CHECKRED SECURITY

SoW and Value Proposition Document

Complete Cloud Security

SSPM | CNAPP | CSPM | CIEM | CWPP | ADPM | KSPM | DNSPM | Compliance

CheckRed LLC
5220 Spring Valley Dr. Ste 604
Dallas, TX 75254

checkred.com

sales@checkred.com

Introduction

CheckRed is a fast-growing SaaS and cloud security company that is committed to simplifying security complexities, detecting risks, and strengthening resilience. We empower our clients with the context they need to protect their SaaS and cloud environments. As your partner-in-security, our SSPM, CNAPP, CSPM, CIEM, CWPP, ADPM, KSPM, DNSPM, and compliance capabilities will help your organization focus on improving risk security posture.

CheckRed offers a single platform that manages the risk and compliance posture for both - SaaS and cloud environments. With an emphasis on simplicity, complete visibility, scanning & alerting capabilities, and efficient remediation workflows, CheckRed meets the security needs of all enterprises and provides visibility / professional service workflows for organizations.

The CheckRed framework

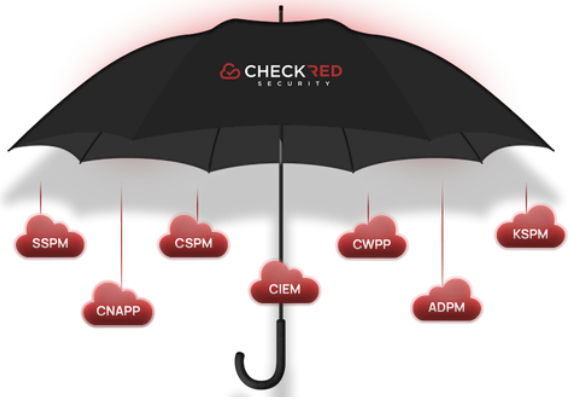
A reimagined approach to cloud and SaaS security

1. **Inspect**: Audit your cloud and SaaS asset inventory based on customized rules with the help of agentless scanners
2. **Detect**: Uncover any risk with a high degree of accuracy and gain total visibility into cloud and SaaS assets
3. **Prioritize**: Classify alerts based on their severity and steer your focus toward issues that matter the most
4. **Remediate**: Receive personalized recommendations for each detected alert in the form of remediation workflows
5. **Report**: View all pertinent security information on a single dashboard and use the ticketing system to respond to alerts

Complete Cloud Protection in One Platform

SSPM + CNAPP + CSPM + CIEM + CWPP + KSPM + ADPM + DNSPM + Compliance

Our commitment to providing SSPM ,CNAPP, KSPM, ADPM and DNSPM under one umbrella has set us apart in the industry, allowing organizations to streamline their security operations and gain comprehensive visibility into their cloud environments.



SaaS Security Posture Management (SSPM)		
1	**Identity access management**	Include multi-factor authentication (MFA), single sign-on SSO, third-party user access, domain authentication and legacy authentication protocols.
2	**Data leakage protection**	Ensure correct configuration to protect against data leakage from any user account.
3	**Access control for external users**	Ensure that the configurations are set correctly for external users to be verified and trusted. Enforce limited access and permissions.
4	**Third Party App Risk**	Offers visibility into the associated third-party applications and the access / permissions that have been granted.
5	**Privacy control**	Allow teams to check the configurations that control visibility between coworkers and service providers.

CheckRed LLC
5220 Spring Valley Dr. Ste 604
Dallas, TX 75254

checkred.com

sales@checkred.com

Cloud-Native Application Protection Platform (CNAPP)

CNAPP is an all-encompassing platform that integrates **CSPM, CIEM, and CWPP** functionalities. This unified approach provides the necessary tools and resources to monitor threats, identify vulnerabilities early on, and take swift action to secure your applications, ultimately leading to a more proactive and streamlined security posture.

