From Containment to Protection

Moving beyond sandboxing to a more effective, complete, and efficient threat investigation and remediation approach

This white paper explores the differences between traditional sandboxing—a commonly used technique for malware detection and threat containment—and Xcitium ZeroDwell Containment, a next-generation approach to protecting endpoints without disrupting user experience. Traditional sandboxing typically executes suspicious files in isolated environments to observe behavior but suffers from performance drawbacks and delays in threat resolution. In contrast, Xcitium ZeroDwell Containment moves unknown files to virtualized execution, enabling undisrupted user operations while concurrently analyzing the threat, thus reducing time to verdict and avoiding the performance limitations that impact sandboxing.

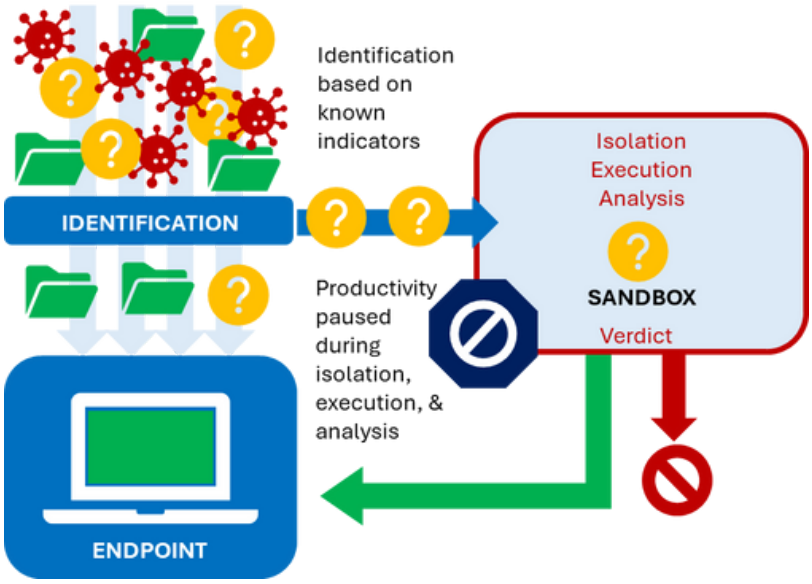
Legacy Sandboxing and Threat Containment

As cyber threats evolved in sophistication, companies employed various technologies to protect systems. Sandboxing has long been a staple in cybersecurity, isolating potentially harmful files from the host system in secure environments where behavior is analyzed. This approach negatively impacts user experience due to latency and the delay in delivering a verdict.

How Sandboxing Works:

In legacy sandboxing, suspicious files or programs are placed in an isolated environment—"sandbox"—where they are executed safely to observe any malicious behavior. If deemed safe, they're released for normal operation. If malicious, further actions (quarantine or deletion) occur. This process involves several steps:

1. **File Identification:** Detection of suspicious files based on certain known indicators (e.g., unknown source, abnormal behavior).
2. **Isolation and Execution:** The file is executed in an isolated sandbox environment.
3. **Behavioral Analysis:** The system observes file behavior to detect malware signatures or suspicious actions.
4. **Verdict and Action:** After analysis, the file is either blocked or allowed to execute on the primary system.



This approach includes some significant challenges that may stand in the way of full protection.

- **Incomplete Threat Detection:** Logic and automation must be in place to determine if a file is threatening enough to be moved to the sandbox. This decision is typically based on a series of “known” indicators of threat.
- **Delayed Verdicts:** Sandboxing requires significant time to analyze files, causing noticeable delays. The entre time the host system is unable to execute related actions as the sandbox analyzes the file.
- **False Positives:** Some benign files exhibit behavior that can be mistakenly flagged as malicious, leading to unnecessary alerts.
- **High Resource Consumption:** Running files in a sandbox environment requires substantial processing power, potentially impacting system performance.
- **Evasion Techniques:** Advanced malware can detect the sandbox environment and modify its behavior, delaying or avoiding detection.

