Synopsys complements regular expression pattern matching with application context and language semantics to detect many types of secrets that can put your systems and data at risk if they end up in the wrong hands.

- Passwords
- Access tokens
- SSH keys
- API keys
- Cloud provider secrets
- Generic secrets
- Source code
- Configuration files
- Scripts
- IaC templates
- Text files

Synopsys scans for more than 200 specific secrets patterns that are associated with popular technologies, such as AWS, Docker, and GitHub. This protects integrations with these systems from being exploited.

However, according to "The State of Secrets Sprawl, 2023" report, 67% of secrets detected in public repositories in 2022 were found using generic secrets scanning techniques. Generic scans identify text strings that resemble commonly used secrets without needing to define these patterns in advance. This is an effective complement to specific secrets detection, as these scans don't require advanced knowledge of what you're looking for and can help uncover vulnerabilities that would otherwise slip through the cracks. Synopsys combines specific secrets scans and generic secrets scans to

ty is early in4.5e deelDpmeenUpeloeeeSU