Cloud Security Posture Management (CSPM)		
1	**Multi-Cloud Visibility**	A comprehensive view across cloud platforms providing empowered and context-aware visibility in a dynamic environment.
2	**Assess & Prioritize Risk**	Enables identification, analysis and prioritization of security issues, ensuring optimal use of organization's critical security resources.
3	**Flexible Remediation Workflow**	Empowers the security team to quickly remediate any issues detected by scans. Alerts are created with contextualized remediation steps if manual intervention is needed.
4	**Integrate Seamlessly**	Built for seamless integration with all major CSPs and many SIEMs, providing a comprehensive view of risk.
5	**Minimize Time to Detect & Respond**	Get a risk-assessed and prioritized view of cloud security and compliance posture with a minimal investment of time in remediation.

Cloud Infrastructure Entitlement Management (CIEM)		
1	**Identity Discovery**	Analytical driven discovery and entitlement management of multi-cloud and SaaS identities.
2	**Identity Governance**	Analyze excessive permissions, govern access, and assess compliance across multiple frameworks. Assess segregation of duty (SoD), user lifecycle management, and RBAC.
3	**Prioritization**	Flexible prioritization following NIST ERM framework.
4	**Remediation**	Reduce IAM risk with guided remediation while supporting automated, semi-automated, and manual remediation workflows.
5	**Reporting**	Enhance organizational cybersecurity posture and streamline compliance efforts through comprehensive insights and proactive risk management enabled by robust reporting capabilities.

Cloud Workload Protection Platform (CWPP)		
1	**Runtime Visibility**	Live monitoring and analysis of system activities, enabling swift detection and response to security misconfigurations within cloud environments.
2	**Workflow Configurations**	Empower customized orchestration of security measures to seamlessly integrate & automate across varied cloud environments to mitigate risks and protect workloads effectively.
3	**Host Visibility**	Assess host security posture & ops, facilitating monitoring, threat detection, & responsive actions throughout cloud infrastructure.
4	**Workload Vulnerabilities**	Identify & assess security weaknesses within cloud-based workloads, bolstering system resilience and defending against cyber threats.
5	**Integrity Monitoring**	Ensure stability & security of digital assets by consistently validating & identifying any unauthorized alterations or tampering occurring within cloud-based environments.

Continuous Compliance		
1	**Continuously monitor compliance risks and maintain industry standards**	Compliance policies, security frameworks and benchmarks against industry standards and best practices. Rules are derived from CSP best practices and Popular frameworks. - ISO 27001:2022, PCI DSS 3.2.1, PCI DSS 4.0, NIST 800-53r5, NIST 800171r2, HIPAA, and more.

CheckRed LLC
5220 Spring Valley Dr. Ste 604
Dallas, TX 75254

checkred.com

sales@checkred.com

Active Directory Posture Management (ADPM)		
1	**Monitoring & Detection**	Monitoring of AD environment for policy violations. Identify critical events, such as changes to domain controllers or AD configurations.
2	**Identity Management**	Management of identities – users, groups, service accounts, domains, non-human identities, & domain password policies.
3	**Password & Authorization Policies**	Enforcing strong password policies and user properties to enhance security.
4	**Configuration Management**	Ensure that AD configurations align with best practices and organizational policies, including proper management of user accounts, group policies, permissions, and access controls.
5	**Security Assessments & Audits**	Continuous security assessments and audits to identify misconfigurations and compliance issues such as old passwords, excessive group memberships, limited group memberships, stale users, frequent password changes, cross-domain interactions, password not required, and weak password policies.
6	**Compliance & Governance**	Ensure compliance with regulations & standards such as NIST, HIPAA, ISO 27001, & more. Assisting organizations in maintaining information security policies to improve AD security posture.

Kubernetes Security Posture Management (KSPM)		
1	**Visibility & Inventory**	Provide unified monitoring and assessment of Kubernetes resources and security configurations across multiple cloud environments (EKS, AKS, GKE, & LKE).
2	**Secure Configuration Policies**	200+ secure Kubernetes configuration policies including - audit configuration, Pod security, encryption and network security. Provide support for custom security policies.
3	**Compliance Management**	Continuously monitor Kubernetes resources for compliance with various regulatory standards, frameworks (ISO, CIS, NIST). Provide a singular dashboard view for all compliances.
4	**Remediation Workflows**	Remediate identified alerts by various options including Console and CLI.
5	**Dashboards**	Consolidated view of Kubernetes environment, including Kubernetes posture, inventory, and account dashboards with detailed insights into risks and trending metrics.
6	**Reporting**	Alerts, mis-misconfiguration, compliance reports and custom reports available in CSV, PDF, and DOCX.

