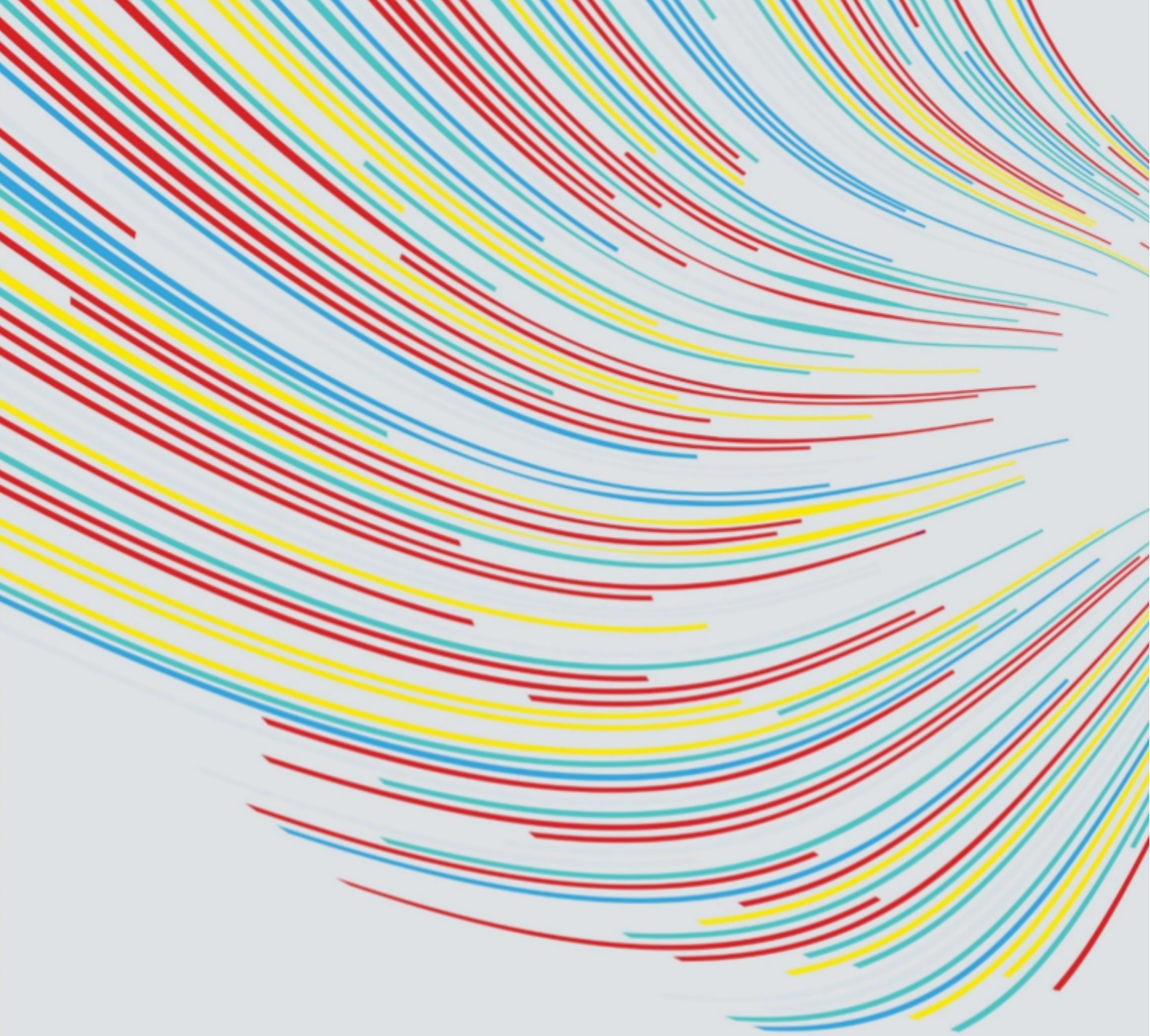


SMS-based Second-Factor Authentication (2FA) Shields

Product Description

RedShield

Commercial in confidence

SMS-based Second-Factor Authentication (2FA) Shields

Product Description

Introduction

RedShield is a service that fixes exploitable elements within the software of your web applications and APIs, then adds further protections against Distributed Denial of Service (DDoS), bots, and malicious users.