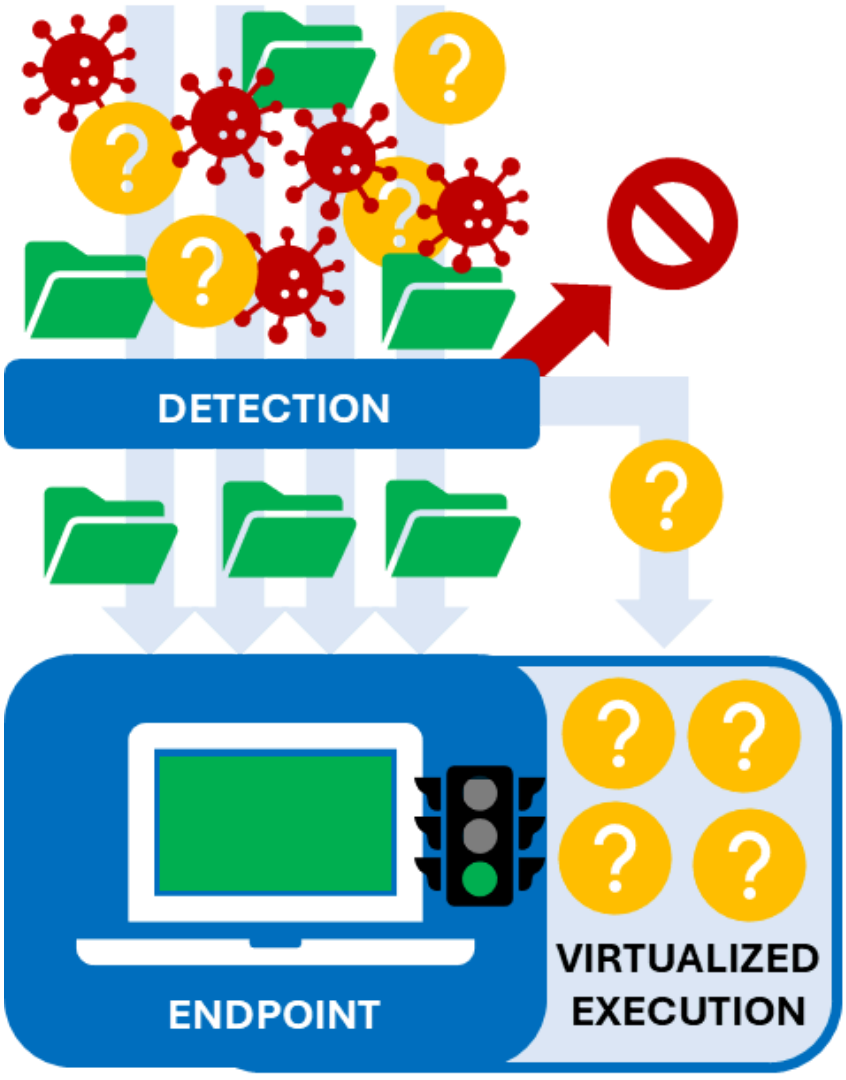
The impact of sandboxing on user experience

A significant drawback of sandboxing is its impact on the end-user experience. Sandboxing introduces latency as the system awaits a threat verdict, significantly slowing application performance or access. Moreover, sandbox environments can produce false positives or even allow evasive malware to avoid detection by remaining dormant, leading to prolonged analysis times and increased resource demands.

The bottom line is sandboxing only provides partial protection and can introduce significant obstruction to operations. There has to be a better way.

The Better Way – ZeroDwell Containment and Virtualized Execution

Xcitium's ZeroDwell Containment offers an alternative to sandboxing that delivers near-instant containment (but it's a different, better type of containment) without disrupting operations. This transformative approach to protection immediately isolates unknown files (all unknown files) to a kernel-level virtualized environment as soon as they are introduced to the system.



- **Known Bad** blocked
- **Known Good** allowed
- **Unknown** executed in virtualized environment

No negative impact on productivity

Every **Unknown** receives a definitive verdict and is addressed accordingly

Key processes include:

- **Dynamic Detection:** Xcitium detects all files and treats them appropriately. Known bad files are immediately blocked; known good files are always allowed; and all unknowns are sent for virtualized execution in ZeroDwell Containment.
- **Virtualized Execution:** ZeroDwell Containment automatically isolates all unknown files to a kernel-level virtualized environment that allows safe interaction and verdicting without impacting system performance.
- **Real-Time Analysis:** The technology allows the file to execute in virtualization at the kernel level (where it can do no damage) and concurrently performs comprehensive analysis (including AI, behavioral analysis, adaptive analysis, and human analysis) returning a verdict. Files identified as “good” are added to a known-good list and will be allowed to execute going forward, unknown files that are identified as “bad” are terminated and will be recognized as dangerous and treated accordingly going forward. As this all happens in the virtualized environment, there is no requirement for the file to wait in a sandbox. Security processes are significantly streamlined.
- **Zero Delay for Users:** Unlike sandboxing, ZeroDwell Containment maintains full usability for the end-user, providing seamless access while the threat analysis and remediation proceeds.

