DATASHEET

Certificate Monitoring.

Know before any certificate expires, across your domains, services, and internal infrastructure.

DOCUMENT	Product Datasheet
PRODUCT	Certificate Monitoring
PUBLISHED	July 2026
PRICING	$0.01 per host per day · portal.generatorlabs.com/signup

Certificates expire on a date printed inside them, and they still take down sign-ins, APIs, and checkouts every week, because renewals fail silently and nobody is watching the result. Certificate Monitoring is the independent check: it validates the certificate a real client actually receives from every endpoint you run, around the clock, and warns you with days to spare instead of minutes.

01

Why Monitor

Maximum certificate lifetimes are being phased down from 398 days to 47 by March 2029, multiplying renewals roughly eightfold. Renewal automation helps, but it fails through its environment, dependencies, permissions, and policy, and it fails silently. The average organization already reports nine certificate-related incidents a year, each taking hours to find and fix.

Lifetime schedule: CA/Browser Forum ballot SC-081v3. Incident figures: Keyfactor, 2024 PKI & Digital Trust Report.

47 days	9	5.3h
MAX LIFETIME BY 2029	INCIDENTS PER YEAR	TO FIND AND FIX EACH

02

Every check validates what a connecting client sees, independent of your issuance and renewal tooling.

What It Checks

`expiry`	**Expiration**	Continuous expiry tracking with alert thresholds you set anywhere from 0 to 90 days before a certificate lapses, so renewals become scheduled work.
`trust`	**Chain and Identity**	Full certificate chain validation, hostname and Subject Alt Name matching, and revocation status, the failures that break clients even when the date looks fine.
`config`	**Configuration**	Cryptographic algorithm strength and DNS CAA record configuration, caught before an auditor or an outage finds them.
`change`	**Change Detection**	Fingerprint monitoring alerts you when a certificate is renewed, replaced, or changed unexpectedly, whether or not you made the change.

03

TLS is not just HTTPS: mail, directory, and file transfer services carry certificates too, and fail just as silently.

Where It Checks

Every TLS Service	HTTPS, SMTPS, IMAPS, and LDAPS, plus STARTTLS for mail (SMTP, IMAP, POP3), directory (LDAP), and file transfer (FTP).
Behind Load Balancers	Checks every IP behind a hostname, so one node serving a stale certificate cannot hide behind its healthy neighbors.
Private Networks	On-premise agents monitor internal endpoints and internal CAs, the certificates that fail quietest.
Monitoring Profiles	Group hosts with shared settings and thresholds, and manage everything in the portal or over the REST API.

04

Notification channels include email, Slack, SMS, and webhooks,

Alerts, Evidence, and Pricing

When a check fails or an expiry approaches, alerts go out through your choice of more than a dozen channels, including email, Slack, SMS, and webhooks. Compliance

with contact groups and scheduling.

dashboards summarize every monitor into valid, expiring, expired, and error, with per-period check history suitable as continuous-monitoring evidence for SOC 2, PCI DSS 4.0, and HIPAA audits.

Pay for What You Monitor

Certificate Monitoring is $0.01 per host per day. No plans, no tiers, no per-check surprises: add an endpoint and it is watched 24/7.

Certificate Monitoring runs on the same Generator Labs platform as Blacklist Monitoring, with shared contacts, alerting, and API access. Spot-check any hostname for free at mrdns.com/ssl-check.

Know Before It Expires

Add an endpoint and Generator Labs Certificate Monitoring will validate its certificate around the clock: expiry, chain, identity, and configuration, with alerts where your team works.

portal.generatorlabs.com/signup