SecureLint

Browser Security & Data Protection Brochure 2026

Real-time API key masking, phishing & brand-impersonation detection, SSL verification, and enterprise email DLP — 100% local in your browser

Stops secrets, phishing & data leaks before they ever leave the browser

Summary

Browsers have quietly become the riskiest surface in modern work. Every API key pasted into a code editor, every login link opened in Gmail, every credential typed into a SaaS form passes through the same browser tab — usually with no security layer watching it at all.

SecureLint closes that gap. It is a lightweight, agentless browser extension that detects and masks exposed secrets in real time, flags phishing and brand-impersonation attempts before a page finishes loading, verifies SSL and domain trust, and blocks risky outbound data transfers — all without sending a single byte of your content to an external server.

This brochure walks through how SecureLint protects individual developers and entire enterprise teams, the detection engine behind it, and what's included across the Pro and Enterprise plans.

What Makes SecureLint Different

Most security tools either watch network traffic or scan files after the fact. SecureLint works at the point of action — inside the browser tab, as you type, paste, click, and send — and does all of its analysis locally. Nothing you type, mask, or scan is ever transmitted to a SecureLint server, making it safe to use even on the most sensitive credentials, customer data, and source code.

Why Teams Choose SecureLint

1

Secrets Are Masked the Instant They Appear

100+ detection patterns catch AWS, GCP and Azure credentials, JWT tokens, database connection strings, private keys, and Stripe/Twilio/SendGrid keys the moment they're typed or pasted — masking them before they're ever visible on screen.

2

Phishing Is Blocked Before the Page Loads

A 14-layer engine checks domain age, SSL validity, redirect chains, and lookalike branding against 500+ tracked brands in 100+ languages — flagging fake sites and spoofed senders in milliseconds.

3

Outbound Data Leaks Are Stopped at the Send Button

Enterprise Email DLP intercepts Gmail, Outlook and Yahoo Mail sends that contain secrets or sensitive data heading to a personal domain — masking the content and blocking the send before it leaves the inbox.

4

Every Call Gets a Privacy Sweep

Meeting Mode detects active Zoom, Google Meet or Teams sessions and automatically blurs API keys and credentials across every open tab — so nothing sensitive is ever visible on a shared screen.

5

Zero Data Ever Leaves the Browser

Detection, masking and phishing analysis run 100% locally. No keystrokes, secrets or page content are transmitted to a SecureLint server — making it safe for the most regulated, security-conscious teams.

Core Protection Pillars

Four engines run in parallel, silently, on every page you visit:

1

Instant Secret Detection & Masking

100+ regex and AI-assisted patterns scan every keystroke across CodeMirror, Monaco, Ace, Notion, Jira, Confluence and any contenteditable field — masking secrets the moment they appear, with context-aware partial masks for dev tools and full masks for writing apps.

2

Phishing & Brand-Impersonation Detection

Real-time SPF/DKIM/DMARC analysis, link risk scoring and AI brand detection identify fake sites, spoofed senders and lookalike domains for any company worldwide — before you ever click.

3

Enterprise Email DLP

When an employee tries to send company data to a personal domain, SecureLint blocks the send button, masks the sensitive content and notifies the IT admin — closing the most common accidental-leak channel.

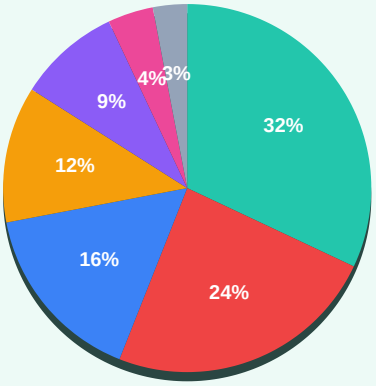
4

SSL, Domain & Wallet Protection

Live SSL certificate and DNS verification, domain-age alerts, clickjacking and pastejacking shields, and 15+ known crypto wallet-drainer kit signatures keep every tab safe from emerging web threats.

What SecureLint Catches

SecureLint's 14-layer engine watches for far more than leaked keys. Across a protected browser, detections break down into a broad mix of credential, phishing, and web-threat categories — all handled locally, in real time.



