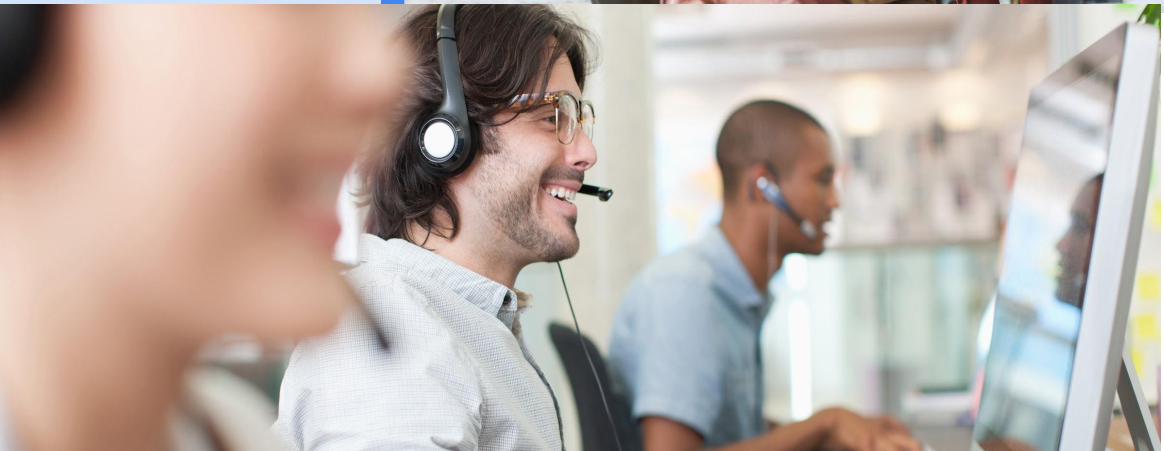
Protect your business with ChromeOS—the most secure OS out of the box[1]



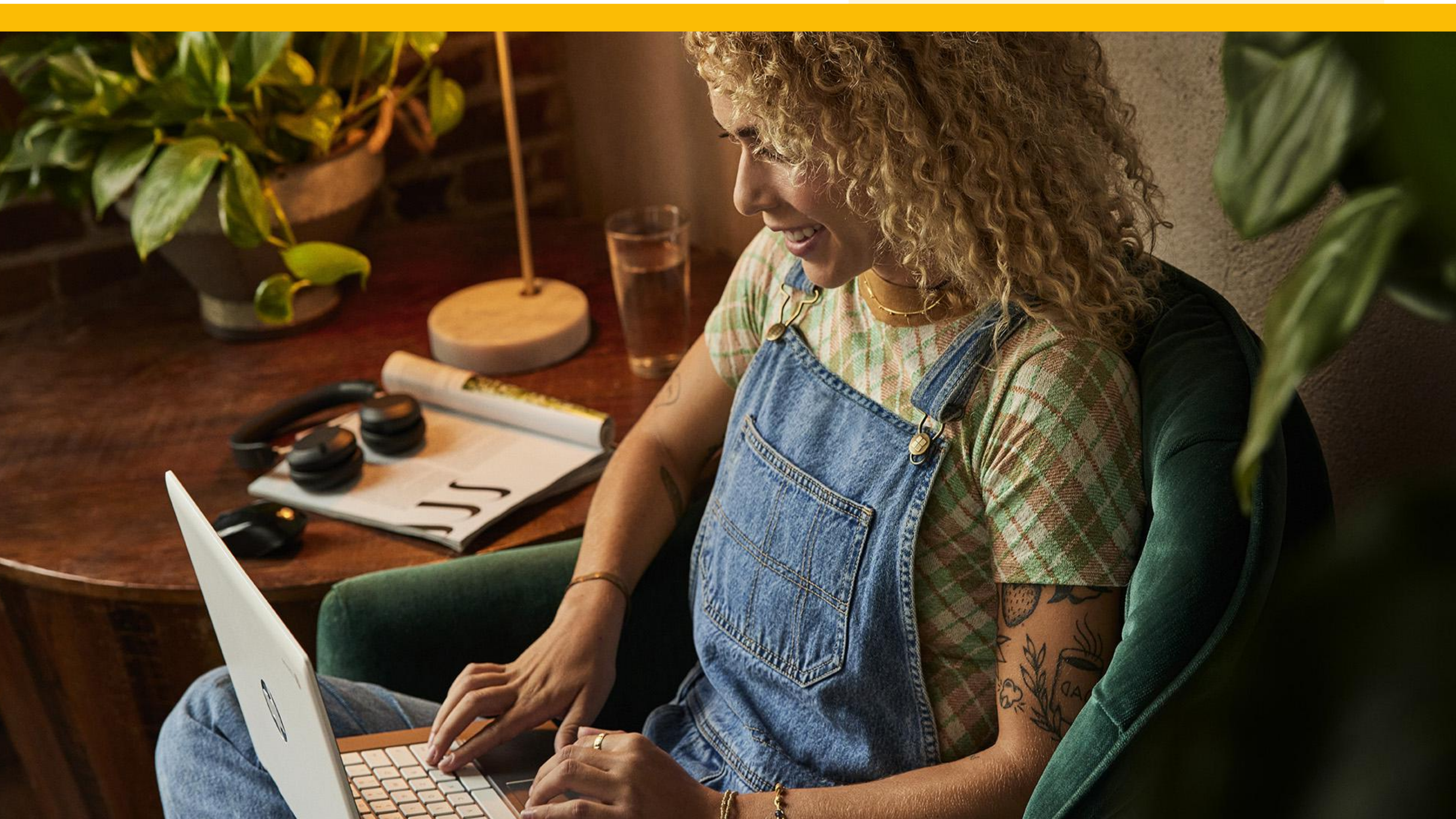
[1] Atredis Partners Google ChromeOS Competitive Analysis, 2024

