xcitium

Managed Detection and Response (MDR)

A Better Approach to Managed Detection and Response

Xcitium MDR combines cutting-edge technology with expert human oversight to deliver exceptional security outcomes. Built on our patented ZeroDwell technology and a natively architected platform, Xcitium minimizes the attack surface, eliminates false positive alert fatigue, and ensures fast, effective threat response through 24/7 SOC monitoring.

Incident Response Included

Expertise

Proactive Protection

Unified Platform

Why Choose Xcitium MDR?

Xcitium MDR includes all the traditional layers of endpoint protection alongside ZeroDwell technology. It also incorporates robust RMM and device management tools, making it a comprehensive, co-managed solution. Customers benefit from full visibility into their environments, as our SOC team manages threats from the same portal that customers access. This transparency ensures that while we shoulder the burden of monitoring, reporting, and responding, no telemetry or data is hidden from you.

With full visibility and integrated tools, Xcitium's SOC analysts focus on the most critical threats, ensuring high-fidelity alerts are prioritized and swiftly acted upon. This co-managed approach minimizes risk, reduces disruption, and enhances your organization's overall security posture.

Xcitium MDR Delivers:

- Comprehensive protection with ZeroDwell technology
- 24/7 managed threat hunting and monitoring
- Hands-on Response and Remediation
- Seamless, proactive defense with full customer visibility

The Xcitium Advantage

Peace of Mind: Entrust your security to a team of seasoned experts supported by our patented ZeroDwell technology, which proactively neutralizes unknown threats.

Cost Efficiency: Xcitium MDR streamlines your security operations by consolidating multiple functions into a single, comprehensive managed service—eliminating the need for additional vendors and reducing overall costs.

Unmatched Protection: Delivering superior threat defense, Xcitium MDR goes beyond traditional offerings. Our confidence in ZeroDwell's efficacy means incident response is always included at no extra charge.

Enhanced Visibility: Extend your security with Xcitium Complete, offering deeper network and cloud monitoring by ingesting third-party data sources via syslog to our network sensor. This enables our SOC team to provide guided incident response and remediation, ensuring a proactive and comprehensive approach to threat management.

Contact Us

☎ +1 973-859-4000

www.xcitium.com

Managed Detection and Response (MDR)

ZeroDwell Technology: Patented kernel-level API virtualization isolates and neutralizes unknown threats by securely executing them in a virtual environment that mimics critical system components. This proactive protection eliminates disruptions to business operations.

Native SIEM: Xcitium's natively architected SIEM is fully integrated into the platform, providing advanced log ingestion, correlation, and real-time threat analysis without relying on third-party tools. This ensures seamless operations, enriched insights, and faster response times.

Continuous Endpoint Monitoring and Protection: Ensures continuous monitoring of logs generated by Xcitium's Advanced Endpoint Protection technology. The platform includes natively architected antivirus, HIPS, firewall, and ZeroDwell capabilities, designed to prevent breaches entirely. In cases where rogue endpoints or devices without protection pose a risk, Xcitium's SOC team triages and investigates alert activity to ensure your environment remains secure.

24/7/365 SOC Monitoring and Response: Expert SOC team provides constant monitoring, high-fidelity alerting, and live remediation support. Xcitium's unified platform alleviates the need for an in-house SOC, reducing operational complexity while maintaining unparalleled vigilance.

Threat Hunting and Global Threat Intelligence: Empowered by Xcitium's Verdict Cloud, our SOC team conducts continuous threat hunting and leverages 300+ behavioral alerts to deliver actionable insights, detailed kill-chain reports, and updates on emerging threats.

Integrated RMM and Device Management: Included in Xcitium MDR, our RMM tools enable seamless management of endpoints, remote access, and live remediation. Both customers and SOC analysts can leverage these tools to respond quickly to security events and optimize operational efficiency.

Incident Response at No Additional Cost: Patented proactive defense measures with a full endpoint security stack allows Xcitium to include incident response and remediation as part of the MDR service, with no additional charges, delivering peace of mind.

