



XCITIUM

OPENEDR

OPEN SOURCE ENDPOINT
DETECTION AND RESPONSE
(EDR) - FREE TO ALL

WHAT IS OPEN SOURCE SOFTWARE?

Open Source software and technology is free, publicly accessible code that anyone can take, try, change, improve, and even distribute as part of their own products, however they see fit. Open source code development is collaborative and is validated by peer review, community usage, and self-paced production.

WHAT IS XCITIUM OPENEDR?

Open Source platforms like Atlassian, GitHub, and Linux have proven that when entire communities contribute to a code base together, many businesses, individuals, and organization no longer need to solve the same software solutions over and over, again and again, separately and on their own. Currently, there is a significant skills shortage in the cybersecurity industry, so participating in the articulation of complex security and code requirements using OpenEDR means you immediately gain expansive software development, technological innovation, and widely-tested operational efficiency. You are free to simply deploy and use the established Xcitium OpenEDR code provided by Xcitium as a complete free product that provides the telemetry you need to protect and secure your organization's endpoints. Whether or not you contribute to the code base is entirely up to you.

Some organizations do not have the technical expertise and/or infrastructure required to deploy and maintain a self-hosted EDR solution. Therefore, Xcitium provides an Xcitium Platform account for free to all OpenEDR users! Inside the Xcitium Platform, users can experience OpenEDR free of charge, deploy the agent with little effort, visualize event data, and utilize the many other benefits the Platform offers!

WHO NEEDS EDR IN TODAY'S GLOBAL THREAT LANDSCAPE?

While high cost may prohibit some organizations from acquiring commercial EDR tools, our founder, Melih Abdulhayoglu, offers this technology as a free open source project because he believes that endpoint security is a right, not a privilege. Xcitium OpenEDR technology monitors end-user devices to detect threats like ransomware and malware. It allows you to analyze what's happening across your entire organization at a granular, base-event level so you get detailed file and device telemetry information or alerts that reveal potentially larger issues that may be leaving your endpoints vulnerable. This is the baseline capability of Xcitium's OpenEDR platform, and it assures full-spectrum endpoint environment visibility with correlated, actionable data you can use to perform root-cause analyses that will lead to effective patching and remediation of vulnerabilities and exposures.

NEW MALWARE
450,000
RELEASED DAILY



OPEN EDR EFFICACY
GAINS VISIBILITY

A security solution that employs endpoint detection and protection. EDR is always only as good as its visibility across every endpoint.

NEW RANSOMS
EVERY 11 SECS
ENACTED DAILY



OPEN EDR ALERTING
MITIGATES RISKS

MITRE ATT&CK CHAIN mapping and visibility is a foundational EDR component. A Crowdstrike blog boasts that its XDR is rooted in EDR data.

VICTIMS DAMAGED
\$350M
IN RANSOMS PAID



OPEN EDR CORRELATIONS
REDUCES COST

Limited cyber training, a high learning curve, and a finite number of available experts to address risks means EDR is an important alternative.

OPEN EDR DEPLOYMENT OPTIONS

There are two ways to immediately access and deploy OpenEDR from openedr.com:

- **SELF-HOSTED.** (1) Download the free source code; (2) deploy the OpenEDR agent to your endpoints; and (3) host the OpenEDR platform instance on your own server: zero fees paid to Xcitium, no restrictions on security policies, usage or storage.
- **XCITIUM-HOSTED.** (1) Register for a free OpenEDR Platform account with Xcitium; (2) deploy the OpenEDR agent to your endpoints; (3) host the free OpenEDR platform on Xcitium servers; security policies are set, an event data storage charge applies and is limited to 3 days storage. This option includes an Xcitium whiteglove team that helps you install and deploy the Xcitium-hosted OpenEDR platform. **Get Started Now:** [How to deploy OpenEDR](#)

XCITIUM-HOSTED OPEN EDR - KEY CAPABILITIES



MITRE ATTACK CHAIN MAPPINGS, TRACKINGS, CONTEXTUALIZATIONS, VISUALIZATIONS

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



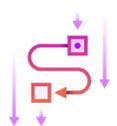
CONTINUOUS EDR MONITORING | SECURITY POLICY

Every EDR instance comes with a default endpoint security policy. 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. You can change the status of alerts as you take counter-actions to streamline responses and follow-up efforts.



INCIDENT INVESTIGATION

The event search screen allows you to run queries to return any detail at base-event-level granularity. Aggregation tables are clickable, letting you easily drill down into specific events or devices.