DNS Posture Management (DNSPM)		
1	**Unified Visibility and Discovery of all Major DNS Providers**	DNS providers include Akamai Edge DNS, Linode DNS Manager, AWS Route 53, GCP Cloud DNS, Azure DNS, Cloudflare DNS.
2	**Auto Discovery & Event Detection**	Gain a unified view of all DNS change events in zones / domains / records.
3	**Search/ Asset Context Enrichment**	Easily search across DNS providers with in-depth asset context to understand what is attached to where.
4	**DNS Misconfiguration Detection**	Monitor and detect DNS misconfigurations in record types: A, TXT, MX, SRV, PTR, SOA, DNSKEY, CAA, RRSIG.
5	**Runtime Threat Detection**	Stay on top of runtime threats including NXDomain spikes, Dangling CNAME, sub domain takeover, improper TTL setting.
6	**Data Threat Detection**	Continuous security checks detect internal network exposure, private IP, sensitive information exposure, and DNSSEC validation failures
7	**Drift Detection**	Gain visibility to who changed what and where.
8	**Name Collision**	Stay ahead of Active Directory name collisions.
9	**DNS Amplification Threats**	Prevent DDoS attacks aimed at DNS servers.
10	**Remediation Workflows**	Provides guided remediation instructions with manual, automated and semi-automated workflows and alert prioritization.

CheckRed LLC
5220 Spring Valley Dr. Ste 604
Dallas, TX 75254

checkred.com

sales@checkred.com

Unique Product Capabilities

MSSP Support & Overview

CheckRed's product yields the best fit environment for MSSPs. CheckRed is the only **multi-tenant** platform that allows service providers to manage and monitor various customers' environments in a single window. Generated alerts can be viewed by the admin/analyst for any of the customer accounts.

CSPM + SSPM

CheckRed supports both CSPM and SSPM to perform assessments of cloud and SaaS infrastructure to identify misconfigurations, entitlements, and visibility to ensure adherence to security standards and best practices.

CIEM

CheckRed is the only product in the market providing CIEM capabilities for SaaS and cloud solutions.

Deployment

CheckRed follows a simple registration process and is deployed effortlessly to perform agentless deep scanning of resources.

Risk Analytics

With CheckRed's scanner & rule engine equipped with unique assessment patterns, it provides risk scores of configured cloud environments. A risk score is vital to rectify the cloud environment to utilize remediation workflows provided with alerts.

Prioritization

CheckRed enables identification, analysis, and prioritization of security issues to ensure optimal use of your organization's critical security resources.

Multi-Cloud Visibility

CheckRed provides a comprehensive view across cloud platforms providing empowered and context-aware visibility in a dynamic environment.

Remediation Workflow

CheckRed empowers your security team to quickly remediate any issues our scans surface. Alerts are created with contextualized remediation steps if manual intervention is needed.

Customizable Dashboard

CheckRed supports customization of representations for all the alerts, Cloud/SaaS inventory details. Compliances are displayed over the dashboard.

Scanner Coverage

Simplified multi-cloud posture and entitlement management with 1000+ scanner rules.

Collaboration Tools

CheckRed can push alerts & notifications and allocate tickets to connected tools like Slack and Jira.

AI Search

Integrated natural language processing (NLP) for ease of search and visibility.

Pricing Model

CheckRed provides the ONLY fully integrated solution on a single platform at a fraction of our competitors end user pricing for their single purpose platforms (e.g.: SSPM only). **We deliver a significant financial advantage to end users and our partners**.

We also offer two completely unique pricing advantages.

1. **Users**: the only pricing variable we have are the numbers of users within the company. This should provide our end users with simplicity and understanding of their budget moving forward.
2. **User Bands**: we offer very large usage bands. We do not force an end of year true up unless something dramatic has happened to your user base. Our goal is to allow you to be able to budget from year to year without having to modify your annual subscription due to moderate changes in user count.

