xcitium

WHITE PAPER

Execution Governance as Proof of Cyber Control Enforcement

How Execution Governance helps CISOs demonstrate that cybersecurity controls are not only deployed, but continuously enforced, validated, and delivering intended outcomes to boards, auditors, regulators, and insurers.

Table of Contents

1. Why Cyber Insurers Are Raising the Bar **5**

1.1 The Shift From Tooling to Proof 5

1.2 The Rise of Measurable Cyber Assurance 5

2. The Reporting Gap in Detection-First Security **6**

2.1 Visibility VS Enforcement 6

2.2 Why Alerts are Not Proof of Control 6

3. The New CISO Accountability Model **7**

3.1 Four Accountability Audiences 7

4. Execution Governance Explained **8**

4.1 What Execution Governance is 8

4.2 Three Core Principles 8

4.3 How Execution Governance Works in Practice 8

5. Execution Governance as an Assurance Model **9**

5.1 From Security Control to Reporting Framework 9

5.2 Five Assurance Dimensions 9

5.2.1 Measurable Enforcement Visibility 9

5.2.2 Policy Validation 9

5.2.3 Auditability 9

5.2.4 Runtime reporting 9

5.2.5 Containment evidence 9

6. How the Insurance Conversation Changes **10**

6.1 Practical Reporting Outputs 10

+1 973-859-4000 www.xcitium.com

7. The Future of Cybersecurity Reporting **11**

7.1 Provable Enforcement as the New Standard 11

7.2 Three Dimensions of Measurable Resilience 11

7.3 Positioning Execution Governance Strategically 11

8. Execution Governance in Action: A Scenario Walkthrough **12**

8.1 The Scenario: A Ransomware Execution Attempt 12

9. Compliance Framework Alignment **14**

9.1 How Execution Governance Maps to Major Frameworks 14

9.2 The Audit Readiness Advantage 14

10. Addressing Common Questions **16**

10.1 "We Already Have Zero Trust. Is this the Same Thing?" 16

10.2" We Already Run EDR and XDR. How is this Different?" 16

11. Conclusion **18**

12. References **19**

13. Legal Disclaimer **19**

13. About Xcitium **20**

Executive Summary

The cybersecurity accountability model is changing. Cyber insurers, boards of directors, and regulators are no longer satisfied with traditional security reporting that demonstrates monitoring capability. They are asking a harder question: where is the proof that your controls actually work?

Most organizations can produce extensive detection evidence: EDR dashboards, SIEM telemetry, SOC metrics, incident response reports. What they cannot produce is proof of execution governance: documented evidence that unknown code was restricted, runtime enforcement was applied, and execution controls operated according to policy.

This is the reporting gap that Execution Governance closes. Rather than demonstrating that threats were detected after execution, Execution Governance gives CISOs audit trails, enforcement records, and containment evidence that prove control effectiveness before damage occurs.

The result is a fundamentally different conversation with insurers, boards, and auditors: one grounded in provable enforcement rather than probabilistic detection.

> *Cyber insurers no longer want proof you can detect attacks. They want proof you can enforce control.*

+1 973-859-4000 www.xcitium.com

1. Why Cyber Insurers Are Raising the Bar

1.1 The Shift From Tooling to Proof

For years, cyber insurance underwriting focused on tool deployment. Did the organization have endpoint protection? Was a SIEM in place? Was multi-factor authentication active? Tool presence was treated as evidence of control.

That model is breaking down. High-profile breaches at organizations with mature security stacks have demonstrated that tool deployment and control effectiveness are not the same thing. Insurers have responded by shifting their evidentiary requirements.

Today, insurers are asking operational questions:

- How do you govern unknown execution?
- What proof exists that execution controls are enforced at runtime?
- Can you demonstrate that prevention policies are operationally active?
- How do you prevent unrestricted execution of untrusted code?
- What measurable evidence supports your prevention claims?

1.2 The Rise of Measurable Cyber Assurance

These questions represent a structural shift in how insurers think about cyber risk. The concern is not whether an organization can respond to a breach. It is whether controls are robust enough to prevent breaches from materializing.

Detection-first architectures are fundamentally reactive. They produce evidence of response capability: how quickly threats were detected, how effectively they were contained after the fact. Valuable information. But not proof of enforcement.

INSURER PERSPECTIVE
An organization that detects a ransomware attack within four hours is demonstrating response capability. An organization that can prove unknown code was automatically governed and restricted before it could execute on live systems is demonstrating enforcement capability. These are different claims. Insurers are pricing them differently.