CLOUD-BASED ARCHITECTURE

Xcitium 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 incident details with ease. Note that OpenEDR does not rely on cloud connectivity to perform detections.



FILELESS MALWARE DETECTION

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



ENTERPRISE-SCALE, MSP-READY SOFTWARE FOR BOTH LARGE, MID AND SMALL BUSINESSES

Whether you're an enterprise with thousands of endpoints, a Partner or MSP serving hundreds of customers, a school district, or a small business with a handful of remote workers, the OpenEDR agent can be instantly deployed via a group policy that provides automatic updates every release.

UPGRADE TO XCITIUM ADVANCED FROM OPENEDR ANYTIME

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

Xcitium Advanced EDR’s kernel-level ZeroDwell virtualization is a pre-emptive breach prevention technology that precedes detection and response by containing all Unknowns and attacks at runtime. If an unknown object enters your endpoint, it is instantly untrusted, by default, and automatically ushered into containment –guilty until proven innocent. In containment, the Unknown object can operate as it likes (because **contained attacks** are no longer threats), but they can cause no damage to your endpoint or environment, and containment does not disrupt your endpoints or business operations in any way.

This zero trust approach protects endpoints proactively while setting the groundwork for EDR (or managed XDR to include cloud and networks) as the critical next step for actively protecting, monitoring, securing, hardening and responding to known and unknown objects and future threats. Xcitium Advanced EDR’s continuous monitoring collects attacks and anomalous events from endpoints and centralizes them in the Xcitium threat cloud, leveraging Xcitium Threat Laboratories intelligence as well as recommended security policy. Our Verdict Cloud analyzes and identifies all contained unknown files on the virtualized endpoint, and returns a fast malicious/benign verdict while EDR efforts are focused on real actionable alerts, not alert fatigue.

With Xcitium Advanced, you get actionable alerts based on customizable security policy that notifies you about the actions of contained activity that could represent ransomware, memory exploits, PowerShell abuses, 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 focuses on remediation and resolving revealed vulnerabilities. Xcitium can even clearly see attacks disguised as trusted applications in containment. Without Xcitium EDR, the contained threat often goes unnoticed, allowing an attacker to steal or ransom your company’s confidential data.

DON'T FEAR THE UNKNOWN. CONTAIN IT.

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, allowing detection efforts to be conducted without exposing the endpoint to risk during the process. **Zero Dwell Containment is also compatible with your existing security stack as a first line of defense add-on.**

FULL SPECTRUM VISIBILITY

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

AN EDR WITHOUT ALERT FATIGUE

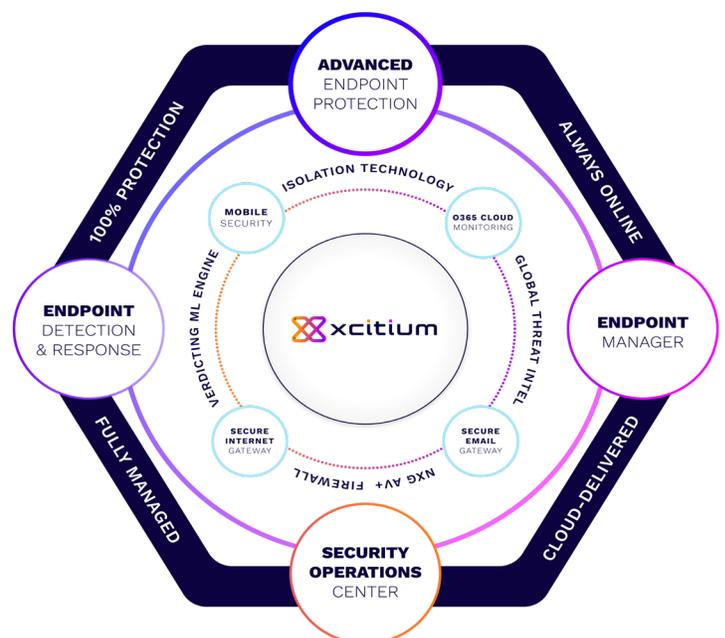
Gain full context of an attack to connect the dots on how hackers are attempting to breach your network without a flood of alerts.

ENDPOINT MANAGER

Reduces 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 addressed and managed by Xcitium





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 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 (Xcitium Essentials), endpoint detection & response (Xcitium Advanced - EDR), and managed detection & response (Xcitium Complete - MDR / MXDR). Since inception, Xcitium has a track record of zero breaches when fully configured.

CONTACT

sales@xcitium.com • support@xcitium.com