

Wie sichert und kontrolliert Cyber Crucible Endpunkte?

Kurze Antwort: Auf zwei Arten. Das Produkt selbst ist eine autonome Endpunktschutzlösung, die auf Kernel-Ebene arbeitet, und Cyber Crucible kontrolliert seine eigenen Unternehmens- und Entwicklungsendpunkte im Rahmen eines formalen Programms. Beides basiert darauf, dass der privilegierteste Code intern entwickelt wird.

Produkt-Endpunktschutz

Das Produkt bietet autonomen Schutz vor Ransomware, speicherbasierten (dateilosen) Angriffen und Prozessinjektion, durchgesetzt auf Kernel-Ebene. Es ist bewusst von Betriebssystembibliotheken entkoppelt, sodass das Produkt auch dann weiterläuft, durchsetzt und meldet, wenn Angreifer diese Bibliotheken im Arbeitsspeicher kompromittieren oder kapern. Da Erkennung und Reaktion lokal ausgeführt werden, bleibt der Schutz auch bei einem Ausfall des Management-Backends oder in einer bewusst air-gapped Bereitstellung bestehen.

Integrität der Lieferkette und unabhängige Validierung

Die Erkennungsalgorithmen, Kernel-Heuristiken, Sensoren und Treiber werden intern entwickelt und gepflegt; es sind keine unüberprüften Drittanbieterbibliotheken oder versteckten Telemetrie-Hooks in der Software eingebettet. Da die Komponente mit den höchsten Privilegien firmeneigen ist, wird eine ganze Klasse von Risiken durch Drittanbieter-Lieferketten beseitigt und nicht nur verwaltet. Alle Windows-Kernel-Treiber werden im Rahmen des Windows Hardware Compatibility Program (WHCP) von Microsoft validiert und signiert.

Kontrollen für Unternehmensendpunkte

Verwaltete Endpunkte folgen genehmigten sicheren Konfigurationsbaselines, führen Endpunktschutz und Scans aus und wenden dieselben Kontrollen auf Wechsel- und tragbare Medien wie auf feste Medien an, wobei die unbefugte Nutzung von Medien eingeschränkt ist. Die Softwareinstallation unterliegt einer Richtlinie, Daten im Ruhezustand auf Endpunkten werden verschlüsselt, und Endpunkte werden im Rahmen des Patch-Management-Programms aktuell

gehalten.

Ausrichtung an Rahmenwerken und die ehrliche Grenze

Die Endpunktkontrollen richten sich an den CIS Critical Security Controls (v8) und NIST SP 800-53 (SI-3, CM-2, MP-7) aus. Es wird keine Zertifizierung beansprucht. Detaillierte Konfigurationsstandards und Nachweise werden Prüfern unter NDA zur Verfügung gestellt.

Revision #1

Created 2026-07-24 23:30:51 UTC by Dennis Underwood

Updated 2026-07-24 23:30:51 UTC by Dennis Underwood