2. The Reporting Gap in Detection-First Security

2.1 Visibility VS Enforcement

Detection-first security excels at generating visibility. Modern EDR, XDR, and SIEM platforms produce rich telemetry. SOC teams have more data than at any point in the history of the industry.

But visibility and enforcement are distinct capabilities. Visibility means the organization can see what is happening. Enforcement means it can prove that specific controls actively restricted what was permitted to happen.

What detection-first provides	What detection-first cannot provide
Alert telemetry and investigation data	**Proof that unknown execution was governed**
Incident response timelines and metrics	**Audit trail of runtime enforcement decisions**
Threat intelligence and behavioral analysis	**Evidence that prevention policies were operational**
SOC workload and MTTR reporting	**Documented containment of untrusted execution**
Compliance dashboard coverage	**Measurable enforcement visibility for insurers**

2.2 Why Alerts are Not Proof of Control

Every alert, by definition, describes something that was already permitted to execute. When an EDR platform fires an alert, it is reporting on execution that has already occurred on a live system. That is evidence of a detection event. Not evidence that a control prevented unrestricted execution.

When a CISO presents an alert volume report, they are demonstrating that detection tools are active. What they are not demonstrating is that execution was governed before it reached live systems.

THE ENFORCEMENT GAP
A security architecture that detects malicious execution on a live system has already permitted that execution to occur. Detection-first tools do not prevent execution. They respond to it. This is the enforcement gap that cyber insurers are increasingly asking CISOs to address..

3. The New CISO Accountability Model

CISOs are operating in a significantly more complex accountability environment than a decade ago. The audiences demanding cybersecurity assurance have expanded well beyond the IT department, and each brings distinct expectations about evidence.

3.1 Four Accountability Audiences

Audience	What they currently receive	What they increasingly require
Cyber Insurers	Security tool inventory, incident history, response SLAs	Proof of runtime enforcement, execution governance evidence, measurable prevention claims
Board of Directors	Risk dashboards, incident summaries, investment metrics	Demonstrable control effectiveness, enforceable governance posture
Regulators	Compliance documentation, audit logs, policy records	Evidence of operational controls, runtime policy enforcement
Operational Leadership	Uptime metrics, incident frequency, remediation timelines	Proof that business operations are structurally protected, not just monitored

The common thread across all four audiences is a shift from monitoring evidence to enforcement evidence. CISOs who can only demonstrate detection and response will increasingly find themselves at a disadvantage in insurance negotiations, board conversations, and regulatory reviews.

> **Detection proves visibility.** *Execution Governance proves enforcement.*

4. Execution Governance Explained

4.1 What Execution Governance is

Execution Governance is the principle that unknown or untrusted code should never receive unrestricted access to operating system resources, memory, files, credentials, or network functions without governance controls. It is a structural security model built on a simple premise: preventing unauthorized execution is more provable than detecting it afterward.

Unlike detection-first architectures, which observe and respond to execution behavior on live systems, Execution Governance controls what code is permitted to do before it can access real system resources. Unknown processes run in governed containment environments where their behavior can be analyzed and restricted without exposing production systems.

4.2 Three Core Principles

Governed Execution	Runtime Enforcement	Deterministic Control
Unknown code operates within defined boundaries, not on live production systems. Execution is permitted only under governed conditions with documented restrictions.	Policy enforcement happens at runtime, at the kernel level, before code can access system resources. Enforcement is active and continuous, not retrospective.	Control outcomes are deterministic rather than probabilistic. Each enforcement decision is logged, auditable, and reportable as evidence of control effectiveness.

4.3 How Execution Governance Works in Practice

When an unknown file attempts to execute, Execution Governance intercepts it before it can access production system resources. The process runs in a contained environment where its behavior is observed, analyzed, and restricted. Throughout this process, the governance platform generates an auditable record of every enforcement decision.

This enforcement record is the foundation of the new insurer conversation. Rather than presenting alert volumes or response timelines, CISOs can present documented evidence that specific unknown processes were governed according to policy, that execution was restricted before any production system access was granted, and that containment was applied consistently and measurably.

5. Execution Governance as an Assurance Model

5.1 From Security Control to Reporting Framework

The strategic value of Execution Governance for CISOs is not just operational. It is evidentiary. Execution Governance transforms cybersecurity from a monitoring model into a provable control model. Every enforcement decision generates evidence. Every containment action creates an audit trail. Every policy enforcement instance becomes reportable.