Detections by Threat Category

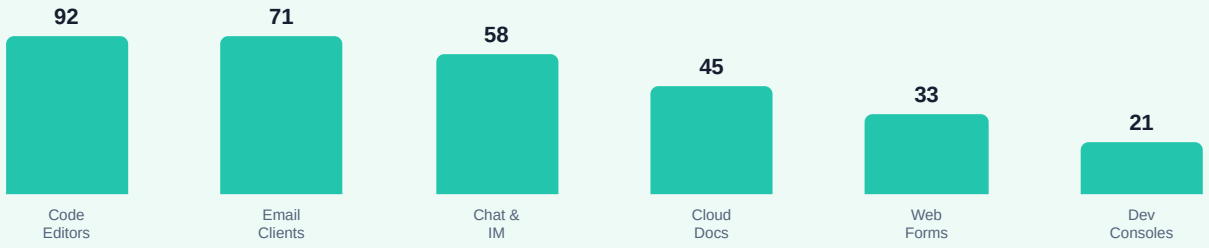
representative mix across a protected browser

- Exposed Secrets & API Keys
- Malicious / Risky Links
- Clickjacking & Pastejacking
- Other Web Threats
- Phishing & Brand Impersonation
- SSL & Domain Issues
- Crypto Wallet Drainers

Where Secrets Get Masked

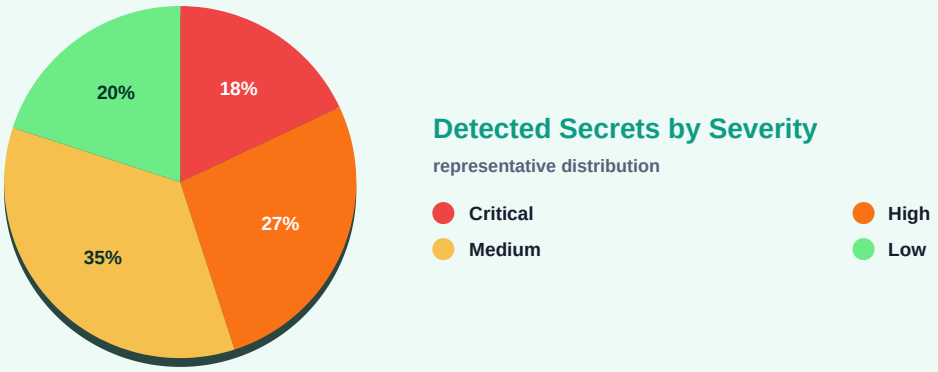
Secrets don't only leak from code. SecureLint masks them everywhere they appear — from editors and email clients to chat, cloud docs, and web forms.

Secrets Masked by Source App (typical workday)



Every Finding, Triaged

SecureLint doesn't just flag secrets — it scores each one Critical, High, Medium or Low, so teams fix the most dangerous exposures first. A live per-session counter shows exactly what was caught and when.



Why Severity Triage Matters

Not every detection carries the same risk. A live production AWS secret or database connection string is an immediate, critical exposure; a low-entropy token in a sandbox may simply need awareness. By scoring every finding the moment it appears, SecureLint turns a noisy stream of alerts into a clear, ranked work list.

For security teams, this means triage happens automatically. Critical and High findings can trigger blocking and admin notification, while Medium and Low findings are masked and logged for review — all without a single secret leaving the browser. The result is faster response on what matters most, and far less alert fatigue.

Key Capabilities

1

Real-Time Secret Masking — 100+ Patterns

Detected secrets are replaced with ████ blocks the moment they appear. The original stays in memory and is masked on-screen — nothing leaves the tab. Every finding is scored Critical, High, Medium or Low so you know exactly what to fix first.

2

Phishing Detection With 0–100 Trust Scores

Every inbound email is silently scanned: SPF, DKIM and DMARC signals checked, links scored for threat probability, and attachments fingerprinted. 500+ brands tracked for impersonation across 100+ languages — flagged in milliseconds.

