



ENDPOINT SECURITY

• REAL-TIME PREVENTION

• OS-LEVEL ENFORCEMENT

• ON-DEVICE AI FORENSICS

• AIR-GAP FRIENDLY

Real-time endpoint security enforced inside the operating system - stopping credential theft, ransomware and data exfiltration before data leaves the device.

ABOUT 1STPROTECT

1stProtect is a real-time endpoint security platform that enforces protection inside the operating system itself, stopping credential theft, ransomware and data exfiltration at the moment they happen rather than after an alert.

Its modular engine line - more than 18 engines including CredentialProtect, RansomProtect and ExfilProtect - pairs OS-level enforcement with an on-device AI investigation engine that performs forensics and automated response locally, without sending sensitive data to the cloud.

Traditional endpoint tools detect attacks and respond after the fact, and the window between alert and action is where the damage happens. Because 1stProtect investigates and enforces on the endpoint itself, it also fits organizations with strict data-sovereignty requirements or limited connectivity.

THE PROBLEM

Detection-and-response finds out about the breach after the data is gone. The window between alert and action is where the damage happens.

HOW 1STPROTECT SOLVES IT

1stProtect enforces policy inside the operating system and stops credential theft, ransomware and exfiltration in real time.

CAPABILITIES

CredentialProtect

Blocks credential theft at the operating-system level - tokens, hashes and secrets stay where they belong.

ExfilProtect

Stops sensitive data from leaving the endpoint - at the moment of theft, not hours after the alert.

RansomProtect

Recognizes and halts encryption behavior in real time, before file systems are damaged.

On-endpoint AI investigation

Local forensics, root-cause analysis and automated response on the device itself. Nothing sensitive is sent to external systems.

QUICK FACTS

FOUNDED: 2025, San Francisco (launched at RSAC 2026) LEADERSHIP: Kervin Pillay (CEO), Rafel Ivgi (CTO)

FUNDING: \$20M - Andra Capital & All Blue Capital

ENGINES: 18+ incl. CredentialProtect · RansomProtect · ExfilProtect · SelfProtect · LensGuard

WHO BUYS IT CISOs, SOC managers, infrastructure leads

See 1stProtect *on your own terms.*

1stProtect is distributed by Cyberdis: a demo tailored to your environment, or a full proof of concept - run by a Cyberdis engineer, sold through channel partners.

cyberdis.io/vendors/1stprotect/

info@cyberdis.io