The key element within RedShield's technology stack that enables us to fix your software is an edge compute platform.

RedShield developers create custom software objects called "Shields" that execute on this platform to modify application behaviour. With this approach, RedShield is able to achieve very similar results to a full stack development team without having to touch source code.

This document outlines the product description for an Application Specific Shield that RedShield has developed to address a specific requirement – preventing malicious users from logging in to compromised accounts.

Note: Application Specific Shielding utilizes a RedShield managed service component and either RedShield Cloud or RedShield Private Node platforms.

Product SKU

RS-NZ-LIC-SET/MON-ASP-4-P	Application Specific Level 4 Shield Custom transformation (application specific) of request and/or response with state, or bespoke Javascript response rewrite This SKU includes: Scoping + Creation + Customization + Tuning
RS-NZ-LIC-SET/MON-ASP-5-P	Application Specific Level 5: Bespoke security control creation This SKU includes: Scoping + Creation + Customization + Tuning

SMS-based 2FA Shield

Implementation Details

The SMS-based 2FA shields are designed to prevent attackers from logging in to compromised accounts.

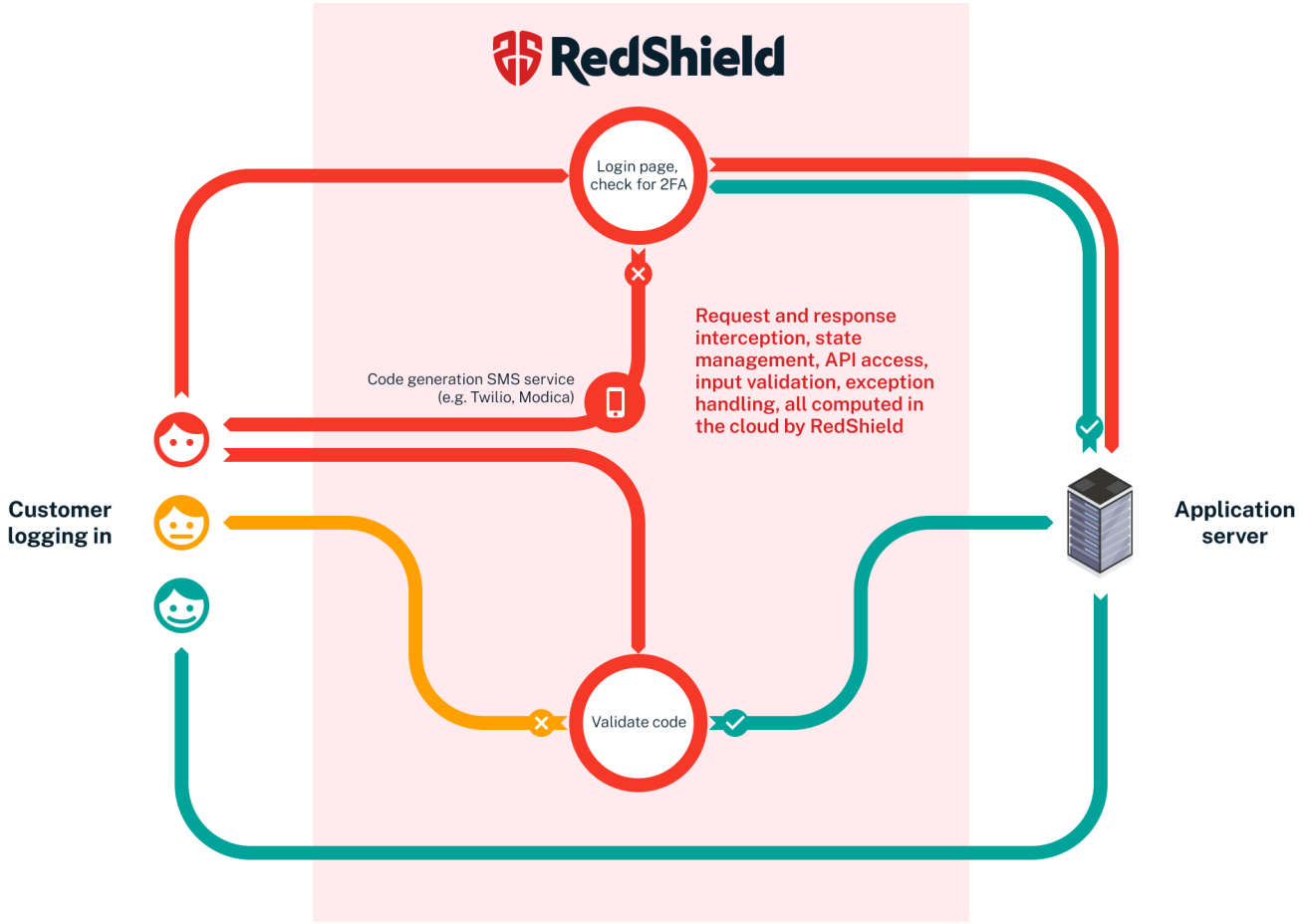
Accounts may be compromised due to password re-use, credential stuffing attacks or compromised email accounts. There are shields to address these issues, including login-lockout and password complexity shields.

