Addendum to MSS Transition Service Description

Cloud Web Application Firewall (WAF)

Scope, Features and Responsibilities

Trustwave's Cloud WAF helps protect your web application(s) from attack. Trustwave's transition and delivery teams are assigned to help Clients facilitate the successful configuration and rollout of Client's managed service.

- Trustwave's MSS Transition for Cloud WAF will follow the standard MSS Transition Service Description unless otherwise specified.
- Trustwave and Client responsibilities are covered under the Service Responsibilities section in the MSS Transition Service Description.
- The Transitioning service is deemed to be delivered and operational when all of the following has occurred:

1. Client's instance is created in the Platform;
2. Client has access to the Portal to view event data and reports;
3. the SOC has management control of the WAF;
4. the WAF is configured with initial baseline and tuning completed;
5. Security events are triggered to Security Operations team (if Managed Security Threat Monitoring is subscribed).

Service Features

- Preparation
- Implementation
- User Acceptance Testing and Go-Live
- Baselining & Tuning
- Transition to Service Operations

Preparation

Trustwave will work with Client to complete the discovery document and help ensure optimal configuration based on Client's response on the Discovery Document.

Trustwave will provide Client with access to systems and relevant information and help clarify relevant features included in the service.

Implementation

Trustwave will assist Certificate Authority in Certificate Verification Process and configure SSL certificate on the Platform.

Trustwave will setup Client's Platform and implement the configuration on the security policies based on the inputs provided during the preparation phase. Security policies will be deployed in detection mode for baselining.

User Acceptance Testing and Go-Live

Client will conduct User Acceptance Testing of the security policies and provide approval to proceed with Go-Live in detection mode. Client will perform the required configurations on DNS server to re-direct web application traffic to flow through the Cloud WAF.

Baselining & Tuning

Trustwave will monitor the web traffic in detection mode for baselining and generate an analysis reports based on findings and propose recommendations for tuning. Client will provide approvals for proceeding with tuning of security policy to minimize false-positives rate.

Trustwave Engineers configure and tune the security policies as recommended and deploy the policy in blocking mode. Client will conduct regression testing to ensure a fully functional WAF and ensure that legitimate traffic is not being blocked. Client will develop and complete a test to review the implemented configurations and provide approval for WAF policy to be deployed to production environment.

Transition to Service Operations

Upon completion of the optimization of security policy, Trustwave will configure security alerts to the Security Operations teams involved. Cloud WAF will be transitioned to the SOC team for management. Commence necessary procedures and support for newly on-boarded Client.

Trustwave Responsibilities and Acknowledgements

- Establish and maintain contact with Client.
- Navigate Client through the provisioning process.
- Review and assess Client information through the use of the Discovery Document as necessary to complete the provisioning process.
- Assess, configure and baseline the Managed Cloud WAF service based on information and instructions provided by Client.
- Provide applicable user guides, introduce and review Client's usage and understanding of applicable system access and implement the applicable support process and procedures.
- Help Client to deploy its WAF polices and that they are functioning as intended.

Client Responsibilities and Acknowledgements

- Respond to requests from the Trustwave provisioning team when establishing contact and collecting the Discovery Document.
- Accurately complete the Discovery Document.
- Make available an onsite resource capable of technical detailed requirements review and response throughout the transition phase of the Managed WAF service.
- Make available an onsite resource capable of assisting Trustwave in implementing and deploying the Managed Cloud WAF and quality assurance testing.
- Provide and maintain appropriate credential access to Client's Cloud WAF that is compatible with available Trustwave connection standards.
- Read all provided user guides and documentation and confirm Client's understanding of the processes in the documentation.
- Implement all changes relevant and required to implement the Managed Cloud WAF to accommodate successful implementation of the service.
- Client acknowledges that Trustwave is not responsible for delays in provisioning the service as a result of inaccurate Client Information, Client kick off meeting attendance or lack thereof, user acceptance testing delays and limitations of any third-party technology provider.
- Client is responsible for issues occurring within Client's environment; including initial and ongoing changes to Client's DNS.

Definitions:

Portal means the Trustwave service management web portal.

Platform means the Web Application Firewall management console utilized in providing the service.