Xcitium ZeroDwell Containment delivers several significant advantages compared to legacy sandboxing:

- **Enhanced Malware Detection:** Xcitium's virtualization approach eliminates the risk of evasion, as malware cannot alter behavior based on environment checks. In addition, because it detects and addresses ALL unknowns the risk of new, unrecognizable malware signatures and behaviors is entirely eliminated.
- **No Verdict Delay:** Due to its virtualized execution approach, ZeroDwell Containment operates without the latency of sandboxing, providing near-instantaneous analysis.
- **Seamless User Experience:** Files execute instantly (yet safely), providing uninterrupted access to applications and data without latency or lag.
- **Lower Resource Usage:** By virtualizing the threat rather than replicating the environment, ZeroDwell Containment reduces the need for heavy resource consumption.

Enhanced User Experience and Faster and More Accurate Verdicts

ZeroDwell Containment's revolutionary approach to protection lies in its ability to deliver a seamless experience without interruption. Sandboxing interrupts the user, delaying file access while analysis occurs. In contrast, Xcitium's virtualized execution approach allows users to safely interact with files in real-time, with no interruptions, and none of the latency or incompetence of sandbox containment. This approach eliminates disruptions and improves operational efficiency while concurrently dramatically improving protection and reducing risk.

Comparative Analysis

In a side-by-side comparison, Xcitium ZeroDwell Containment with virtualized execution significantly outperforms sandboxing across several key dimensions:

Feature	Sandboxing	Xcitium ZeroDwell Containment
Threat Analysis Speed	Significant delays	Instantaneous
Impact on User Experience	Noticeable delays	Seamless, real-time
Susceptibility to Evasion	High (malware can detect sandbox)	None (virtualized execution prevents evasion)
False Positive Rate	Higher due to sandbox sensitivity	Lower due to accurate verdicting
Resource Utilization	High due to duplicate environments	Low due to virtualized execution

Practical Application and Real-World Impact

The Xcitium approach to protection will benefit any organization that requires continuous, high-security operations with minimal disruption. Key applications include:

- In industries where latency and false positives can lead to costly downtime ZeroDwell Containment offers instantaneous protection without impacting business speed.
- For organizations that rely on critical applications to remain functional during threat analysis, ZeroDwell Containment preserves data and application access without disruption.
- ZeroDwell Containment allows large organizations to implement robust security with minimal impact on user productivity and workflow continuity.
- For organizations with limited security staff or experience, ZeroDwell Containment (possibly augmented by Xcitium managed detection and response) can raise the bar for cybersecurity far beyond legacy methods.

Conclusion

The evolution of the threat landscape requires solutions that balance effective protection with seamless user experience. Traditional sandboxing fails to meet these needs due to delays, vulnerability to evasion, and resource consumption. Xcitium ZeroDwell Containment transcends these limitations, offering a real-time, no-delay, low-resource, solution that protects systems without hindering user productivity.

ZeroDwell Containment exemplifies the future of threat containment, combining advanced virtualized execution techniques with an emphasis on complete protection and usability. As organizations face increased threats, ZeroDwell Containment provides the ideal approach to raise the bar on both security and operational efficiency.

The Business Case for Xcitium

- **Cost Savings**: Mitigates the financial impact of breaches and reduces response overhead.
- **Regulatory Compliance**: Meets and exceeds global cybersecurity standards.
- **Future-Proofing**: Adapts to evolving threats without the need for frequent updates.

Why Xcitium is the Future of Cybersecurity

Xcitium's Unified Zero Trust Platform sets a new standard in cybersecurity, replacing reactive detection with proactive containment. By eliminating assumptions and delivering comprehensive protection across endpoints and cloud workloads, Xcitium empowers organizations to stay ahead of adversaries and safeguard their digital assets.