If accounts are already compromised, the SMS-based 2FA shields will prevent attackers from logging in with legitimate credentials. The shields work by requiring users to provide a code supplied via SMS message to their cell phone number. Without changing your application code, this solution has been designed to:

- Handle all exceptions and serve the correct error pages or messages to the user;
- Connect to an API (e.g. Twilio) to send the code via email or text message;
- Perform the verification of the SMS code;
- Confirm the responses are valid;
- Manage the number of second-factor attempts and display an error or message appropriately; and
- Submit the login request to the application server once all checks and balances have been met.

If the user does not have a mobile number registered to the account, and the email provider is believed to be uncompromised, shields will fall back to sending an email as the second-factor challenge.

This solution has been designed with your customers' experience in mind; the shield will hook into the existing application code so the second-factor challenge can be presented without needing to reload the page and lose any details the customer has already entered.



Application Specific Shielding — Product Details

SMS-based Second-Factor Authentication (2FA) Shields

Description	SMS-based 2FA shields are created, configured and tuned for each application See detailed shield description above
Applications	VAuth client <Application> Two shields are required (one for each application), as these are customized and tuned separately
Level	5
Customer Dependencies*	API to retrieve customer details Twilio SMS sending account details SendGrid email sending account details (or other APIs if preferred)
SKU	RS-XX-LIC-SET/MON-ASP-5-P

*RedShield will need to intercept and modify the application's user interface (UI) in order to insert multi-factor authentication (MFA) entry fields into the existing authentication flow. This may require assistance from the application developers if RedShield is unable to reverse engineer the application's UI logic (e.g. if the javascript is minified, or there is no clear insertion point).

Application Specific Shielding — Service Level Agreements

Priority	Definition	Response Target
Priority 1 (Urgent)	Site outage. Major security incident such as a DDOS or concentrated attack	<1 hour, 24 x 7
Priority 2 (High)	Site at risk of outage. Partial service degradation.	<4 hours, 24 x 7
Priority 3 (Normal)	Minor service degradation or risk of same	<8 hours, within Business Hours
Priority 4 (Low)	Request for information. Assistance with offline tasks such as testing and configuration	<3 Business Days
Deployment		
Application Specific Shielding:		
Level 5 Shield (Per Hostname / Application)		

Customers can raise support queries via email (support@redshield.co) or via the phone numbers below.
Note: For P1 and P2 SLAs to apply issues must be raised via the RedShield support phone numbers.

Location	Phone Number
United States of America:	+1 424 396 1117
United Kingdom:	+44 118 324 2423
Australia:	+61 2 8880 0766
New Zealand:	+64 4 887 1117

The RedSecure Customer Incident Response Process is outlined in "RedShield's Incident Response Standard Operating Procedure".