ZERO THREAT ADVANCED

ENDPOINT DETECTION & RESPONSE

xcitium

THE WORLDWIDE CHALLENGE

RANSOMWARE IS A SOPHISTICATED BUSINESS.

NEW MALWARE
300,000
CREATED DAILY
↓

EDR IS NOT ENOUGH
99% DETECTION

Current security solutions depend upon detection before they can prevent. Detection efficacy rates are not good enough.

NEW RANSOMS
11 SECS
CREATED DAILY
↓

REPUTATION SERVICES
UNPREDICTABLE

Third-party intelligence services fuel the detection world but remain too slow and inefficient to be relied upon all the time.

VICTIMS PAID
$350M
IN RANSOMS
↓

INSUFFICIENT
EXPERTISE

Limited cyber training, a high learning curve, and finite number of available experts to address your risk.

THE SOLUTION

CLOUD-BASED ENDPOINT DETECTION AND RESPONSE

There's no question that you need to deploy endpoint security tools and platforms that are built for protection. But that's not enough. Attackers are smart. They understand how those solutions work and they continuously develop techniques to slip under their radars. You also need real-time, continuous visibility so you can identify zero-day and file-less attacks, and that visibility must lead you to accurate root-cause analysis for effective remediation.

EDR allows you to analyze what's happening across your entire environment at a base-event level. This granularity enables accurate root-causes analysis needed for faster and more effective remediation. Process hierarchy visualizations, which are proven to be the best way to convey this type of information, provide more than just data, they offer actionable knowledge. Easy-to-navigate menus makes it easy to get details on endpoints, hashes, and base and advanced events. You get detailed file and device trajectory information and can navigate single events to uncover a larger issue that may be compromising your system.

THE XCITIUM DIFFERENCE

Only Xcitium can maintain 100% effectiveness in preventing ransomware and zero-day's from causing harm!

100% CYBERSECURITY EFFECTIVENESS | ZERO INFECTED ENDPOINTS
100% CYBERSECURITY SCALABILITY | ZERO RANSOMS PAID

KEY CAPABILITIES

ATTACK CHAIN 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.

RECOMMENDED SECURITY POLICY

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

SUSPICIOUS ACTIVITY 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 ZeroThreat 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

ZeroThreat Advanced EDR uses a lightweight agent 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.

VALKYRIE VERDICT 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.

COMPATIBLE WITH VIRTUALIZED CONTAINMENT

Unknown executables and other files that request runtime privileges are automatically run in Xcitium's patented virtual container that does not have access to the host system's resources or user data.

ENTERPRISE LEVEL & MSP READY

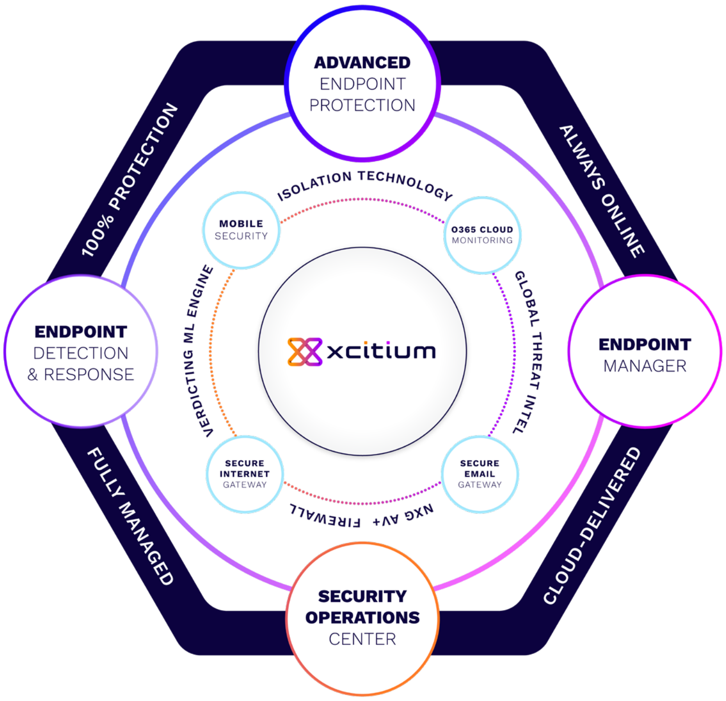
Whether you're an enterprise with thousands of endpoints or an MSP serving hundreds of customers, the EDR agent can be instantly deployed via group policy object or the Xcitium ITSM with automatic updates every release.

THE RESULTS

ELIMINATE THREATS & RESOLVE RECURRING EVENTS

EDR continuously collects events from your endpoints, centralizing them in our threat cloud that leverages Xcitium Threat Laboratories intelligence and Xcitium Recommended Security policy. Our cloud-based sandboxing uses the Valkyrie file-verdicting system to isolate unknown files attempting to run on endpoints to return a fast good/bad verdict.

You get instant alerts based on your customizable security policy to notify you about suspicious activity that could represent ransomware, memory exploits, PowerShell abuse, and many other threats. Alerts are also triggered when the Xcitium Recommended Security Policy is violated. The malicious behavior was performed by signed and trusted applications such as PowerShell and Regedit, a traditional endpoint tool would not have flagged it—which is exactly why the attacker used this approach. Without EDR, the threat could have gone unnoticed, allowing the attacker to steal all the company's confidential data.



UNIFIED MANAGED SECURITY

ZEROTHREAT PLATFORM

A single unified endpoint solution offering exploit prevention, advanced threat hunting, and endpoint management to stop ransomware, avoid breaches, and sustain your business.

ZEROTHREAT ADVANCED EDR

Move from Detection to Prevention with ZeroThreat Auto Containment™ to isolate infections such as ransomware & unknown threats without any disruption of your endpoints or your business.

ENDPOINT DETECTION AND RESPONSE

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

ENDPOINT MANAGER

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

MANAGED SERVICE

With 24•7•365 SOC Investigation and Remediation, vulnerabilities due to a lack of resources, processes, and possibly the technology to maintain all these technologies is fully covered and managed.

ABOUT US

Xcitium, formerly known as Comodo Security Solutions, is used by more than 3,000 organizational customers & partners around the globe. Founded with one simple goal – to put an end to cyber breaches. Xcitium's patented 'Zero Threat' technology uses Kernel API Virtualization to isolate and remove threats like zero-day malware & ransomware before they cause any damage. Zero Threat is the cornerstone of Xcitium's endpoint suite which includes advanced endpoint protection (AEP), 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