This positions Execution Governance not merely as a security control among many, but as an assurance framework: a systematic approach to generating the enforcement evidence that insurers, boards, and regulators are now demanding.

5.2 Five Assurance Dimensions

5.2.1 Measurable Enforcement Visibility

Every execution governance decision is logged and quantifiable. CISOs can report on the volume, frequency, and nature of enforcement actions taken, providing a metrics-based view of control effectiveness that alert-based reporting cannot replicate.

5.2.2 Policy Validation

Execution Governance provides ongoing evidence that prevention policies are operational, not merely configured. A policy that exists in a console but is not actively enforced provides no assurance. Execution Governance proves enforcement is active.

5.2.3 Auditability

Every containment action generates an auditable record. These records can be presented to insurers, regulators, and auditors as direct evidence of control operation, satisfying evidentiary requirements that detection logs alone cannot meet.

5.2.4 Runtime reporting

Unlike compliance documentation that captures point-in-time configuration, execution governance reporting captures continuous runtime enforcement. This provides a dynamic view of control effectiveness across the full operational period, not just at audit time.

5.2.5 Containment evidence

When unknown code is governed and restricted, the governance platform documents what was contained, when, and under what policy conditions. This containment evidence directly answers the question: "Can you prove execution controls were enforced?"

> *Security tooling is no longer enough. Insurers now expect measurable assurance.*

6. How the Insurance Conversation Changes

The practical impact of Execution Governance on the insurer relationship is best understood through the contrast between two types of CISO conversations.

Without Execution Governance	With Execution Governance
When asked about control effectiveness: "We monitor all endpoint activity and detect threats quickly. Our SOC responds to critical alerts within four hours. Last quarter we investigated 847 incidents."	**When asked about control effectiveness:** "Unknown execution was automatically governed and restricted according to policy, and we can provide documented evidence of every enforcement decision taken during that period."
When asked about unknown execution: "Our EDR monitors all process execution and flags suspicious behavior for SOC review."	**When asked about unknown execution:** "Unknown processes are placed in governed containment before they can access production resources. We have an audit trail of every containment decision."
When asked for enforcement proof: "We can provide our alert dashboard and incident log from the past 90 days."	**When asked for enforcement proof:** "Here is our enforcement record: [X] unknown processes governed, [Y] containment actions taken, zero instances of unrestricted unknown execution on production systems."

The practical impact of Execution Governance on the insurer relationship is best understood through the contrast between two types of CISO conversations.

The difference is not rhetorical. The second set of answers provides specific, measurable, auditable evidence. Organizations that can demonstrate execution governance are in a structurally stronger position during underwriting, renewal, and claims conversations.

6.1 Practical Reporting Outputs

Execution Governance enables CISOs to provide insurers with a new category of security evidence:

- **Enforcement Summary Reports:** Volume and frequency of execution governance decisions
- **Containment Records:** Documented evidence of unknown process restriction
- **Policy enforcement audit trails:** Proof that governance policies were operationally active
- **Runtime enforcement dashboards:** Continuous view of governance activity
- **Measurable prevention evidence:** Demonstrable proof of control effectiveness over time

7. The Future of Cybersecurity Reporting

7.1 Provable Enforcement as the New Standard

The cybersecurity reporting landscape is moving toward a model centered on provable enforcement rather than observed detection. This shift is being driven simultaneously by insurers, regulators, and boards. Each arriving at the same conclusion from different directions: knowing that threats were detected is less valuable than being able to prove that controls prevented them.

Organizations that build execution governance capabilities now, and the reporting infrastructure to evidence them, will have a measurable advantage in insurance negotiations, regulatory conversations, and board-level risk discussions.

7.2 Three Dimensions of Measurable Resilience

Provable Enforcement	Measurable Resilience	Operational Assurance
Documented evidence that specific controls operated as designed, measurable by enforcement volume, containment rate, and policy compliance.	Quantifiable security posture tracked over time, benchmarked against policy requirements, and reported to insurers as evidence of sustained control.	Confidence for boards, insurers, and regulators that security controls are not merely deployed but actively enforced, with the audit trail to prove it.

7.3 Positioning Execution Governance Strategically

For CISOs, the strategic case for Execution Governance is straightforward: it is the only security architecture that generates the enforcement evidence the current accountability environment demands. Detection-first security will remain a core component of any mature security program. But it cannot produce proof of enforcement, because it operates on execution that has already occurred.

