xcitium

DATASHEET

ZeroThreat Complete X/MDR

WHAT IS ZEROTHREAT COMPLETE X/MDR?

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 extended ZeroThreat Complete X/MDR provides a variety of supplementary benefits, especially ZeroThreat virtualization as the pre-emptive prevention technology that precedes detection and response, so this level of X/MDR becomes critical for organizations with limited or almost no resources dedicated to proactively protecting, monitoring, securing, and responding (including threat hunting) for known and unknown objects.

COMPLETE BREACH PREVENTION AND THREAT MANAGEMENT

Breach protection with patented ZeroThreat Virtualization technology is the world's only active breach prevention strategy employing true Zero Trust virtualization that stops ransomware, malware, and cyber-attacks from causing any damage. This means you get absolute 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 and are accelerating. Once protected with ZeroThreat, your team can focus on threat hunting, attack engineering, environment monitoring and hardening because there is no more alert fatigue: contained attacks are no longer threats!

REAL-TIME FORENSICS AND BEHAVIORAL ANALYSIS

Proactive in-built endpoint detection and response-level forensics offers continuous visibility and insight into the applications and processes running in your environment. Enabling you to rapidly detect threats before they become vulnerable, reducing dwell time, and gaining a full understanding of the means, methods and root cause associated with suspicious activity and/or malware.

XCITIUM ZEROTHREAT X/MDR IS BUILT AROUND FOUR FOUNDATIONAL PILLARS.

HUNTING-ON-THE-GO. Xcitium's highly skilled team of security specialists are dedicated to continuously hunting for anomalies, suspicious activity and threats across your organization's endpoints, network, and cloud environments.

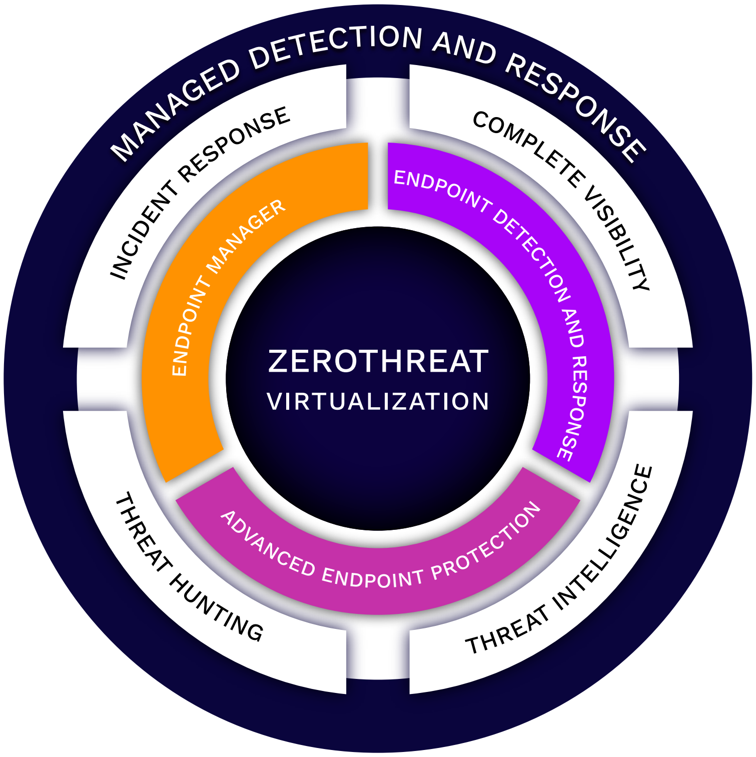
INCIDENT RESPONSE. Leverage a team of expert forensic analysts to conduct in-depth investigations. Receive a detailed timeline of attack activity with analyses of artifacts such as MFT$, Windows Event Logs, Registry, Web History, and so on.

FULL VISIBILITY WITH REAL-TIME ALERTING. Routed to our state-of-the-art Xcitium Platform, triaged events, alerts, and harmful behavior are presented and addressed quickly.

UNIFICATION OF THREAT INTELLIGENCE. 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 ZEROTHREAT COMPLETE X/MDR WORKS

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



■ **DEPLOY**

Become efficient and operational in hours from deployment

▼ **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 ZeroThreat containment is preventing any damage in real-time

▼ **REMEDIATE**

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

● **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 X/MDR

01. Zero Powered Protection: Security has never been a process of setting and forgetting. Now, attack intensity is increasing dramatically worldwide. So it is more important than ever to protect first with ZeroThreat Virtualization, 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. Growing Threat Landscape: Threats and attacks are continuously evolving and becoming more advanced, strategic and persistent. Ransomware attacks such as Colonial Pipeline and JBS Foods are just a few examples of notably-sized organizations that have suffered extortion. Organizations, regardless of size are highly likely to experience an attack or 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 buildi 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 X/MDR solution allows you to focus your efforts entirely on analyzing events, conducting investigations, and enacting round-the-clock monitoring.

05. Critical business value: With ZeroThreat protection coupled with an extended X/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 your business productivity.

BUSINESS BENEFITS

- Real-time monitoring and alerting for suspicious activity
- Advanced Endpoint Protection using our ZeroThreat Virtualization with Auto-Containment 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 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

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 ‘ZeroThreat’ technology uses Kernel-levle API Virtualization to isolate and remove threats like zero-day malware & ransomware before they cause any damage to any endpoints. ZeroThreat is the cornerstone of Xcitium’s endpoint suite which includes advanced endpoint protection (AEP), endpoint detection & response (EDR), and extended managed detection & response (X/MDR). Since inception, Xcitium has a track record of zero breaches when fully configured.

CONTACT

sales@xcitium.com • support@xcitium.com