Streamlined Efficiency and Reduced TCO: Xcitium's natively architected platform combines ZeroDwell, detection, and response minimizing alert fatigue and operational overhead. This holistic approach reduces total cost of ownership while maximizing security outcomes.

Customizable Reporting and Full Visibility: Xcitium provides complete transparency with weekly and monthly reports, threat dashboards, and periodic vulnerability scans. Customers maintain full visibility into their environment while the Xcitium SOC handles the monitoring, reporting, and response.

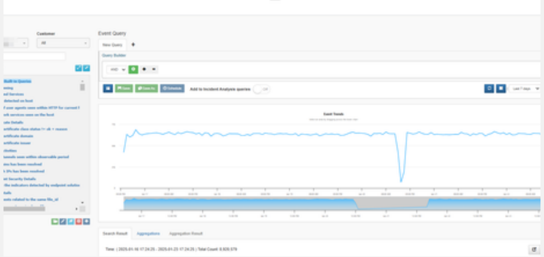
Complete Co-Managed Security: Xcitium MDR empowers customers with full access to their environment through a shared portal. The SOC team operates within the same platform, providing transparency, collaborative management, and peace of mind.

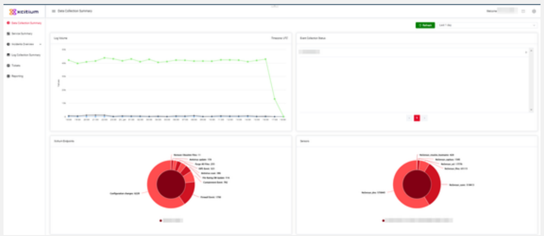
YOUR IMPORTANT FILES, DOCUMENTS, PHOTOS, VIDEOS, DATABASES HAVE BEEN ENCRYPTED!

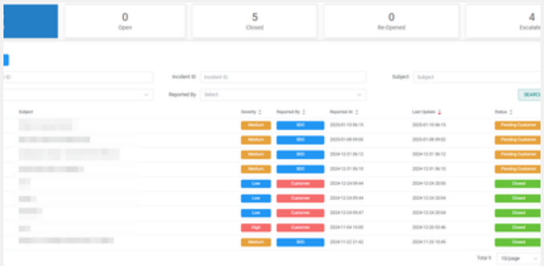
The only way to decrypt and restore your files is with our private key and program. Any attempts to restore your files manually will damage your files.

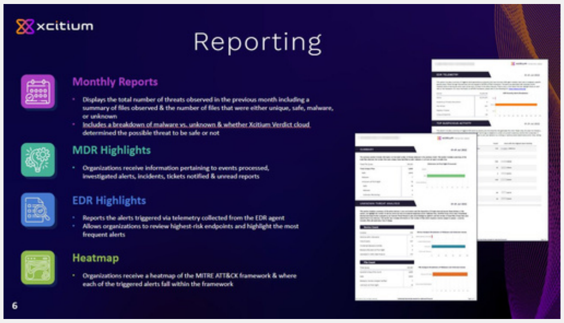
To restore your files follow these instructions:

1. Download and install Tor Browser from https://torproject.org/
2. Run Tor Browser
3. In the tor browser open website: [illegible]
4. On the website enter your recovery id: RECOVERY ID: [illegible]
5. Follow the instructions









Reporting

Monthly Reports

- Displays the total number of threats observed in the previous month including a summary of files observed & the number of files that were either unique, safe, malware, or unknown
- Includes a breakdown of malware vs. unknown & whether Xcitium Verdict cloud determined the possible threat to be safe or not

MDR Highlights

- Organizations receive information pertaining to events processed, investigated alerts, incidents, tickets notified & unread reports

EDR Highlights

- Reports the alerts triggered via telemetry collected from the EDR agent
- Allows organizations to review highest-risk endpoints and highlight the most frequent alerts

Heatmap

- Organizations receive a heatmap of the MITRE ATT&CK framework & where each of the triggered alerts fall within the framework

Contact Us

+1 973-859-4000

www.xcitium.com