

Features Breakdown



EPP Capabilities		
Signature-based anti-malware protection	✓	✓
Machine learning/algorithmic file analysis on the endpoint	✓	✓
Machine learning for process activity analysis	✓	✓
Process isolation	✓	✓
Memory protection and exploit prevention	✓	✓
Protection Against Undetected Malware	✓	✗
Application whitelisting	✓	✓
Local endpoint sandboxing/endpoint emulation	✓	✗
Script, PE, or fileless malware protection	✓	✓
Integration with on-premises network/cloud sandbox	✓	Requires additional product(s)
Real-time IoC search capabilities	✓	✓
Retention period for full access to data	No limit	30 days
Endpoint Firewall	✓	✓
FW Learning Mode	✓	✗
Automatically creates network traffic rules	✓	✗
URL Filtering	✓	✓
Host Based IPS	✓	✓
USB device Control	✓	✓
Full Device Control (Device Control based on Device Class product ID, Vendor ID and Device Name)	✓	✓
Agent self-protection/remediation or alerting when there is an attempt to disable, bypass, or uninstall it	✓	✓
Ransomware protection	✓	✓
Protect/block ransomware when "Offline" or "Disconnected" from the internet?	✓	✗
VDI support	✓	✓
Manage, and maintain, an application control database of known "trusted" applications?	✓	✓
Multi-tenant cloud based service	✓	✓
EPP management console available as an on-premises virtual or physical server/application	✓	✗
Consolidated EPP management console to report on, manage, and alert for Windows macOS clients and mobile	✓	✓
Data loss prevention	✓	✓
Mobile Device Management	✓	Requires additional product(s)
Mobile threat Defense	✓	Requires additional product(s)
Vulnerability and patch management	✓	Requires additional product(s)
Network/Cloud sandboxing	Cloud Sandbox	Requires additional product(s)
Security Orchestration, Analysis and Response (SOAR) Integration	✓	✓
Network discovery tool	✓	✗
Remote Access	✓	✗
Remote scripting capabilities	✓	✗
Default Deny & ZeroThreat Virtualization		
Default Deny Security with Default Allow Usability	✓	✗
Run unknown files with ZeroThreat Virtualization Protection	✓	✗
Create Virtual environment for any unknowns	✓	✗
Virtualize file system, registry, COM on real endpoints	✓	✗
EDR		
Telemetry (observables)		
Interprocess Memory Access	✓	✓
Windows/WinEvent Hook	✓	✓
Device Driver Installations	✓	✓
File Access/Modification/Deletion	✓	✓
Registry Access/Modification/Deletion	✓	✓
Network Connection	✓	✓
URL Monitoring	✓	✓
DNS Monitoring	✓	✓
Process Creation	✓	✓
Thread Creation	✓	✓
Inter-Process Communication (Named Pipes, etc) up to this	✓	✓
Telemetry data itself can be extended in real time	✓	✗
Event chaining and enrichment on the endpoints	✓	✗
Detection/Hunting/Reporting		
Adaptive Event Modelling	✓	✗
Behavioral analysis (e.g. analysis over active memory, OS activity user behavior, process/application behavior, etc.)	✓	✓
Static analysis of files using capabilities such as machine learning (not including signature based malware detection)	✓	✓
Time-series analysis	✓	✓
Integration with automated malware analysis solutions (sandboxing)	✓	✗
Threat Hunting interface or API for searching with YARA/REGEX/ElasticSearch/IOC	Yes without Yara	IOC / Regex
Support for matching against private IOC	✓	✓
Threat Intelligence integration (TIP, upload, webservice connector, etc) to enrich and contextualize alerts	✓	✓
Linking telemetry (observable data) to recreate a sequence of events to aid investigation	✓	✓
Process/attack visualization	✓	✓
Incident Response Platform (IRP) or orchestration integration?	✓	✓
Vulnerability reporting (ex. reporting on unpatched CVEs)	✓	✓
Alert prioritization based on confidence, able to define thresholds for alerting.	✓	✓
Alert prioritization factors system criticality	✓	✓
Able to monitor risk exposure across environment organized by logical asset groups	✓	✓
Reporting interface identifies frequent alerts that may be appropriate for automating response	✓	✓
Response		
Remote scripting capabilities	✓	✗
Quarantine and removal of files	✓	✓
Kill processes remotely	✓	✓
File retrieval	✓	✓
Network isolation	✓	✓
Filesystem snapshotting	✓	✓
Memory snapshotting	✓	✓
MDR		
Managed endpoints		
Manage customer endpoints and policies	✓	✗
Incident Investigation & Response	✓	✓
Preemptive containment	✓	✗
Application profiling (AI support)	✓	✓
Customizable policy creation	✓	✗
Central monitoring of all endpoints	✓	✓
Live remote inspection	✓	✓
Tuning of monitoring rules for reduction of false positives	✓	✗
Forensic analysis	✓	✓
Managed network		
Cloud-based SIEM and Big Data Analytics	✓	✗
Log data collection/correlation	✓	✗
Threat intelligence integration	✓	✗
Network profiling (AI support)	✓	✗
Available as virtual or physical	✓	✗
Integrated file analysis (cloud sandbox)	✓	✗
Full packet capture	✓	✗
Protocol analyzers for 40+ different protocols such as TCP, UDP, DNS, DHCP, HTTP, HTTPS, NTLM, etc. w/full decoding capability	✓	✗
Managed cloud		
Includes ready-to-use cloud application connectors for:		
Azure	✓	Requires additional product(s)
Google Cloud Platform	✓	Requires additional product(s)
Office 365	✓	Requires additional product(s)
AWS	✓	Requires additional product(s)
Threat detection for cloud applications	✓	✗
Log collection from cloud environments	✓	Requires additional product(s)
Generating actionable incident response from cloud application	✓	✗
Threat intelligence and Verdict		
Holistic security approach Combined network, endpoint, cloud	✓	✗
Internal security sensor logs (IOCs)	✓	✓
Expert Human Analysis	✓	✗
ML & Behavioral Analysis and Verdict	✓	✓
Open source threat intelligence feeds	✓	✓
Information sharing with industry	✓	✓
Clean web (phishing sites, keyloggers, spam)	✓	✓
Deep web (C&C servers, TOR browsers, database platform archives—pastebins)	✓	✓
Cyber Adversary Characterization	✓	✗
Security operations center (SOC)		
Global, real-time support (24 / 7 /365)	✓	✓
Dedicated cybersecurity expert	✓	✓
Breach (case) management	✓	✓
Security monitoring	✓	✓
Incident analysis	✓	✓
Incident response (handling)	✓	✓
Extensive threat hunting (scenario-based)	✓	✓

About Xcitium

Xcitium, formerly known as Comodo Security Solutions, is used by more than 3,000 organizational customers & partners around the globe. Founded with one simple goal to put an end to cyber breaches, Xcitium's patented 'ZeroThreat' technology uses Kernel API Virtualization to isolate and remove threats like zero day malware & ransomware before they cause any damage. ZeroThreat is the cornerstone of Xcitium's endpoint suite which includes advanced endpoint protection (AEP), endpoint detection & response (EDR), and managed detection & response (MDR). Since inception, Xcitium has a zero breach track record when fully configured.

1-888-551-1531 • sales@xcitium.com • support@xcitium.com