



XCITIUM

ESSENTIALS

PRE-EMPTIVE, PROTECTIVE
RUNTIME THREAT CONTAINMENT

PRE-EMPTIVE ENDPOINT BREACH PREVENTION

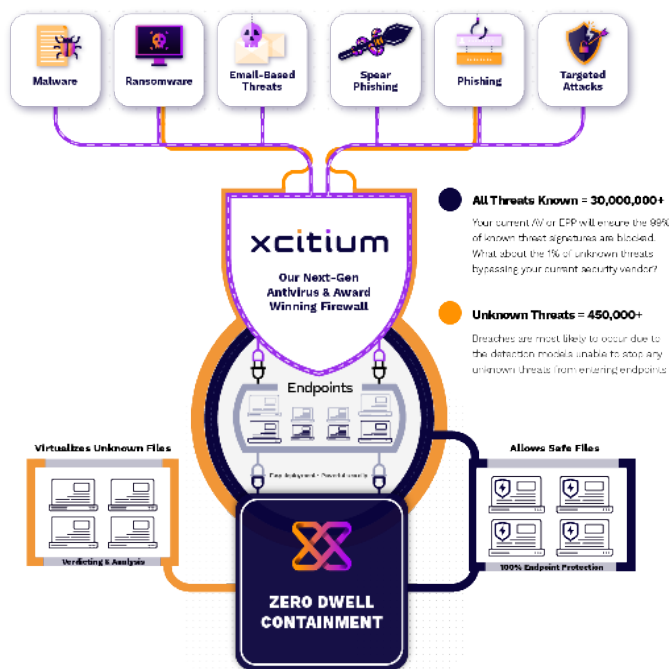
Xcitium Essentials

While no one can stop malware and ransomware from entering your network, XCITIUM's Essentials technology prevents cyber attacks from causing any damage with proactive zero-trust containment of all Unknown files and objects at runtime. Applications running in a secure Essentials container cannot make permanent changes to other processes, programs, or data on the 'real' endpoint system. **This is how to neutralize endpoint attacks without any productivity or business disruption.**

HOW IT WORKS

Xcitium Essentials employs kernel-level virtualization that allows business endpoints to run any unknown/untrusted files and applications virtually, in an automated manner, based on default-deny and/or custom rules and security policies. Essential's **ZeroDwell Containment feature** pre-empts detection-first strategies with automated, breach-free containment. This means protection is now the first and most powerful line of cyber defense.

ZeroDwell, zero-trust containment allows any untrusted (but harmless) applications (aka "unknowns") the freedom to operate, while 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 **ZeroDwell Containment**, malware and ransomware are rendered absolutely incapable of damaging or breaching that endpoint to move laterally across your network to other hosts or critical assets.

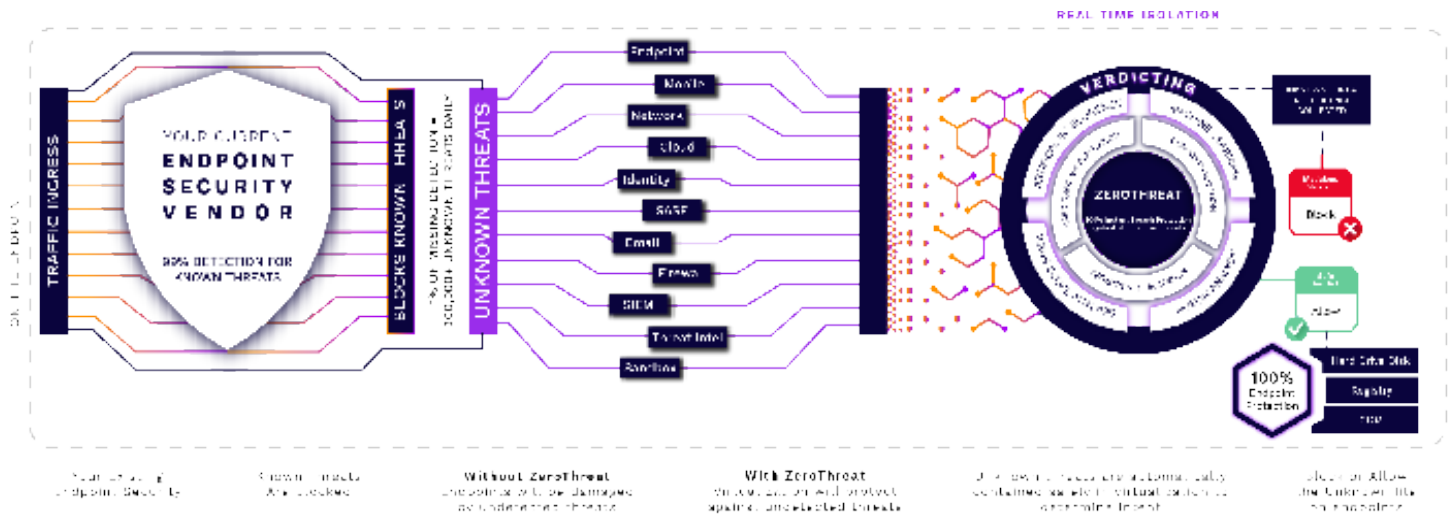


- **All Unknown files are instantly and automatically ushered into a virtualized, protective ZeroDwell environment for immediate verdicting and forensic analysis.**
- **Xcitium's Verdict Cloud assesses all contained, Unknown files. Contained attacks are no longer threats! Benign files are simply released from containment!**
- **0% of Xcitium customers have ever experienced a breach. For the past 4 years and over 1M endpoints, Xcitium customers have not experienced any attacker damage.**

MOVE FROM DETECTION TO PREVENTION WITH ZERODWELL CONTAINMENT.

ZERODWELL CONTAINMENT - FOOTPRINT

ZeroDwell 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 (XTRL), and the Verdict Cloud engine, a file safety determination service used to assess isolated files and objects to provide a malicious or safe verdict about contained Unknowns. ZeroDwell 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, ZeroDwell Containment 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 expert security team immediately engages whenever additional analysis or further event interpretation is needed. **Zero Downtime.**

COMPATIBLE WITH OTHER ENDPOINT SECURITY TECHNOLOGIES. ZeroDwell 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 2.2011, Trend Micro Maximum Security 17.7, and Windows Defender. Additional vendor compatibility testing is currently 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. It was founded with one simple goal – to put an end to cyber breaches. Xcitium’s patented ZeroDwell Containment uses Kernel API Virtualization to isolate and neutralize threats like zero-day malware & ransomware before they cause any damage. Xcitium Essentials ZeroDwell 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.

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

©XCITIUM INC. ALL RIGHTS RESERVED

