XCITIUM ADVANCED

PROACTIVE EDR WITH
PRE-EMPTIVE CONTAINMENT

THE WORLDWIDE CHALLENGE

UNKNOWNS & RANSOMWARE ARE SOPHISTICATED INDUSTRIES

NEW MALWARE
450,000
RELEASED DAILY

EDR ALONE = BREACHES
99% DETECTION
Current security solutions employ detection as a prelude to protection. This is backwards.. An undetected 1% means ongoing damage & breaches.

NEW RANSOMS
11 SECS
ENACTED DAILY

REPUTATION SERVICES
UNPREDICTABLE
Third-party intelligence services fuel the detection world but remain too slow and inefficient to be relied upon for full protection.

VICTIMS DAMAGED
$350M
IN RANSOMS PAID

INSUFFICIENT EXPERTISE
HIGH COST SKILLS
Limited cyber training, a high learning curve, and finite number of available experts to address your risk. Add in the high cost of alert fatigue.

THE XCITIUM ADVANCED SOLUTION

PROACTIVE ENDPOINT DETECTION AND RESPONSE (EDR)

There's no question there is a need for EDR. Yet, detection-first EDR tools provide insufficient security. Attackers are smart. They understand how detection-first solutions work, and they continuously develop techniques to slip under everyone's radar to attack as "Unknowns." Unknowns cannot be detected. **But when you add protection-first, real-time ZeroDwell Containment to an EDR solution's front end, suddenly you experience a paradigm shift and see breaches and ransom incidents plummet.**

The value of EDR becomes evident AFTER protecting first with ZeroDwell Containment. When attacks are preemptively contained, there is no more alert fatigue because contained attacks are no longer threats. With threats contained, real-time, continuous endpoint visibility and actionable alert management is where EDR capabilities shine. Now you can harden your environment against zero-day and file-less attacks, and EDR's full-specturm visibility leads to immediate and accurate root-cause analysis for effective patching and remediation. In this new context Xcitium EDR allows you to analyze what's happening across your entire organization at a granular, base-event level so you get detailed file and device trajectory information that reveals potentially larger issues that may be leaving your endpoints vulnerable. ZeroDwell Containment makes proactive EDR possible.

THE XCITIUM DIFFERENCE

Only Xcitium's patented ZeroDwell Containment prevents breaches, ransomware, and zero-day's from causing harm!

ZERO TRUST | ZERO BREACH | ZERO DAMAGE | ZERO DOWNTIME

XCITIUM ADVANCED

Xcitium Advanced combines the benefits of the Xcitium Essentials product with advanced endpoint security Anti-Virus (**AV**), Viruscope (**NGAV**), endpoint detection and response (**EDR**), Host Intrusion Prevention System (**HIPS**), Firewall (**FW**), and endpoint management (**EM**) capabilities, to deliver exploit prevention, comprehensive visibility, enhanced reporting, threat hunting, and endpoint management from a 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 you can focus on alerts that matter.

INCIDENT INVESTIGATION

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 does not have access to the host system's resources or user data. ZeroDwell Containment means malware cannot move laterally across your network or organization.

ENTERPRISE LEVEL & MSP READY

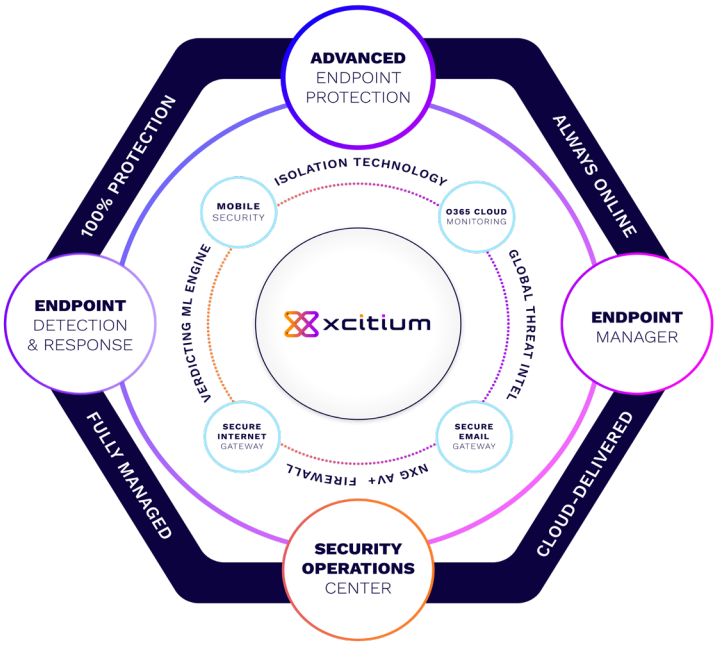
Whether you're an enterprise with thousands of endpoints or an MSP serving hundreds of customers, the EDR agent can be instantly deployed via group policy object or the Xcitium ITSM with automatic updates every release.

PROACTIVE EDR

CONTAIN THREATS IN REAL TIME, GAIN DEEP VISIBILTY, & HARDEN AGAINST FUTURE ATTACKS

Xcitium Advanced EDR continuous monitoring. is actively collecting attacks and anomalous events from your endpoints and centralizes them in the Xcitium threat cloud, leveraging Xcitium Threat Laboratories intelligence as well as recommended security policy. Our Verdict Cloud then analyzes and identifies the contained unknown files safely virtualized on endpoints and returns a fast malicious/benign verdict while EDR efforts are focused on real alerts, not alert fatigue.

With Xcitium Advanced, 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 IoCs. Alerts are also triggered when the Xcitium Recommended Security Policy is violated. Dwell time on your real endpoint is literally zero, and no damage is possible, while your EDR tech is now empowered for focus on remediation and resolving revealed vulnerabilities. For example, malicious behavior disguised as action typically performed by signed and trusted applications such as PowerShell and Regedit would not be similarly 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.



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, advanced threat hunting, and endpoint management to stop ransomware, avoid breaches, and sustain your business. **ZeroDwell Containment is also compatible with existing EDR security infrastructure as an add-on first line of defense.**

Move from Detection to Prevention with ZeroDwell Containment to isolate attacks such as ransomware & unknowns without any disruption of your endpoints or business opreations.

FULL SPECTRUM VISIBILITY

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

EDR WITHOUT ALERT FATIGUE

Gain full context of an attack to connect the dots on how hackers are attempting to breach your network without a flood of alerts burdening your security teams (contained attacks are not longer threats).

ENDPOINT MANAGER

Practice cyber hygiene to reduce the attack surface by identifying applications, understanding where your vulnerabilities lie, and remediating with patches.

MANAGED EDR SERVICE

Many vulnerabilities are caused by a lack of resources and maintenance processes, and possibly by a lack of the technology required to integrate and coordinate security technologies, but every one of these issues are fully covered and managed by Xcitium Advanced EDR's 24•7•365 SOC Investigation and remediation services.

ZERO TRUST. ZERO BREACHES.

ZERO DWELL. ZERO DAMAGE.

THE POWER OF ZERO.
UNLEASHED.

ABOUT US

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

CONTACT

SALES@XCITIUM.COM
SUPPORT@XCITIUM.COM