Execution Governance adds an enforcement layer beneath detection, ensuring that by the time detection systems observe behavior, that behavior has already been governed, restricted, and documented. The result: a security posture that is both more resilient and more provable.

> *Execution Governance transforms cybersecurity from a monitoring model into a provable control model. The future of cyber resilience will be measured by enforceable control.*

8. Execution Governance in Action: A Scenario Walkthrough

Abstract principles are most useful when grounded in practice. The following scenario illustrates the same attack, a targeted ransomware execution, as it unfolds under a detection-first architecture and under Execution Governance.

8.1 The Scenario: A Ransomware Execution Attempt

A finance team employee receives a phishing email containing a link to a document hosted on a legitimate-looking cloud storage service. The document, when opened, drops and attempts to execute an unknown payload. The payload is a novel ransomware variant with no prior signature in any threat intelligence feed.

Stage	Detection-First Architecture	With Execution Governance
T+0	Payload lands on endpoint. No signature match. EDR allows execution to proceed on the live system.	Payload lands on endpoint. Execution Governance intercepts before any system access is granted. Process placed in kernel-level containment.
T+2 min	Ransomware begins enumerating file shares and network drives. No alert has fired. Behavioral analysis window is still open.	Contained process attempts file system enumeration. Containment boundary prevents access to real file shares. Enforcement decision logged and timestamped.
T+8 min	Encryption begins on local drives. Behavioral analysis detects ransomware-like patterns and fires a high-severity alert. SOC notified.	Analysis of contained process completes. Verdict: malicious. Process terminated within containment. Zero files on production systems affected.
T+12 min	SOC begins investigation. Lateral movement detection fires as ransomware attempts to spread via network shares. Incident declared.	Enforcement record generated: unknown process intercepted, contained, analyzed, and terminated. Audit trail available for immediate insurer review.
T+90 min	Containment of infected systems underway. Forensic investigation initiated. Insurance notification process begins.	No incident to contain. No production files affected. CISO has documented enforcement evidence, a complete record of governed execution.
Outcome	**Significant file encryption on live systems before detection. Incident response costs. Insurance claim likely. Proof of control: none.**	**Zero production impact. Complete enforcement audit trail. No insurance claim triggered. Proof of control: documented, timestamped, auditable.**

WHAT THIS MEANS FOR INSURERS

In the detection-first scenario, the CISO has an incident to report and a claim to file. In the Execution Governance scenario, the CISO has an enforcement record to share: documented proof that an unknown threat was governed, contained, and eliminated before production systems were reached. These are fundamentally different risk conversations..

+1 973-859-4000 www.xcitium.com

9. Compliance Framework Alignment

Execution Governance does not operate independently of existing regulatory and compliance frameworks. It directly supports the control requirements CISOs are already accountable for delivering and, in many cases, provides measurable enforcement evidence that standard tooling cannot.

9.1 How Execution Governance Maps to Major Frameworks

Framework	Control References	What the Framework Requires	What EG Provides
NIST CSF 2.0	PR.PS, PR.PT, DE.CM	Protective technology managed to ensure security and resilience; runtime monitoring of endpoints	**Kernel-level enforcement records, containment audit trails, measurable runtime policy enforcement**
ISO 27001	A.8.15, A.8.19, A.5.37	Logging and monitoring of activity; management of technical vulnerabilities; documented operating procedures	**Per-execution enforcement logs, automated containment documentation, auditable governance records**
CMMC 2.0	SI.2, SI.3, CM.2	System and communications protection; malicious code identification; security configuration enforcement	**Runtime enforcement of execution policy, containment of unknown code, configuration compliance evidence**
SOC 2 Type II	CC6.1, CC6.7, CC7.2	Logical access controls; restriction of unauthorized software; system monitoring	**Documented access restriction at runtime, enforcement of software execution policy, continuous monitoring evidence**
HIPAA	164.312(a)	Access controls, audit controls, integrity controls for ePHI systems	**Execution access restriction logs, runtime integrity enforcement, audit trails for systems handling protected data**

+1 973-859-4000 www.xcitium.com

9.2 The Audit Readiness Advantage

A critical and often overlooked benefit of Execution Governance is its impact on audit preparation. Most compliance frameworks require point-in-time evidence: configuration records, access logs, and incident documentation gathered in the weeks before an audit. This creates a recurring operational burden and a fundamental question about whether audit-period evidence reflects normal operating conditions.

