

# Business Continuity: ChromeOS & Chrome Enterprise Premium

A rapid-deployment Business Continuity solution using ChromeOS and Chrome Enterprise Premium (CEP). Ensures critical operations continue during ransomware attacks via Zero Trust access. Features Context-Aware Access, deep content inspection and data isolation on managed or BYOD devices, preventing lateral malware movement while preserving forensic evidence.

## Features

- ▶ **Clean Room** isolated recovery environment for critical operations.
- ▶ Chrome Enterprise Premium for deep content inspection and DLP.
- ▶ Zero Trust Context-Aware Access policies (Device/User/Location).
- ▶ Rapid deployment **Break Glass** protocols.
- ▶ Secure BYOD enablement via managed CEP browser profiles.
- ▶ Ransomware-resilient, read-only OS architecture.
- ▶ Rapid conversion of Windows devices to ChromeOS Flex Identity Provider integration (Okta, Entra ID, Google).
- ▶ Disaster Recovery playbook design and simulation workshops.

## Benefits

- ▶ Designed to restore operational continuity during major cyber/ransomware incidents rapidly.
- ▶ Prevents lateral malware movement via isolated browser environments.
- ▶ Enables secure access from unmanaged devices (BYOD).
- ▶ New version: AI-powered threat detection and Protection against malware, phishing and malicious websites.
- ▶ Malware deep scanning: in-depth scanning to identify and block malicious threats.
- ▶ Device and posture checks: limiting sensitive data access for non-compliant devices.
- ▶ Rapid Recovery Time Objective (RTO) for executive command.
- ▶ Data Loss Prevention (DLP): prevents your data from leaving your organisation.
- ▶ Scalable recovery from Gold Command (Executives) to the broader workforce.
- ▶ Low-cost **insurance policy** compared to the costs of operational downtime.

