Zero Trust with Chrome Enterprise Premium

Adopt a zero trust model to secure your remote workforce, save money, and reduce risk.

SPECIALIZATION

Security

Google Cloud

OVERVIEW

Improve your organization's security posture and save money by implementing a zero trust security model that provides secure access to applications and data based on user and device identity rather than traditional perimeter-based security. Onix's zero trust consulting services provide guidance that helps organizations plan, design, implement, and manage their Chrome Enterprise Premium environments for Workspace and Google Cloud.

KEY FEATURES

Identity and context-aware access control

Configure and implement policies to enforce granular access controls to applications, VMs, and APIs.

Integrated threat and data protection

Prevent data loss and thwart threats such as malware and phishing. Utilize real-time alerts and detailed reports.

Support in the cloud, on-prem, or both

Securely and easily access SaaS apps, private web apps, and cloud resources on Google Cloud, on other clouds, or on-premises.

Reduce costs and streamline support

Retire legacy, perimeter-based security platforms and related services and overhead.

Data Loss Prevention

Understand risks and configure controls to improve data protection across the user base using Chrome.

CAPABILITIES

- Agentless deployments
- No new software required
- BYOD and non-employee use cases
- Native malware/phishing capabilities
- Built-in data insights
- Device telemetry
- Strong partner ecosystem

- New DLP capabilities that leverage AI/ML to classify information
- Native zero trust access for SAML-based apps
- Cost management
- VPN replacement strategy
- Simplified licensing and pricing

BUSINESS OBJECTIVES

- Improve security
- Simplify management
- Gain more insights
- Protect sensitive data
- Save money

Take the next step.

To learn more about Onix's zero trust offering with CEP, get in touch with our team of experts:

sales@onixnet.com