NicSRS Launches sslTrus CaaS – A Powerful SSL Automation Tool for SMBs

As certificate lifespans shrink, NicSRS delivers a lightweight, automated solution tailored for SMBs—helping reduce complexity, avoid outages, and stay secure.

NicSRS Launches sslTrus CaaS

HONG KONG, HONG KONG, March 17, 2026 /EINPresswire.com/ -- NicSRS, a leader in cloud-based security distribution and PKI automation, today announced the launch of sslTrus CaaS (Certificate-as-a-Service), a groundbreaking lightweight solution designed to automate and streamline the lifecycle management of SSL certificates. The complexity of managing certificates manually has become a critical vulnerability as the 199-day SSL has officially been implemented since March 15th. With the introduction of sslTrus CaaS, NicSRS is setting a new standard for efficiency and security.

sslTrus CaaS Introduction
Focusing on automated SSL certificate management, sslTrus CaaS provides a lightweight solution for users with 1-10 SSL certificates. This service supports the automatic application, deployment, and renewal of certificates during the subscription period. Leveraging continuous monitoring and alerts, it proactively ensures the secure and reliable use of certificates. Users can flexibly choose between cloud push or installing an Agent (clmBot) based on their deployment environment to achieve full lifecycle automation of certificate management, completely avoiding the risk of service interruptions caused by expired certificates and inadequate management.

Core Features of sslTrus CaaS

- Automation Made Possible for Even 1 Certificate
Even with just 1 certificate, users can get started with sslTrus CaaS automation immediately. Over the past few years, there have been some more expensive and complicated solutions created to help with the certificate management for large enterprises. However, it needs to be addressed that SMBs with limited budget and maintenance staff also need certificate automation, and especially so as the certificate lifespans get shorter. sslTrus CaaS now presents

itself as an ideal choice for individual developers, startups, and SMBs, etc.

- Automatic and Unified Workflow
The entire certificate lifecycle management can be achieved within a single sslTrus CaaS subscription, from SSL application, issuance, deployment, reissuance to revocation. This unified, automated workflow ensures continuous business operations and allows users to scale security with ease, all while reducing operational overhead.

- Certificate Monitoring
sslTrus CaaS acts as a “guardian”. It provides a three-tier monitoring mechanism that continuously monitors the validity and security of SSL certificates.
#CT Log mionitoring: Scans the public Certificate Transparency logs of major CAs worldwide. If an unauthorized certificate is issued, the users will be notified immediately to prevent malicious domain hijacking.
#OCSP monitoring: Real-time checks on certificate revocation status; Immediate alerts are triggered if a certificate is revoked by a CA, preventing the use of invalid certificates.
#SSL deployment status monitoring: Proactively scans certificates in actual use, verifying their validity periods and configuration statuses.

- Multiple CAs and SSL Types Supported.
sslTrus CaaS includes an sslTrus DV SSL for free, and users can upgrade to OV or EV SSL, or select from other CA SSLs based on their own needs. It’s far more flexible than other products as sslTrus CaaS has already integrated with various CAs, including GeoTrust, PositiveSSL, GlobalSign, and sslTrus, etc. If the users have such an automation need, they don't have to change the SSL brand they’re using.

- Supreme Convenience Without Compromising Security
Traditional automation tools often require passwords or SSH keys for servers where SSL certificates are deployed, which in itself introduces new security risks. sslTrus CaaS only requires deploying the clmBot on the client end to complete the deployment of SSL certificates. No password is needed. The clmBot will automatically scan the web server, identifies the location of SSL certificates (such as Nginx configuration directories or Apache configuration files) and the protected websites, and completes the automated deployment and configuration of SSL certificates.

- Broad Compatibility
sslTrus CaaS ensures smooth deployment across the existing infrastructure, with seamless integration for mainstream operating systems, web servers (such as Apache, IIS, Tomcat, and Nginx) and cloud services.

NicSRS pointed out that with the implementation of 199-day SSL started on March 15th, it has become imperative to implement certificate automation without delay. "It‘s forseeable that there

will be more and more service interruptions caused by poor certificate management. This year the maximum validity has been shortened to 199-day, and next year it will be 100 days, and in 2029 just 47 days. The time to move from manual processes to fully automated management is not next year—it is right now."

Andrea Cao
NicSRS
email us here
Visit us on social media:
LinkedIn