As employee mobility increases so does the possibility of compromising data. Project plans, patient data, customer information, financial documents, and code fly across secured and unsecured networks every millisecond. This is the data that **your enterprise depends on.**

The average cost of a data breach is over

$4.88M

Average Cost of Data Breach Report, Statista, 2024



chromeOS

Protect your data with ChromeOS Data Controls

ChromeOS Data Controls enable IT and security teams to identify and mitigate data loss risk on ChromeOS endpoints. Admins can set up rules to prevent data leakage based on the data source, the destination, wherever it is being moved to, and whoever is moving data.

These data controls help stop risky behaviors like:

- Copying and pasting
- Screenshotting
- Screen recording
- Screen sharing
- Printing

IT and security teams can identify and mitigate data loss risk and prevent leakage by setting up data control rules based on various scenarios.

Where the data comes from

Source-based rules protect valuable data stored in business-critical locations, apps, or softwares. Within minutes, rules can be set up to prevent using the data or information from an HR or accounting platform.

Where the data is going

Destination based rules prevent data from being pasted and shared externally. For example, admins can set up a rule to prevent data from being pasted into personal email, blogs, social media, websites or apps.

Who is moving the data

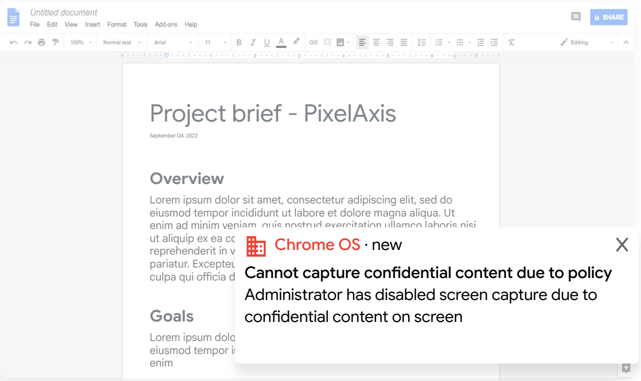
User-based rules prevent accidental errors by blocking certain users or groups from sharing data. To maintain productivity, other users can be allowed to copy, paste, print, and screenshot important data for work purposes.

chromeOS

Quick and simple information protection

ChromeOS Data Controls empower security admins to:

- Automatically turn on the electronic privacy screen when a user is viewing content
- See data control events and their reports when they happen
- Report, warn, or block users at any moment
- Prevent pasting information from Workspace to external platforms
- Block screen sharing on specific Chrome or web apps



Project brief - PixelAxis

September Q4, 2022

Overview

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea co reprehenderit in v pariatur. Excepteu culpa qui officia d

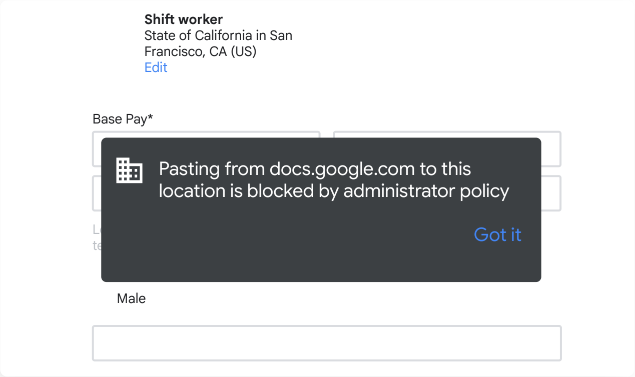
Goals

Lorem ipsum dolo eiusmod tempor i enim

Chrome OS · new

Cannot capture confidential content due to policy

Administrator has disabled screen capture due to confidential content on screen



Shift worker
State of California in San Francisco, CA (US)
Edit

Base Pay*

Pasting from docs.google.com to this location is blocked by administrator policy

Male

Tap into the power of Chrome Enterprise Recommended

Work with what you have—ChromeOS integrates seamlessly into your existing security and identity stack.

Data Controls events are available within the SIEM reporting tool of your choice

Identity and Access

netskope, onelogin, okta, cisco, Duo

Endpoint Management

BlackBerry, cisco, Duo, SAMSUNG, SAMSUNG Knox Manage, omnissa

Security Insights and Reporting

CROWDSTRIKE, CORTEX XDR, paloalto networks, Ping Identity, splunk>

Extended detection and response

CROWDSTRIKE