3

Meeting Mode — Auto-Blur on Every Call

The moment SecureLint detects an active Google Meet, Zoom or Teams session, it blurs API keys and credentials across every open tab — and lifts the blur instantly when the call ends. No scrambling before a screen share.

4

Enterprise DLP, Dashboards & Audit Logs

Outbound send blocking, centralized incident dashboards, custom policy management and full audit logs with user attribution give security teams workforce-wide visibility — all while data stays local in each browser.

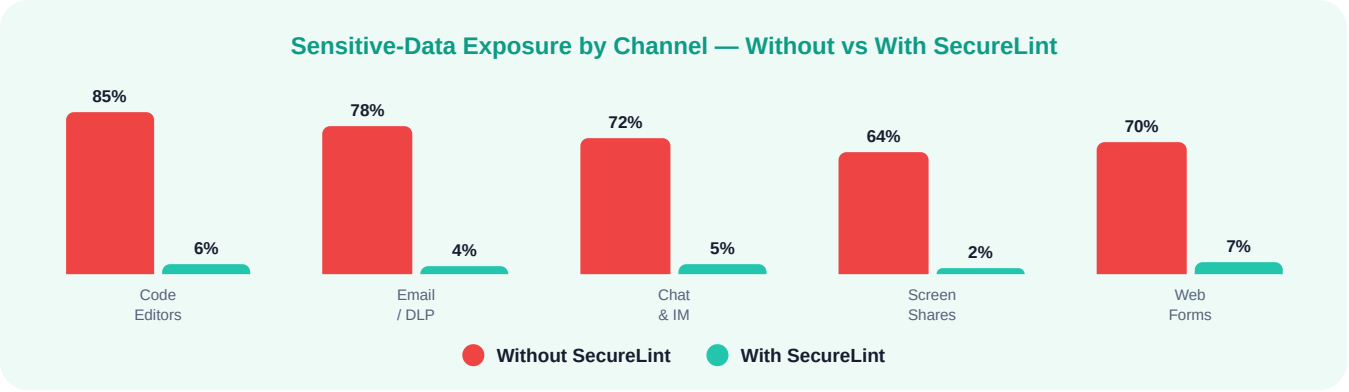
SecureLint by the Numbers

> **One agentless extension replaces a stack of point tools — and keeps every check inside the browser.**

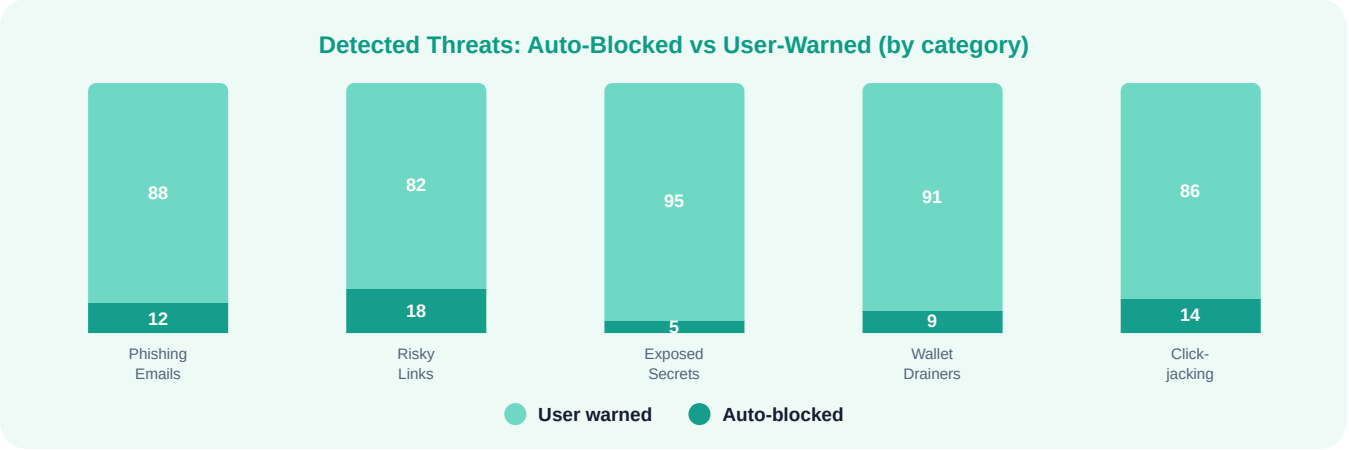
100+ Security checks run on every page load	**500+** Brands tracked for impersonation
14 Detection layers running in parallel	**0** Bytes of your content sent to any server

