XCITIUM GUIDED

AN MDR-LEVEL HIGH-FIDELITY ALERT TRIAGE & ANALYSIS SERVICE FOR ENDPOINTS

WHAT IS XCITIUM GUIDED?

Xcitium Guided adds MDR-level alert triage and analysis services to the Xcitium Advanced product at an extremely affordable price.

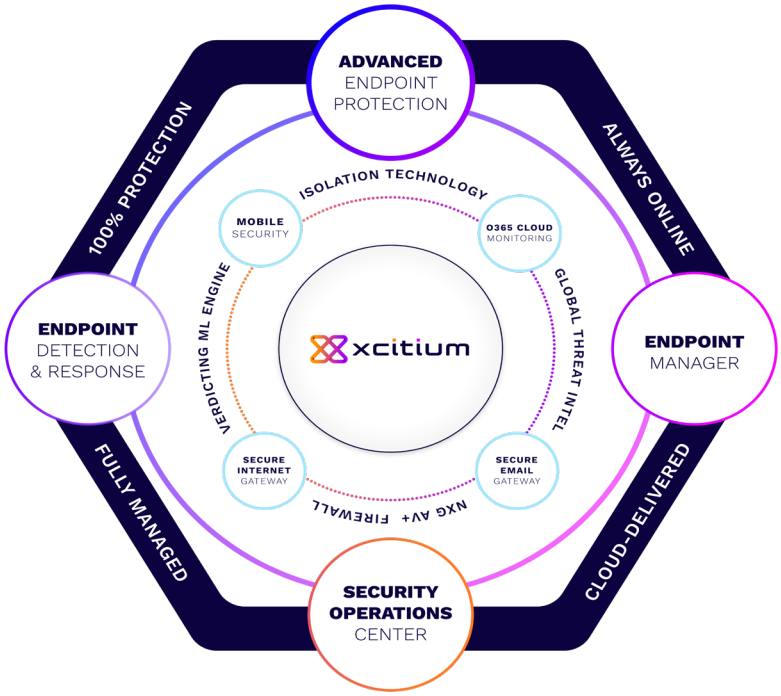
- **Benefit for Xcitium Advanced Customers**
  Xcitium Advanced customers can add the Xcitium Guided MDR-light triage service to their EDR deployment to gain triage and analysis support without needing to increase staff or security expertise. Xcitium takes on endpoint alert management and response activities for those not yet ready to upgrade to full MDR or extended MXDR endpoint | cloud | network services.

XCITIUM GUIDED EXPANDS EDR & ZERODWELL WITH 24-7-365 SOC EXPERTS' EYES ON GLASS

Xcitium's patented ZeroDwell Containment technology is the world's only detection-less breach prevention strategy using Zero Trust virtualization at runtime to stop unknown 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 every other security vendor does, and which is why breaches continue to occur worldwide. Xcitium employs detection-less virtualization as its first line of defense, and then also uses traditional detection techniques **in parallel** as part of continuous monitoring and threat management.

Xcitium Guided expands your Xcitium Advanced deployment to include our 24 x 7 x 365 SOC team's "expert eyes on glass" to manage security alerts for your enterprise. Alerts that are generated in the Xcitium customer console are also reviewed in the SecOps portal where security analysts investigate the attack and the adversarial progressions taking place in virtualization. They determine the threat's type and risk profile, and they monitor virtualization and quarantine operations to deterine if additional remediation is required. Guidance is provided to customers as well, including an assessment of the root cause of the attempted attack, with a ticket and notification sent to the customer outlining analyst recommendation(s).

.



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

XCITIUM GUIDED

CONTAIN THREATS IN REAL TIME, GAIN DEEP VISIBILTY & AN IMPROVED SECURITY POSTURE, & TRIAGE ALERTS TO PREVENT FUTURE ATTACKS

EDR monitoring is continuously collecting attack telemetry and anomalous endpoint events data and performing correlations in concert with the Xcitium Verdict Cloud, leveraging Xcitium Threat Laboratories intelligence as well as recommended security policy. The Verdict Cloud analyzes the contained unknown files that are safely virtualized on your endpoints, and returns a fast malicious/benign verdict while expert SOC triage efforts focus on real alerts, not alert fatigue.

With Xcitium Guided, you get actionable alerts based on customizable security policy that notify you about the actions of contained activity that could represent ransomware, memory exploits, PowerShell abuse, enumeration — specific attack attempts made by the contained threat plus many other adversarial IoCs. Alerts are also triggered when the Xcitium Recommended Security Policy is violated. Dwell time on your real endpoint is reduced to zero, and no damage is possible, while your EDR tech is empowered to focus on hardening against future attacks.

Malicious behavior disguised as action typically performed by signed and trusted applications such as PowerShell and Regedit would not be flagged by other EDR tools —this is exactly why attackers use trusted applications. But Xcitium can see this behavior clearly in containment. Without our EDR, the contained threat often goes unnoticed, allowing an attacker to steal or ransom your company's confidential data. With ZeroDwell, contained attacks are not longer threats!

