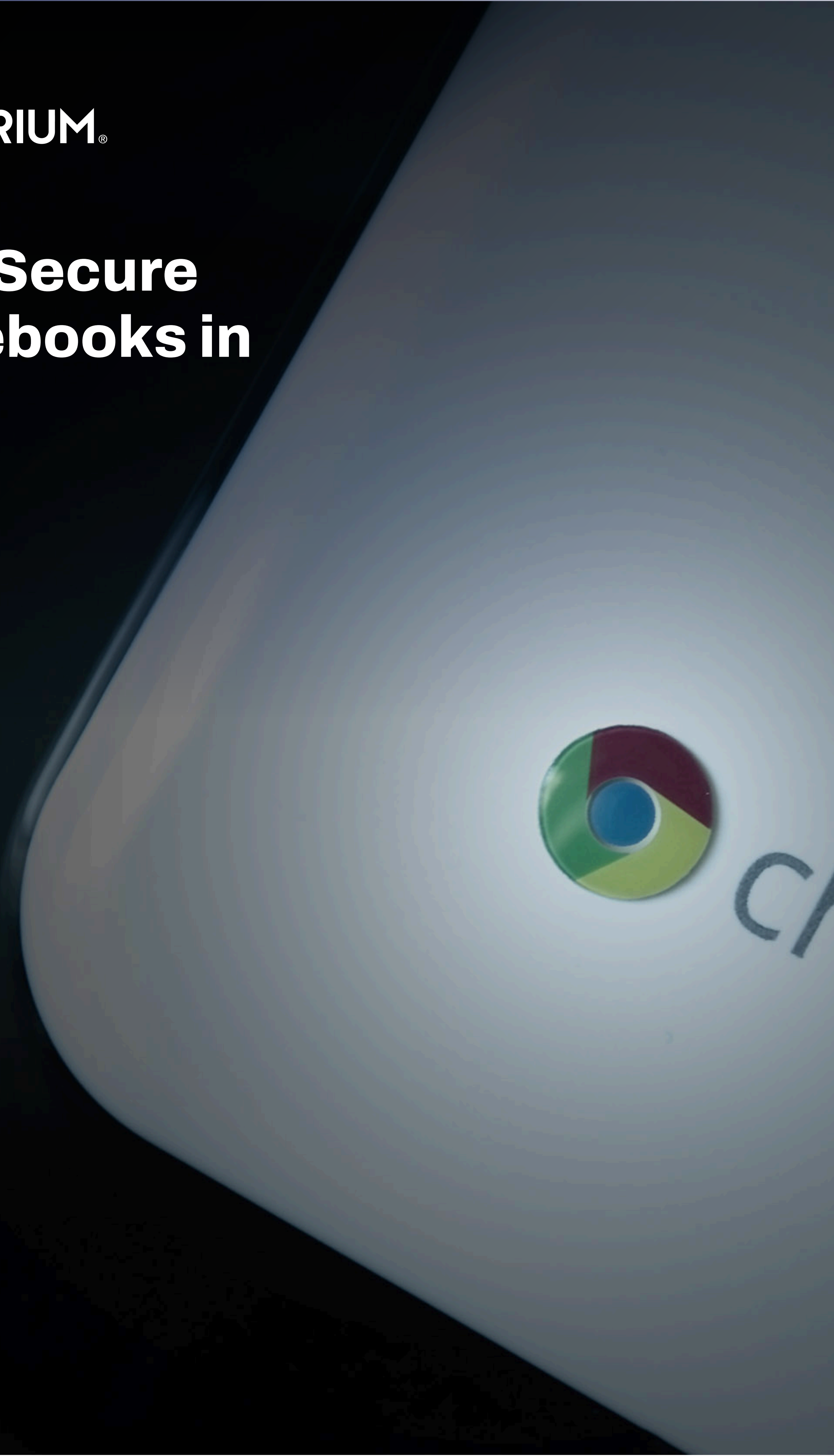
ZIMPERIUM®

How to Secure Chromebooks in 2022



Introduction

Chromebooks have become ubiquitous in the enterprise, educational, public sector, and other environments. By the end of 2021, over 40 million estimated Chromebooks will be shipped and deployed to classrooms, boardrooms, and homes worldwide. Versatile, affordable, and technically capable, these mobile endpoints continue to make their mark on the notebook market in all sectors. Like other platforms that have achieved widespread adoption, Chromebooks have the attention of malicious actors and can present significant cybersecurity risks when not properly secured.

In 2020, Chromebooks outsold Macbooks globally due to their low costs and ability to quickly meet and scale with the rise in distributed data access and productivity needs. With many of the services and software needs offloaded to the cloud, Chromebooks provide stability, scalability, and increased security over legacy systems.

Chromebooks have become integral to educational institutions as well as enterprises around the world. But as with all connected devices, risks against data still exist.

To realize the goal of technology adoption with security confidence and secure and critical data accessed through these mobile Chromebooks, enterprises, public sector and education institutions need advanced mobile security and threat defense.

