XCITIUM ADVANCED - CLIENT SECURITY

ENPOINT DETECTION & RESPONSE (**EDR**) WITH PRE-EMPTIVE ZERO DWELL CONTAINMENT

THE WORLDWIDE CYBERSECURITY CHALLENGE

UNKNOWNS, RANSOMWARE, AI: SOPHISTICATED ATTACK INDUSTRIES

NEW MALWARE
560,000
RELEASED DAILY

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

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
$1.1 BILLION
IN 2023 RANSOMS PAID

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

DETECTION IS NOT PROTECTION & THIS IS WHY BREACHES KEEP HAPPENING.

THE **XCITIUM ADVANCED** - CLIENT SECURITY SOLUTION

PRE-EMPTIVE EDR WITH ZERO TRUST, ZERO DWELL CONTAINMENT

Today's detection-first EDR tools provide insufficient security due to **VENDORS' FAILURE TO DETECT UNKNOWNS**. 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." Malicious Unknowns are designed to be undetectable. **BUT WITH XCITIUM'S DETECTION-LESS ZERO DWELL CONTAINMENT, SUDDENLY THERE IS A SECURITY PARADIGM SHIFT AS BREACHES AND RANSOMS PLUMMET BECAUSE WE PRE-EMPT DETECTION AND ACT ON ALL UNKNOWNS BY DEFAULT. AT XCITIUM, UNKNOWNS ARE GUILTY TILL PROVEN INNOCENT!**

With Xcitium's Zero Trust, Zero Dwell EDR, attacks are preemptively contained with virtualization, so you are protected at runtime; and there is no more alert fatigue or floods of false positives because contained attacks are no longer threats. With Unknowns contained, real-time, continuous endpoint visibility and high-definition actionable alerting are your new security focus. Now you can harden against future attacks using EDR's full-spectrum visibility and immediate, accurate root-cause analysis telemetry for effective patching and environment remediation. This protection-first context 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 endpoint vulnerabilities. **DETECTION-LESS ZERO DWELL DELIVERS EDR WITH PRE-EMPTIVE AI AS YOUR OWN VIRTUAL, BUILT-IN SECURITY ANALYST!**

THE XCITIUM DIFFERENCE

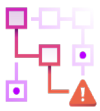
Xcitium's patented ZeroDwell Virtualization prevents breaches, ransomware, AI attacks, and zero-day's from causing harm by denying access to your real resources during auto-containment!

ZERO TRUST | ZERO DWELL TIME | ZERO INTERRUPTION OF ENDPOINTS OR BUSINESS PRODUCTIVITY

XCITIUM ADVANCED - CLIENT SECURITY

Xcitium Advanced - Client Security combines patented Zero Trust Detection-Less Virtualization (**ZeroDwell**), next-gen Anti-Virus (**AV**), Viruscope (**NGAV**), endpoint detection and response (**EDR**), a native, built-in SIEM (**SIEM**), our Host Intrusion Prevention System (**HIPS**), and Firewall (**FW**) capabilities, to deliver exploit prevention, comprehensive end-to-end telemetry and visibility, AI-powered verdicting and correlations, enhanced reporting, and high-definition, actionable alerting all from a centralized SaaS platform.

KEY CAPABILITIES



PRE-EMPTIVE DEFAULT-DENY ZERO TRUST: ZERO DWELL CONTAINMENT

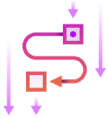
Unknown executables and other files are automatically contained by Xcitium's patented ZeroDwell virtualization and denied access to the host system's resources or user data during AI assessment and verdicting. ZeroDwell Containment means malware cannot access damage or move laterally across your network or organization to perform attack reconnaissance.

CONTINUOUS MONITORING | EDR | RECOMMENDED SECURITY POLICY

Every Xcitium Advanced Client Security 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 & HIGH-DEFINITION ALERTING

Get notified about events such as file-less attacks, advanced persistent threats (APTs), and privilege escalation attempts. Analysts can change the status of alerts as they take counter-actions to dramatically streamline follow-up efforts and harden your environment against future attacks. ZeroDwell Containment ends alert fatigue so you can focus on events 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 Client Security uses a lightweight agent on endpoints to monitor, process, network, download, upload, correlate telemetry, 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 AI analysis and verdict determination of benign or malicious. Benign entities are simply released from containment.

FILELESS MALWARE DETECTION

Not all malware is made equal. Some malware and scripts do not need you to execute a file when built in to the endpoint's memory-based architecture. Only Xcitium Advanced Client Security pre-empts these threats, and all Unknowns, to prevent damage.

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.