Execution Governance generates continuous enforcement evidence as a natural byproduct of normal operation. Every governance decision, containment action, and policy enforcement event is automatically logged throughout the year. When an audit or insurance review arrives, the evidence already exists. The CISO is not assembling documentation. They are presenting it.

AUDIT READINESS
Organizations running Execution Governance enter every audit and insurance review with a continuous, unbroken record of runtime enforcement activity. This shifts the audit conversation from "can you demonstrate that controls exist?" to "here is the evidence that controls operated."

10. Addressing Common Questions

CISOs evaluating Execution Governance typically raise two well-reasoned questions. Both deserve direct answers.

10.1 "We Already Have Zero Trust. Is this the Same Thing?"

Zero Trust Architecture	Execution Governance
Governs identity and network access: who can reach which resources across the infrastructure.	Governs execution itself: what unknown or untrusted code is permitted to do at the operating system level.
Enforces least-privilege at the network, application, and identity layers.	Enforces runtime policy at the kernel level, restricting file system, registry, network, and memory access for governed processes.
Operates as an access control framework. Assumes breach and verifies every request.	Operates as an execution control layer. Governs what code can do regardless of how it arrived on the system.
Does not govern what untrusted code can do once execution has been permitted.	**Directly addresses the enforcement gap that Zero Trust network access leaves at the endpoint execution layer.**

Zero Trust and Execution Governance address different layers of the security stack. Zero Trust controls access to resources. Execution Governance controls what happens when code executes, regardless of whether it arrived through a trusted identity or a compromised one. An attacker who has authenticated through Zero Trust can still execute malicious code on the endpoint. Execution Governance governs that execution.

The practical framing: Zero Trust answers "Who can access this?" Execution Governance answers "What can this code do when it executes?" Both questions matter. Neither answer makes the other redundant.

10.2" We Already Run EDR and XDR. How is this Different?"

EDR / XDR	Execution Governance
Observes execution behavior on live systems and detects threats based on signatures, heuristics, and behavioral patterns.	Intercepts unknown execution before it can access production system resources and governs it within a containment environment.
Fires alerts when suspicious activity is observed. Investigation and response follow detection.	Takes enforcement action before the threat reaches live systems. Containment precedes analysis.

EDR / XDR	Execution Governance
Produces telemetry and alert data: evidence of monitoring activity and response speed.	Produces enforcement records and containment evidence: proof of governance activity and policy enforcement.
By definition, observes execution that has already occurred on the production system. Cannot produce proof of prevention.	**Operates before execution reaches production systems. Generates the enforcement proof that EDR/XDR cannot produce by design.**

EDR and XDR are valuable and should remain part of any mature security program. Execution Governance is not a replacement. It is an additional layer that operates earlier in the execution lifecycle.

EDR produces detection evidence: alerts, behavioral observations, response timelines. These prove the security team is actively monitoring. Execution Governance produces enforcement evidence: containment records, policy enforcement logs, governed execution audit trails. These prove that controls prevented unrestricted execution.

When a cyber insurer asks "Can you prove your execution controls were enforced?" EDR logs answer a different question. Execution Governance answers the one being asked.

THE PRACTICAL RELATIONSHIP
Think of Execution Governance and EDR as complementary layers. EDR watches the perimeter and the environment. Execution Governance governs the execution layer beneath it. Organizations with both have detection capability and enforcement capability, and can prove both to insurers, boards, and auditors.

Conclusion

The cybersecurity accountability model is undergoing a fundamental transformation. Cyber insurers, boards, and regulators are no longer satisfied with monitoring evidence alone. They are demanding proof of enforcement: documented, auditable evidence that execution controls were operationally active and measurably effective.

Detection-first security cannot satisfy this demand by design. It produces evidence of response capability, not enforcement capability. The reporting gap this creates is real, growing, and increasingly consequential for CISOs navigating insurance negotiations and board-level accountability conversations.

Execution Governance closes this gap. By governing unknown execution at the kernel level, generating audit trails of enforcement decisions, and producing the containment evidence that insurers are asking for, it transforms cybersecurity from a monitoring model into a provable control model.

For CISOs who need to answer the question, "Where is the proof your execution controls are working?" Execution Governance is the answer.

Key Principles

"Cyber insurers no longer want proof you can detect attacks. They want proof you can enforce control."

"**Detection proves visibility**. Execution Governance proves enforcement."

"Security tooling is no longer enough. Insurers now expect measurable assurance."