Implementation Assurance Program

Introduction

This is a service provided by CheckRed either to direct customers or to our Partners for their direct customers. The fee is not to be discounted. Generally, our Partners offer this service themselves. If a Partner is not able to provide an implementation service, CheckRed will provide the service for our Partner.

Implementation Assurance Program

The Implementation Assurance Program is designed to ensure that the CheckRed platform is implemented correctly and efficiently. The program includes the following steps:

1. **Discovery**: The first step in the Implementation Assurance Program is to discover the customer's environment and identify any potential issues or risks.
2. **Design**: Once the discovery phase is complete, the next step is to design a customized solution that meets the customer's specific needs.
3. **Implementation**: After the design phase is complete, the next step is to implement the solution in the customer's environment.
4. **Testing**: Once the solution has been implemented, it is thoroughly tested to ensure that it meets all of the customer's requirements.
5. **Training**: After testing is complete, CheckRed provides training to the customer's staff to ensure that they are fully trained on how to use the platform.
6. **Support**: Finally, CheckRed provides ongoing support to ensure that the customer's environment remains secure and up-to-date.

Conclusion

The Implementation Assurance Program is an essential part of CheckRed's cloud and SaaS security posture management solutions. It ensures that customers receive a customized solution that meets their specific needs and that it is implemented correctly and efficiently.

Remediation Assistance Program

Introduction

The Remediation Assistance Program is a service provided by CheckRed either to direct customers or to our Partners for their direct customers. The fee is not to be discounted. Generally, our Partners offer this service themselves. If a Partner is not able to provide a remediation service, CheckRed will provide the service for our Partner.

Remediation Assistance Program

The Remediation Assistance Program is designed to help customers who do not have the resources or the knowledge about how to remediate risks when the CheckRed platform for cloud or SaaS alerts them of a risk. The program includes the following steps:

1. **Risk Assessment:** The first step in the Remediation Assistance Program is to assess the risk and determine the best course of action.
2. **Remediation Plan**: Once the risk has been assessed, a customized remediation plan is created that outlines the steps needed to remediate the risk.
3. **Implementation**: After the remediation plan has been created, the next step is to implement the plan in the customer's environment.
4. **Testing:** Once the remediation plan has been implemented, it is thoroughly tested to ensure that it has been successful in remediating the risk.
5. **Training**: After testing is complete, CheckRed provides training to the customer's staff to ensure that they are fully trained on how to remediate risks in the future.
6. **Support:** Finally, CheckRed provides ongoing support to ensure that customers are able to remediate risks quickly and efficiently.

Conclusion

The Remediation Assistance Program is an essential part of CheckRed's cloud security posture management solutions. It ensures that customers who do not have the resources or knowledge about how to remediate risks are able to do so quickly and efficiently.

CheckRed LLC
5220 Spring Valley Dr. Ste 604
Dallas, TX 75254

checkred.com

sales@checkred.com

Custom Integration Service

Introduction

Custom Integration Service is provided by CheckRed either to direct customers or to our partners for their direct customers. The fee is not to be discounted.

Custom Integration Service

CheckRed provides a custom integration for customers with SOAR or XDR or SIEM solutions that aid in the automated remediation of alerts that are identified by the CheckRed cloud and SaaS security platform.

- The integration is designed to work with any SOAR, XDR, or SIEM solution, and it provides a seamless way to automate the remediation of alerts.
- The integration is easy to set up and configure, and it can be customized to meet the specific needs of each customer.
- With this integration, customers can quickly and easily remediate alerts, reducing the time it takes to respond to security incidents.

CheckRed's custom integration into a customer's existing XDR, SIEM, or SOAR platform aids in the remediation workflow by automatically delivering alert details and recommended remediation details to the platform so that the customer's existing technology can automatically initiate, schedule or validate the remediation. Once the remediation is complete, CheckRed is notified and can initiate another scan to validate that the remediation was successful.

This integration is designed to work with any SOAR, XDR, or SIEM solution, and it provides a seamless way to automate the remediation of alerts. The integration is easy to set up and configure, and it can be customized to meet the specific needs of each customer. With this integration, customers can quickly and easily remediate alerts, reducing the time it takes to respond to security incidents.

This is a one-time fee paid per platform to CheckRed.