ENTERPRISE LEVEL & MSP READY

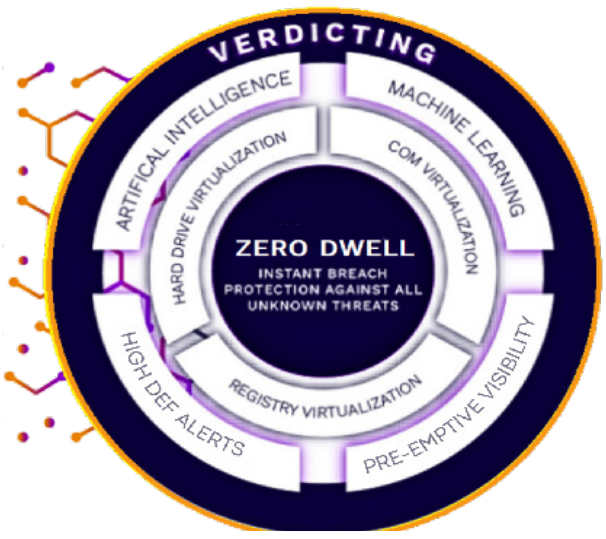
Whether you're an enterprise with thousands of endpoints or an MSP serving hundreds of multi-tenant customers, the EDR agent can be instantly deployed via group policy object or the **Xcitium Itarian Device RMM** with automatic updates every release.

PRE-EMPTIVE EDR

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

EDR monitoring continuously collects attack telemetry and endpoint security data, and performs correlations in concert with the Xcitium Verdict Cloud, leveraging Xcitium Threat Laboratories intelligence as well as recommended security policy. The Verdict Cloud then analyzes all automatically contained "Unknowns" (files and scripts with no known signature or hash) on instantly-virtualized endpoints at runtime to return a fast threat verdict while also generating real alerts without false positives or alert fatigue.

With Xcitium Advanced Client Security, 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. But Zero Dwell denies Unknowns access to real resources, so you can focus on resolving the vulnerabilities revealed by the contained attack. 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 to enact breaches. But Xcitium sees this behavior clearly during virtualized containment. Xcitium's contained Unknown threat would be unnoticed and UNDETECTED by other EDR vendors, allowing an attacker to steal or ransom your company's confidential data. With Xcitium ZeroDwell innovations, contained attacks are no longer threats.



IMMEDIATE TIME-TO-VALUE

ZERO TRUST, ZERO DWELL

Xcitium Advanced Client Security is a Zero Trust endpoint solution providing attack containment at runtime: pre-emptive exploit and damage prevention, innovative **DEFAULT DENY** virtualization of Unknowns that prevents access to your real data and resources, threat detection and response lifecycle optimization, conversion of all Unknowns to Knowns, unparalleled visibility, actionable correlated telemetry, and an end to ransomware, breaches, and business disruption. **ZeroDwell Containment is also compatible with other EDR security infrastructures as an add-on.**

All other EDR vendors provide **DEFAULT ALLOW** security that lets Unknowns into customer environments by default, and then they try to detect undetectable Unknowns. This is why breaches keep happening. It's time to turn to pre-emptive protection with ZeroDwell Containment.

XCITIUM EFFICACY IS CERTIFIED

The Xcitium Advanced Client Security solution is tested and certified by worldwide cybersecurity test labs, based on official guidelines provided by the CyberTransparency Forum; see our public performance statistics here!

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 or false positives burdening your security team.

ADD IT SERVICE MANAGEMENT

Add **ITARIAN DEVICE | RMM** or **ITARIAN MOBILE | MDM** to your EDR deployment; license the robust RMM Platform's IT tools and services to manage, monitor, and control devices and endpoint activities remotely, with full situational awareness, all from a single, central location, for better data-driven decisions, management, and operations. These tools seamlessly integrate with Xcitium security.

ABOUT XCITIUM & ITARIAN

Xcitium cybersecurity solutions are used by more than 6,000 organizational customers & partners around the globe. Xcitium was founded with one simple goal – to put an end to cyber breaches. Our patented ZeroDwell technology uses Kernel-level API virtualization to isolate and remove threats like zero-day malware and ransomware before they cause any damage to any endpoints. ZeroDwell is the cornerstone of Xcitium's Adanced Client Security, Managed SOC, and Managed MDR security offerings. Since inception, Xcitium has a track record of zero breaches when fully configured; see X citium's publicly-published and CERTIFIED performance record here.

Itarian, Xcitium's sister company, produces highly-acclaimed IT tools and services trusted by over 1,000,000 users consisting of MSPs and Business IT teams, administrators and tech experts worldwide.

Xcitium & Itarian deliver **Advanced Managed Security + IT Services** from a single console that enables integrated orchestration of security and IT environment(s) at scale. Xcitium also offers **Xcitium CNAPP** cloud security- extending zero trust from the endpoint all the way to your cloud workloads.

AWARDS & RECOGNITION

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