Executive Overview

- Headquarters: Bloomfield, NJ
- Formerly known as Comodo Security Solutions
- Over 850 Cyber Security Scientists and Engineers
- 27 Patents
- 6,000+ customers
- Zero breaches to date

Product & Service Offerings

- Unlimited Incident Response
- Endpoint Detection and Response, EDR
- Managed Detection and Response, MDR
- Extended Detection and Response, XDR
- Dedicated TAM Resources
- Endpoint Firewall
- Patch Management
- Web Protection
- Email Protection
- Security Information & Event Management, SIEM
- Vulnerability Management
- Anonymous Behavioral Monitoring and Alerting
- Anti-Virus
- Data Loss Prevention
- Domain Monitoring
- Forensics & Analysis, Internal
- Intrusion Detection Services, IDS
- Ransomware Services
- Remediation Services
- Security Assessment & Audit
- Security Optimization
- Unified Threat Management, UTM

Sales Engineer Take On Best Fit

Xcitium is formerly Comodo Security Solutions and has over 6,000 customers so they are often overlooked. They have 27 patents and claim zero breaches to date. They offer an Endpoint Protection Platform with Detection & Response (EDR), a fully managed EDR that they call MDR with 24/7 SOC AND a $1M Warranty included and they also offer a full XDR solution around their EDR and log ingestion & network sensor which includes the warranty. They have a patented solution called Zero Dwell which indentifies unknown threats and run them in a virtualized session to see if they are harmfull before allowing them to access endpoints - if they are deemed as malicious they prevent access across the entire environment in minutes. This is a huge differentiator and they are the only one's doing detection this way. They will work with any size customer and have favorable minimums. They have some of the friendliest customer facing team members I have seen. -Rick Mischka, Cybersecurity FSE

Key Features & Differentiators

- **ZeroDwell Containment Technology:** Patented technology that prevents the execution of unknown threats, ensuring zero breaches when fully configured.
- **Unified Zero Trust Platform:** A comprehensive platform that integrates EDR, ITSM, RMM, XDR, MDR, CNAPP, and SIEM, offering seamless security across endpoints, networks, and cloud environments.
- **Advanced Threat Detection and Response:** Proactive threat hunting, 24/7 SOC services, and incident response through managed detection and response capabilities.
- **Cloud-Native Application Protection (CNAPP):** Continuous monitoring and protection of cloud workloads, including CSPM, KSPM, and CWPP features.
- **Compliance and Reporting:** Automated compliance dashboards and reporting tools that help organizations meet industry standards like PCI-DSS, HIPAA, and GDPR.

Top Industries Served

- Other

Ideal Customer Profile

Xcitium's ideal customer is an **SMB or mid-market enterprise** that requires robust cybersecurity solutions without the complexity and high costs typically associated with legacy systems. They typically lack the large, in-house IT security teams of larger enterprises and are seeking a comprehensive, integrated solution that can protect endpoints, networks, and cloud environments with minimal operational disruption.

Key characteristics include:

- **Size**: Companies with 50-1,000 employees.
- **Industry**: Healthcare, financial services, retail, manufacturing, education, and any other sectors with stringent data protection regulations.
- **Pain Points**: Struggles with managing multiple disjointed security products, compliance challenges, limited IT security resources, and a need for simplified, effective cybersecurity solutions.
- **Roles/Titles**: IT Directors, CISOs, CTOs, and Managed Service Providers (MSPs) who are responsible for securing their organization's infrastructure and ensuring compliance.

Qualifying & Technical Questions

- How are you currently managing cybersecurity across your endpoints, network, and cloud environments?
- What challenges are you facing with your current security setup, particularly in terms of compliance and threat detection?
- Do you have the in-house resources to manage a complex cybersecurity infrastructure, or would you benefit from a more integrated and automated solution?
- How important is reducing alert fatigue and simplifying your security operations to your organization?