"**Execution Governance** transforms cybersecurity from a monitoring model into a provable control model."

"The future of **cyber resilience** will be measured by enforceable control."

+1 973-859-4000 www.xcitium.com

References

The following frameworks, standards, and publications informed the analysis presented in this white paper.

1. **National Institute of Standards and Technology (NIST).** Cybersecurity Framework (CSF) 2.0, NIST SP 800-53, NIST SP 800-137. Available at nist.gov.
2. **International Organization for Standardization.** ISO/IEC 27001:2022 Information Security Management Systems. Available at iso.org.
3. **Cybersecurity Maturity Model Certification (CMMC).** CMMC 2.0 Framework Documentation. US Department of Defense. Available at dodcio.defense.gov.
4. **American Institute of CPAs (AICPA).** SOC 2 Trust Services Criteria. Available at aicpa.org.
5. **US Department of Health and Human Services.** HIPAA Security Rule (45 CFR Part 164). Available at hhs.gov.
6. **MITRE Corporation.** MITRE ATT&CK Enterprise Matrix v15. Available at attack.mitre.org.
7. **Lockheed Martin.** Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.
8. **Turing, A.M..** On Computable Numbers, with an Application to the Entscheidungsproblem. Proceedings of the London Mathematical Society, 1936.
9. **European Union Agency for Cybersecurity (ENISA).** NIS2 Directive: Measures for a High Common Level of Cybersecurity Across the Union.
10. **Securities and Exchange Commission (SEC).** Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Item 106). 17 CFR Parts 229 and 249.
11. **National Vulnerability Database (NVD).** CVE Statistics and Trends, 2023-2025. Available at nvd.nist.gov.
12. **Xcitium Research. ZeroDwell Containment:** Real-World Endpoint Data from 55,042+ Endpoints. Internal Research Publication, April 2026.

Legal Disclaimer

Regulatory and Legal Compliance

References to regulatory frameworks, compliance requirements, and legal standards in this document are provided for informational purposes only and do not constitute legal advice. Organizations should consult qualified legal counsel and compliance professionals to determine the specific requirements applicable to their circumstances and to evaluate how any technology solution may support their compliance obligations.

Third-Party References

This white paper references certain third-party frameworks, standards, incidents, and data sources including MITRE ATT&CK®, the Cyber Kill Chain®, National Vulnerability Database (NVD), and various regulatory frameworks. All third-party trademarks, service marks, and trade names referenced herein are the property of their respective owners. Such references do not imply endorsement by those parties of Xcitium or its products, nor do they imply endorsement by Xcitium of those parties.

The OpenClaw incident referenced in Section 6 is based on publicly reported research findings. Xcitium makes no independent representation regarding the accuracy of third-party incident reports.

Forward-Looking Statements

Certain statements in this white paper regarding future threat trends, regulatory developments, technology evolution, and market conditions are forward-looking in nature. These statements involve known and unknown risks, uncertainties, and other factors that may cause actual developments to differ materially from those expressed or implied. Xcitium undertakes no obligation to update forward-looking statements to reflect events or circumstances after the date of this publication.

Intellectual Property

The Kernel API Virtualization technology described in this white paper is covered by one or more patents owned by or licensed to Xcitium, Inc. ZeroDwell™ is a trademark of Xcitium, Inc. All other product names, company names, and trademarks mentioned herein are the property of their respective owners.

About Xcitium

Xcitium is a prevention-first cybersecurity company redefining how organizations stop breaches. Unlike traditional security models that rely on detection and response, Xcitium eliminates attacker dwell time through patented ZeroDwell™ Containment technology that virtualizes and isolates unknown threats instantly. By allowing unknown files to run safely in secure, isolated environments, Xcitium removes the risk of compromise without disrupting business operations. This detection-less architecture prevents execution risk before an attack can spread, encrypt, or exfiltrate data.

Xcitium's cloud-native platform delivers Managed Detection and Response, Extended Detection and Response, SOC-as-a-Service, and Managed EDR capabilities backed by 24x7 human-led SOC expertise. Powered by its tri-detection intelligence engine combining static, dynamic, and expert analysis, Xcitium provides trusted file verdicts with zero uncertainty.

Organizations and MSPs rely on Xcitium to achieve zero dwell time outcomes, reduce alert fatigue, strengthen cyber resilience, and align security investments with measurable business impact.

For more information, visit **www.xcitium.com.**

200 Broadacres Drive, Bloomfield, NJ 07003