IMMEDIATE TIME-TO-VALUE

ZERODWELL CONTAINMENT

A unified endpoint solution offering attack containment at runtime, threat detection and response lifecycle optimization, exploit prevention, unparalleled visibility, expert alerts triage, and endpoint management to stop ransomware, avoid breaches, and sustain your business.

ZeroDwell Containment is compatible with other security infrastructures as an add-on first line of defense. As adversarial tradecraft evolves, all solutions benefit by preemptive speed and forbidden dwell time.

FULL SPECTRUM EDR VISIBILITY

Gain full context of an attack to connect the dots on how adversaries are attempting to breach your organization.

ELIMINATE EDR ALERT FATIGUE

Xcitium Guided EDR is much better and more usable than other vendors' EDR solutions because our **HIGH DEFINITION EDR** generates only actionable alerts. No alert fatigue means security analysts can dedicate productive time assessing real issues and vulnerabilities in your environment without being flooded by alert overloads and false positives.

ENDPOINT MANAGER

Accelerates the practice of cyber hygiene and reduces attack surfaces by identifying vulnerable systems and applications.

EXPERT SOC AND STREAMLINED ALERTS TRIAGE SERVICE

Many vulnerabilities are caused by a lack of resources and maintenance processes, and possibly by a lack of the expertise required to integrate and coordinate security technologies, but every one of these issues are fully covered and managed by Xcitium Advanced **24•7•365 SOC** alerts triage, investigations and remediation services.

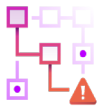
ZERO TRUST. ZERO DWELL. ZERO DAMAGE.

THE POWER OF ZERO.

XCITIUM GUIDED

The Xcitium Guided is an EDR bundle with the Alerts Triage Services add-on, combines ZeroDwell Containment technology (**ZDT**), Anti-Virus (**AV**), Viruscope (**NGAV**), endpoint detection and response (**EDR**), Host Intrusion Prevention System (**HIPS**), Firewall (**FW**), endpoint management (**EM**), and MDR-level **Alerts Triage** capabilities, to deliver exploit prevention, comprehensive telemetry, full-spectrum endpoint visibility, enhanced reporting, endpoint management, and alerts management all from one centralized SaaS platform.

KEY CAPABILITIES



MITRE ATTACK CHAIN MAPPINGS & VISUALIZATIONS

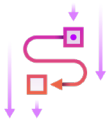
Attack vectors are shown on the dashboard. When combined with file trajectory and process hierarchy visualizations, this accelerates investigations. Process-based events are shown in a tree-view structure to help analysts better understand process behavior.

CONTINUOUS MONITORING | EDR | RECOMMENDED SECURITY POLICY

Every EDR license comes with a default endpoint security policy, which is customizable to meet individual needs. Our sales engineering team is available to work with you to tailor security policy to your requirements, especially endpoint-specific policies.

SUSPICIOUS ACTIVITY DETECTION & ALERTING

Get notified about events such as file-less attacks, advanced persistent threats (APTs), and privilege escalation attempts. Analysts can change status of alerts as they take counter-actions to dramatically streamline follow-up efforts. Because of ZeroDwell Containment at runtime, alert fatigue is a thing of the past and our experts, as well as your team, can focus on alerts that matter.



EXPERT ALERTS TRIAGE AND INCIDENT INVESTIGATION

Security experts triage alerts to determine the severity of the threat and whether or not the alert should be escalated to incident response. The event search screen allows analysts to run queries to return any detail at base-event-level granularity. Aggregation tables are clickable, letting investigators easily drill down into specific events or devices.

CLOUD-BASED ARCHITECTURE

Xcitium Advanced uses a lightweight agent on endpoints to monitor, process, network, download, upload, access file systems and peripheral devices, and log browser events, and it enables you to drill down into incidents with base-event-level granularity.

VERDICT CLOUD DECISION ENGINE

While running in virtualized containment, unknown files are uploaded to the Xcitium global threat cloud for real-time analysis and a verdict determination of benign or malicious. Benign entities are simply released from containment.

FILELESS MALWARE DETECTION

Not all malware is made equal. Some malware does not need you to execute a file when it is built in to the endpoint's memory-based architecture such as RAM. Xcitium EDR can detect against this threat before it appears.

PROACTIVE ZERODWELL CONTAINMENT

Unknown executables and other files that request runtime privileges are automatically run in Xcitium's patented ZeroDwell container that prevents access to the host system's resources and user data. ZeroDwell Containment means malware cannot move laterally across your network or organization.

ENTERPRISE LEVEL & MSP READY

Whether you're an enterprise with thousands of endpoints or an MSP serving hundreds of customers, the EDR agent can be instantly deployed via group policy object or the Xcitium ITSM with automatic updates every release.

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 Xcitium Essentials ZeroDwell technology uses Kernel-level 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), managed detection & response (MDR), and managed extended detection and response (M/XDR). Since inception, Xcitium has a track record of zero breaches when fully configured.

AWARDS & RECOGNITION

OUR CUSTOMERS

SALES

US: 646-569-9114

CA: 613-686-3060

EMAIL

sales@xcitium.com

support@xcitium.com

VISIT

200 Broadacres Drive,
Bloomfield, NJ 07003
United States