOINT FROM NETWORK | EXECUTE CUSTOM COMMANDS | ENDPOINT & MOBILE DEVICE MANAGEMENT | REMOTE ACCESS | CUSTOM COMPLIANCE REPORTING

### IR & ADVANCED THREAT HUNTING

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

### GLOBAL THREAT INTELLIGENCE

XCITIUM VERDICT CLOUD | INTEGRATE WITH OPEN-SOURCE FEEDS | LEVERAGE INTERNAL INTELLIGENCE | 300+ BEHAVIORAL ALERTS | DETAILED KILL-CHAIN REPORTS | EMERGING THREAT REPORTING | WEEKLY / MONTHLY REPORTING

### OPTIONS FOR ADD-ON MANAGED XDR M(XDR): NETWORK & CLOUD MONITORING

NETWORK SENSOR: NETWORK LOG TRAFFIC VISIBILITY (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

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


## 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