One-time Assessment Program

Introduction

The One-time Assessment Program is a service provided by CheckRed either to direct customers or to our Partners for their direct customers. Generally, our Partners offer this service as a manual exercise, the CheckRed Platform can be used to automate the assessment and run a final validation scan with supporting reports.

One-time Assessment Program

CheckRed's security posture management technology can provide one-time security posture assessments by leveraging built-in scanners and tools to evaluate an organization's security posture. These assessments aim to build a baseline view of an organization's security posture and identify areas for improvement.

Here are some ways CheckRed's security posture management technology can facilitate one-time security posture assessments:

Baseline Assessment

CheckRed conducts an initial assessment to establish a starting point for evaluating an organization's security posture. This assessment involves analyzing existing security controls, policies, and procedures.

Risk Identification

CheckRed identifies potential risks and vulnerabilities within an organization's infrastructure, applications, and data. It assesses the effectiveness of existing security measures and highlights areas that require attention.

Compliance Evaluation

CheckRed evaluates an organization's compliance with relevant industry standards, regulations, and best practices. It helps identify gaps in compliance and provides recommendations for remediation.

Remediation Recommendations

Based on the assessment findings, CheckRed provides recommendations for improving an organization's security posture. These recommendations may include implementing additional security controls, enhancing existing processes, or addressing specific vulnerabilities.

Reporting

A typical security posture management report may include the following components:

Assessment Findings

A detailed analysis of the organization's security capabilities, including strengths, weaknesses, and areas for improvement. This section may cover various domains such as network security, access controls, incident response, and more.

Risk Prioritization

An evaluation of identified risks based on their severity and potential impact on the organization. This section helps prioritize remediation efforts by focusing on critical vulnerabilities or weaknesses.

Recommendations

Actionable recommendations to enhance the organization's security posture. These recommendations may include technical controls, process improvements, training initiatives, or policy changes.

By leveraging these capabilities, CheckRed's security posture management technology can help organizations gain insights into their current security posture, identify areas for improvement, and develop strategies to enhance overall security resilience.

Details:

Each assessment engagement

1. Priced per user band
2. One-time fee
3. 30 days access to platform (maximum 3 scans)
4. 90 days access to the platform for data and reporting

CHECKRED SECURITY

Milestones

#	Particular	CheckRed inputs	KBL inputs	Status
Week 1	**Onboarding with CheckRed platform**			
Week 2	**Analysis & validation of inventories and findings by Partner team**			
Week 3	**Analysis & validation of inventories and findings by Partner team**			
Week 4	**Acceptance and suggested improvement for utilizing CheckRed in Partner environment**			

***Please Note**: Weekly cadence shall be scheduled as per both the parties availability to discuss and report any issues, concerns & feedback.*

#	SPOC Name	Level	Contact Details	Email
1	**Chaturbhuj Singh & Vishal Kapoor**	L1	+917769871456 +919900092159	chaturbhuj.singh@checkred.com vishal.kapoor@checkred.com
2	**Sushil Vanve**	L2	+919860425576	sushil@checkred.com
3	**Pavan Gorakavi**	L3	+1 5105652422	pavan@checkred.com

Deliverables

CheckRed offers CSPM, SSPM, KSPM, CIEM, ADPM,DNSPM, and COMPLIANCE deliverables as:

Inventory (EXAMPLE)

Number of assets collected for Active Directory classified according to their respective types.

- Groups
- Users
- Computers
- Services Accounts
  With following attributes
  - Name
  - E-mail
  - Account
  - Security Identifier (SID)
  - Finding
  - Domain
  - Status
  - Type
  - Last Login
  - Created On

Findings (EXAMPLE)

- Old Password
- Excess Group Membership
- Limited Group Membership
- Stale Users
- Frequent Password Change
- Cross Domain
- Circular Groups
- Password Not Required
- Weak Password Policies

Commercials

- The shared POC does not include any commercials
- Commercials for continuous CheckRed monitoring will be shared separately

Terms & Conditions

- Privacy Policies: Link
- End User License Agreement: Link

This SOW has been entered into on the Effective Date.

Signed by
for and on behalf of
CHECKRED
Date:

.....
Director

Signed by
for and on behalf of
[PARTNER NAME]
Date:

.....
Director