Use Case

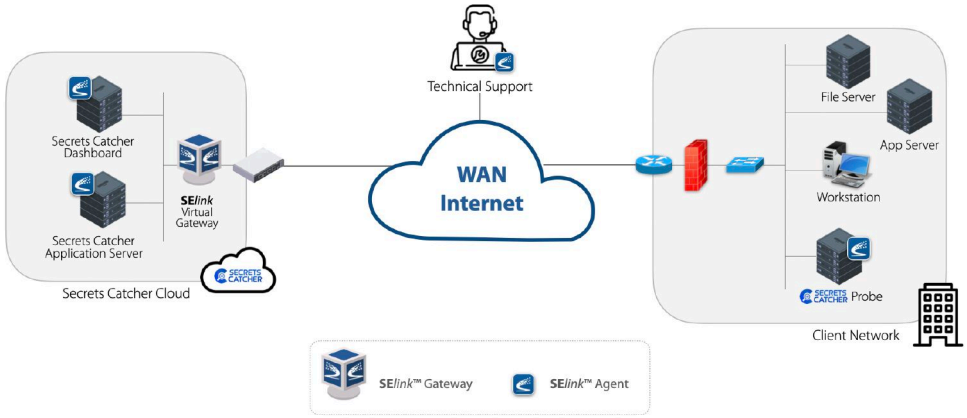
The Zero Trust Defence for Sensitive Credentials

Challenges

Secrets Catcher is an AI-powered cybersecurity solution designed to protect organisations from exposed credentials within network shares and other critical systems. By automatically scanning files and network shares for improperly stored passwords and sensitive data, it uses AI algorithms to evaluate and assign a risk score to each discovered credential. The tool plays a crucial role in preventing privilege escalation, safeguarding Active Directory, and fortifying the IT infrastructure against attacks leveraging compromised credentials. However, challenges remain in addressing broader risks, such as securing communication channels where secrets are transmitted, ensuring continuous protection for secrets in transit, and integrating with legacy systems. Open ports and network layer security also pose significant risks, as attackers can exploit these vulnerabilities to move laterally across systems. Additionally, managing secrets at scale across distributed environments can be complex, highlighting the need for complementary solutions to close open ports, strengthen network security, and enhance end-to-end protection and operational efficiency.

Solution

SElink enhances **Secrets Catcher** by securing the platform communication channels where sensitive information, such as API keys, passwords, and tokens, is transmitted. Powered by Zero Trust Network Access (ZTNA), SElink minimises reliance on multiple firewalls and routers through innovative techniques like port lockdowns and strategic VPN replacement. By enabling secure client-to-client (C2C) connections, it eliminates the need for broad subnets and complex setups. SElink's dynamic micro-segmentation and continuous advanced authentication ensure protection for secrets in transit and at rest, even over poor networks. Its seamless integration with existing infrastructure, including legacy systems, improves operational efficiency, enhances security, and simplifies compliance, all while providing full control over the secure infrastructure and data.



Sector

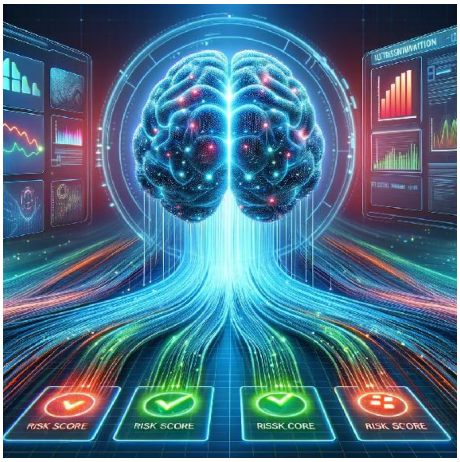
Networks Cyber Security

Objectives

- Mitigate Credential Exposure Risks
- Protect against lateral movements
- Enforce security policies
- Prevent exfiltration and data loss
- Employ micro-segmentation to contain potential breaches and protect assets
- Automate threat detection and remediation workflows
- Compatibility with existing security tools
- Real-time insights into credentials usage

Results

- End-to-End secured credentials
- Data and Network isolation
- Continuous monitoring for immediate action
- **Improved Threat response time**
- **Network Credentials security enhanced for compliance**



Business Unit Creative is an Italian leader in Offensive Security and Cyber Threat Intelligence, enabling organisations to build dedicated cybersecurity business units. It offers services such as red team testing, digital risk assessments, penetration testing, and AI-driven honeypots monitored by its Italian SOC.

Blu5 Group
info@blu5group.com
www.blu5group.com

SECRETS CATCHER

What is Secret Catcher

Secrets Catcher is an advanced, AI-powered cybersecurity solution designed to safeguard organisations against the risks posed by exposed credentials in network shares and other storage environments. Leveraging cutting-edge artificial intelligence and machine learning algorithms, Secrets Catcher identifies, assesses, and mitigates threats associated with improperly stored passwords and sensitive information. The tool automatically scans files across the network to detect embedded credentials, hardcoded secrets, or other sensitive data that could be exploited by attackers. Through intelligent analysis, it assigns a dynamic risk score to each finding, prioritising threats based on potential impact and likelihood of exploitation. This empowers security teams to focus on the most critical vulnerabilities first

How it works

1. Credential Discovery

- Automatically scans files, network shares and repositories for improperly stored passwords and sensitive data
- Advanced pattern recognition to detect credentials, such as usernames, passwords, API and encryptions keys

2. AI-Powered Risk Analysis

- Uses sophisticated AI algorithms to evaluate the criticality and impact of discovered credentials.
- Assigns a risk score to each item, prioritising the most urgent threats

3. Threat Prevention

- Identifies vulnerabilities that could lead to privilege escalation
- Protects critical systems like Active Directory, databases and cloud environments from credential-based attacks and lateral movements

4. Remediation & Mngmt

- Displays findings in a centralised dashboard for visibility
- Provides automated workflows and step-by-step guidance to securely eliminate or mitigate exposed credentials

5. Continuous monitoring

- Continuously monitors credential exposure risks across distributed, hybrid and dynamic IT environments
- Adapts to evolving infrastructure and ensures scalable management of credentials and associated vulnerabilities

6. Reporting

- Generates detailed, customisable reports aligned with industry standards and regulations including ISO 27001, GDPR, NIS2, and PCI DSS
- Maintains an extensive audit trail for internal and external security assessments and external reviews

Why Secrets Catcher

- ✓ Stop threats before they happen
- ✓ Uncover hidden risks in seconds
- ✓ Tailored to meet your organization's unique needs
- ✓ Gain a clear view of your organization's security posture