The Difference It Makes

The clearest way to see SecureLint's impact is to compare sensitive-data exposure on the same channels before and after it's installed. Residual exposure drops to near zero as secrets are masked, sends are blocked, and screens are swept.



How SecureLint Handles Threats



For the highest-confidence threats — exposed live secrets, wallet drainers, confirmed phishing — SecureLint acts decisively, blocking the action before it can cause harm. For lower-confidence or judgement-call cases, it warns the user with a clear trust score and lets them decide.

Block When It's Clear, Warn When It's Not

A good browser security layer has to balance protection with productivity. Block too aggressively and people disable the tool; warn too softly and threats slip through. SecureLint resolves this by tying its response to confidence: deterministic signals like a matched drainer kit or a live secret pattern are auto-blocked, while probabilistic signals like an unusual sender or a young domain surface a warning and a 0–100 trust score.

Because every decision is made locally and in real time, there's no round-trip to a server and no waiting. The user stays in flow, the dangerous actions are stopped, and security teams get a complete, attributable record of what was blocked, what was warned, and why.

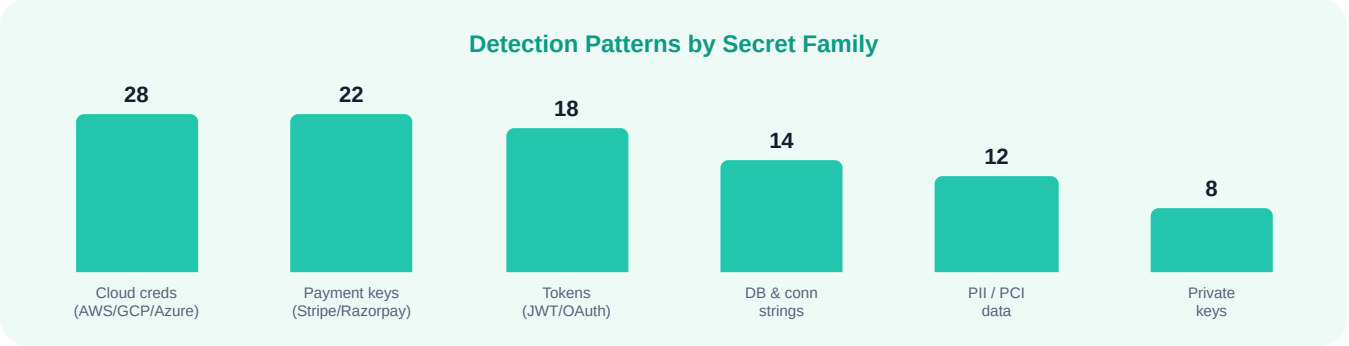
Detection Coverage

Broad enough to catch what matters — precise enough to score every finding.

100+ Secret detection patterns	**14** Engine layers in parallel	**500+** Brands tracked
100+ Languages for scam detection	**15+** Known wallet-drainer kits	**4** Severity levels scored

100+ Patterns, Grouped by Secret Family

SecureLint's pattern library spans the full range of credentials developers handle daily — from cloud provider keys to payment secrets, tokens, database strings, and regulated PII.



Catches Phishing Before You Click

Every inbound email is silently scanned — SPF, DKIM and DMARC signals checked, every link scored for threat probability, and attachments fingerprinted. You see a clear 0–100 trust score before you ever open anything.

⚡

SPF · DKIM · DMARC

Signal analysis on every inbound message, flagging weak or failed sender authorisation instantly.

🔗

Link Hover Scanner

Hover any link in Gmail, Outlook or webmail to see its trust score before you ever click.

