ENDPOINT BREACH PROTECTION ADD-IN PRODUCT

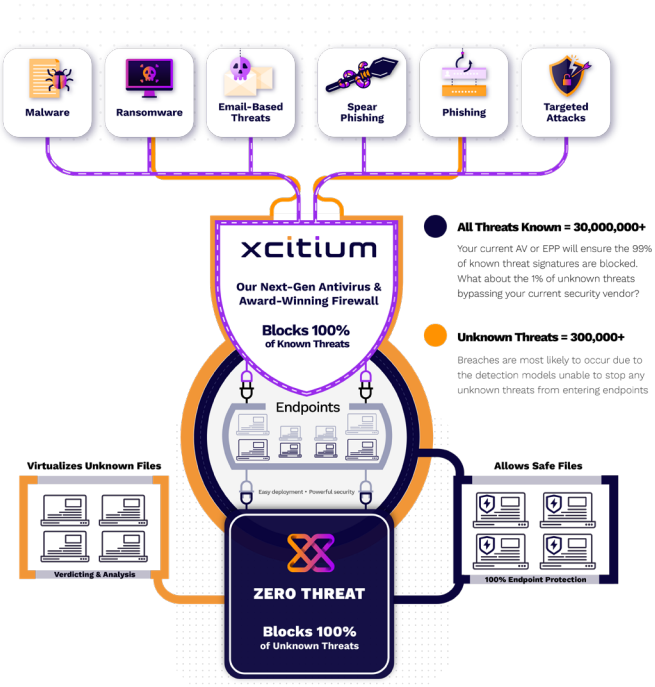
ZEROTHREAT TECHNOLOGY

While no one can stop malware and ransomware from entering your network, XCITIUM's ZeroThreat Technology prevents cyber attacks from causing any damage with true zero-trust encapsulation. Because the endpoint environment is virtualized, applications running in the secure ZeroThreat Technology container cannot make permanent changes to other processes, programs, or data on your 'real' system.

HOW IT WORKS

ZeroThreat Auto Isolation is a virtualization feature that allows business endpoints to run unknown/untrusted files and applications virtually, in an automated manner, based on default and/or custom rules and security policies.

This true zero-trust technology provides untrusted (but harmless) applications (aka "unknowns") the freedom to operate, but all untrusted (and potentially malicious) applications are prevented from damaging your PC or data. Malware and ransomware threats may make it on to an endpoint, but with Xcitium Virtualization, malware and ransomware are rendered absolutely incapable of damaging that endpoint. Nor can they breach that endpoint to move laterally across your network to other hosts or critical assets.

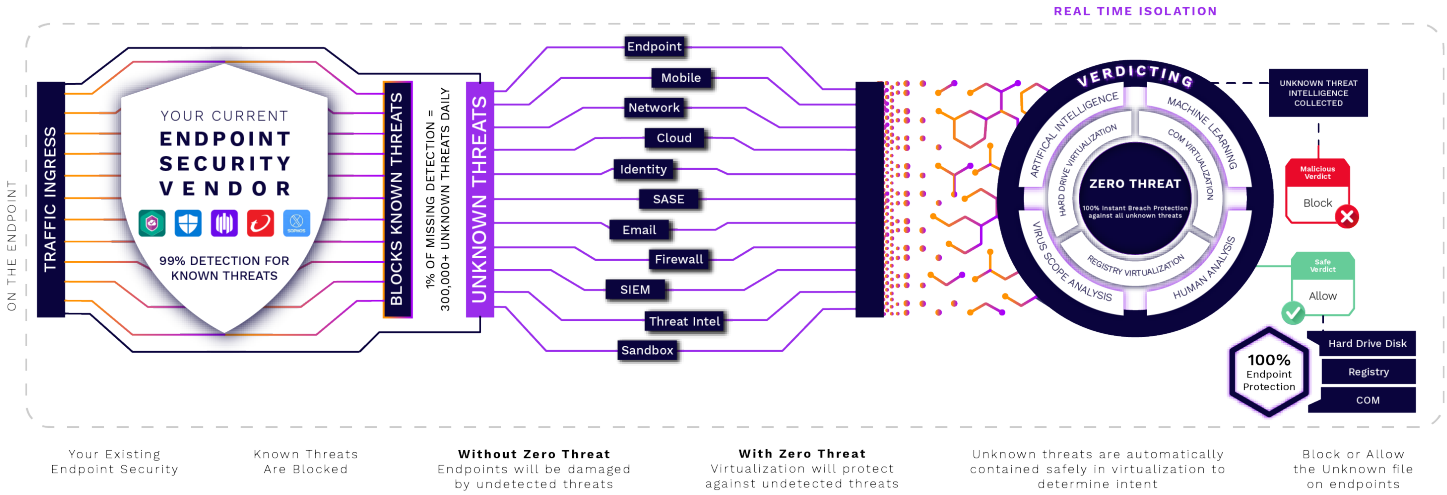


- Trusted verdicts for 100% of unknown files with ZeroThreat & zero stress
- 0% of our customers have experienced a breach
- Unknown files welcomed into a virtualized environment for analysis

MOVE FROM DETECTION TO PREVENTION WITH ZEROTHREAT AUTO VIRTUALIZATION TO INSTANTLY ISOLATE RANSOMWARE, MALWARE & UNKNOWN THREATS

ZEROTHREAT - FOOTPRINT

ZeroThreat technology delivers auto-isolation services that compliment your existing endpoint protection platform or security posture. This standalone product includes a SaaS management console, endpoint client agents, service delivery from the Xcitium Threat Research Labs (CTRL), and the Valkyrie engine, a file safety determination service used to assess isolated files and objects to provide a malicious or safe verdict. ZeroThreat is licensed by the number of endpoints in your organization.



KEY ADVANTAGES: THE POWER OF ZERO

INSTANT RUNTIME VIRTUALIZATION. XCITIUM protects first, proactively, with isolation of unknown objects, then performs sandboxing, detection forensics, and verdicting. This is the right way to protect your endpoints and your business. **Zero Trust. ZeroThreat.**

ABSENCE OF ALERT FATIGUE. Businesses are overwhelmed by threat alerts and false positives, making it almost impossible to identify and investigate genuine unknowns and stealthy threats. Problem solved: At run time, ZeroThreat Technology simply isolates untrusted, unknown objects. File verdicts are simple and conclusive. **Zero Stress.**

ENCOURAGES ATTACKER CONFIDENCE. Xcitium's kernel-level Virtualization ushers unknown, stealthy threats straight into isolation where the malicious file or code can reveal itself without any possibility of damage to the endpoint or the business. And our virtualization and analysis/forensics leave no artifacts that might tip off exploratory malware that it is in a virtualized environment. Gotcha! **Zero Breaches.**

FAST, RELIABLE VERDICTING. Analysis and verdicting are automatic, beginning at the moment of virtualization to determine whether an unknown object is malicious or benign. The Xcitium human-led security team immediately engages whenever additional analysis or further event interpretation is needed. **Zero Downtime.**

COMPATIBLE WITH OTHER ENDPOINT SECURITY TECHNOLOGIES. ZeroThreat Technology is lightweight, easy to install, and fully compatible with 3rd-party security products such as: Kaspersky Security Cloud Personal 21.3.10.391, Sophos Endpoint Agent 2.20.11, Trend Micro Maximum Security 17.7, and Windows Defender. Additional vendor compatibility testing is underway and ongoing. **Zero Damage.**

INDUSTRY LEADER

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 'ZeroThreat' technology uses Kernel API Virtualization to isolate and remove threats like zero-day malware & ransomware before they cause any damage. ZeroThreat 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.

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