Chromebooks Create Information Security Risk

As organizations have begun embracing the platform in record numbers, data shows ChromeOS is on target to become the No. 2 operating system among laptops. Like all platforms, Chromebooks are vulnerable to cyberattacks, presenting security and compliance risks to organizations of all sizes.

Even before 2020, organizations embraced Chromebooks at rapid rates. At the beginning of 2019, K-12 students accounted for over 30 million Chromebooks, and adoption continues to rise as classrooms adopt connected technologies. While the education market is the biggest driver of Chromebook adoption, supply constraints in 2020 and 2021 have forced enterprises to look to these notebooks to fill mobile employee needs. The Chromebook Enterprise market is now expected to account for 30% of business endpoints deployed by 2023.

Unfortunately, this increase in adoption and usage will introduce proportionate increases in mobile privacy and security risks and threats, including:

- Phishing attacks resulting in stealing the identity of the user
- Network attacks where personal information is accessed
- Malicious malware in apps taking control of microphones and cameras
- Compromised extensions stealing personal and private data

Introducing zIPS for Chromebooks

As Chromebooks are increasingly adopted by a variety of different industries, they must be secured with the same level of technology and rigor as other endpoints. Zimperium zIPS for Chromebooks delivers advanced, mobile threat defense capabilities to ChromeOS and provides vital protection to the many organizations and educational institutions embracing this always-connected endpoint.

Zimperium zIPS for Chromebooks is an advanced mobile threat defense solution for enterprises, providing persistent, on-device protection to corporate-owned and BYOD devices. It detects both known and unknown threats, including zero-day, phishing, and network attacks, by analyzing slight deviations to a mobile device's various system parameters. Once deployed to ChromeOS, zIPS for Chromebook begins protecting the device against all primary attack vectors, even when the device is not connected to a network.

Zimperium zIPS for Chromebooks actively detects and remediates ChromeOS endpoints against the attack vectors targeting Chromebooks today with security layers built on machine-learning technology. Delivering on-device detection and determination, zIPS for Chromebook provides critical security to any enterprise and educational institution, including the following capabilities:

- Identify and prevent users from accessing phishing sites
- Filter and limit access to harmful web content
- Detect malicious WiFi networks and alert users to disconnect from the suspicious network
- Assess all Android apps for undesired violations of privacy or insecure development practice

With Zimperium zIPS for Chromebooks, administrators finally have centralized visibility into any attacks, enabling swift remediation, and events can be correlated and viewed in external SIEM and data collection services.

As the mobile attack surface continues to expand and evolve, so does Zimperium's on-device, machine learning-powered detection. Built on the z9 machine learning platform, zIPS detects threats across the kill chain: device, network, phishing, and app attacks.

How do we solve the problem?

Detection
Device, Network, Apps & Phishing threat detection

Visibility
Proactive visibility into risks and vulnerabilities

Remediation
On-device remediation and UEM driven compliance actions

Threat Intelligence
Deep forensics for Threat Hunting & Incident Response

Key Features and Enterprise-Grade Capabilities

Zimperium zIPS for Chromebook's on-device, machine learning-powered detection is capable of scaling with the needs of the modern workforce, securing devices against even the most advanced threats. With a privacy-first approach to data processing, this advanced mobile endpoint security solution enables enterprises to support and secure BYOD devices without sacrificing the end user's data.

Zimperium's advanced mobile threat defense solutions provide mobile endpoint security to enterprises and governments around the world. Built with advanced threat security in mind, zIPS for Chromebooks meets the mobile security needs of enterprises and governments around the world.

PHISHING
APPS
WI-FI
SOFTWARE
SETTINGS
DEVICE

- **Powered by Machine Learning** On-device, machine learning-based detection provides prevention against the latest mobile threats, including zero-day malware.
- **Critical Data, Where You Need It** With integrations into enterprise SIEM, IAM, UEM, and XDR platforms, administrators always have the data they need.
- **Deploy Anywhere** Address local data laws and compliance needs by deploying to any cloud, on-premise, or air-gapped environments.
- **Zero-Touch Deployment** Deploy and activate Zimperium zIPS on your employees' and contractors' mobile endpoints without the need for complicated activation steps by the end-user.
- **Critical Data** Comprehensive device attestation enables enterprises to have a complete picture of their mobile endpoint security and shores up Zero Trust architectures through existing integrations.
- **Complete Mobile Coverage** No matter the mobile device, from tablet to phones, Zimperium provides complete security coverage across Android, iOS, and ChromeOS.
- **Dynamic Content Filtering** Minimize web-based threats through advanced detection and prevention for malicious and risky sites through 70 content categories and granular policies.

About Zimperium

Zimperium, the global leader in mobile security, offers the only real-time, on-device, machine learning-based protection against Android, iOS, and Chromebook threats. Powered by z9, Zimperium provides protection against device, network, phishing, and malicious app attacks. For more information or to schedule a demo, contact us today.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244