👤

Reply-To Spoofing

Flags replies that silently redirect to free mail domains — a classic credential-harvest signal.

🧠

AI Brand Detection

Identifies any company worldwide in 100+ languages and verifies the domain actually matches.

🌐

Homograph & Typosquat

Catches lookalike domains using IDN homograph tricks and typo-based impersonation.

📋

Clipboard & Click Guard

Blocks pastejacking and invisible click-hijacking overlays before they can act.

Privacy by Design

All scanning, masking and phishing analysis happens locally inside the browser. SecureLint never reads, stores or transmits your secrets — no tracking, no ads, no third-party SDKs.

Security Best Practices

> **Whether you run a two-person dev team or a global security organisation, these five habits — backed by SecureLint — contain the riskiest data leaks at the browser:**

Mask Secrets at the Source, Not After the Leak

Keep SecureLint active in every editor and email client so credentials are masked the instant they appear — before they reach a screen share, a chat window, or a commit. Detection at the point of typing is far cheaper than cleaning up an exposed key.

Treat Every Inbound Link as Untrusted

Use the link hover scanner and 0–100 trust scores before clicking. Let SecureLint check SSL validity, domain age, redirect chains and brand match in real time, so a convincing lookalike never gets the click.

Turn On Meeting Mode for Every Call

Auto-blur API keys and credentials across all open tabs the moment a Zoom, Meet or Teams session begins. Demos, interviews and live reviews stay productive without ever exposing secrets on a shared screen.

Enforce Email DLP Across the Team

Block outbound sends of secrets or PII to personal domains and route incident alerts to IT admins. The most common accidental leak — the wrong recipient on a sensitive email — is stopped at the send button.

Keep Everything Local

Rely on 100% in-browser processing so sensitive data is analysed without ever being transmitted. Local-only detection removes a whole class of third-party risk and dramatically simplifies compliance and audit.

Simple, Transparent Pricing

One Pro plan with everything included — choose the billing period that suits you. Longer commitments save more. Teams that need DLP, dashboards and admin controls can talk to us about Enterprise.

MONTHLY

₹499/mo

₹499 billed monthly

QUARTERLY

₹449/mo

₹1,347 billed quarterly

10% savings

Most Popular

ANNUAL

₹334/mo

₹4,008 billed yearly

33% savings

Every Pro plan includes

- ✓ Real-time phishing detection on every page
- ✓ API key & secret detection — 100+ patterns
- ✓ AI brand detection in 100+ languages
- ✓ Clickjacking & pastejacking protection
- ✓ SSL certificate & domain-age checks
- ✓ AWS, GCP, Azure & JWT credential masking
- ✓ Password breach monitoring (HaveIBeenPwned)
- ✓ Multi-layer AI engine with auto failover

Enterprise

Email DLP & send blocking · admin dashboard · custom policies · audit logs · unlimited team members · dedicated support & SLA

Contact Sales

One Extension. Every Browser.

SecureLint is delivered as a lightweight, agentless browser extension with no impact on browsing speed or user experience.

Chrome
Available

Edge
Coming Soon

Firefox
Coming Soon

Safari
Coming Soon

For Individuals & Developers

Universal Editor Support
CodeMirror, Monaco, Ace, Google Docs, Notion, Jira & more

Context-Aware Masking
Partial masks in dev mode, full masks in writing mode

Password Breach Monitor
Checks against HaveIBeenPwned in real time, privacy-safe

Wallet Drainer Detection
15+ known crypto drainer kits flagged before they connect

For Security & IT Teams

Email DLP & Send Blocking
Blocks outbound sends to personal domains, notifies admins

Centralized Dashboard
Masked-secret and phishing events across the workforce

Custom Policy Management
Define what's blocked, masked or escalated per team

Audit Logs & Reporting
Full attribution for compliance and incident review

Start Protecting Your Secrets in Seconds.

Install SecureLint and get real-time API key masking, phishing protection and SSL verification — instant, private and zero-config.

Install Extension — Get Started →

🖥 100% Local Processing 🚫 No Tracking or Ads 🔐 No Third-Party SDKs