Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Larry Hogan | Governor
Boyd K. Rutherford | Lt. Governor
Michael G. Leahy | Secretary
Lance Schine | Deputy Secretary

SERVICE AGREEMENT

Between
The Maryland Department of Information Technology and
Subscribing Entity
For
Managed Firewall Services (FY2021)

This Service Agreement forms a part of the Memorandum of Understanding between the Maryland Department of Information Technology ("DoIT") and subscribing entity ("Customer"). The parties agree as follows:

1 Services Covered

The Department of Information Technology (DoIT) Managed Firewall Service establishes the customer's perimeter access behind a professionally managed Palo Alto Next-Generation Firewall. Customer rulesets, operations, and traffic are segregated using the virtual system functionality of the hardware platform. Monitoring of service availability, including triage and investigation of security issues, happens in the State's Security Operations Center (SOC), where 24 x 7 x 365 monitoring and staffing ensures the highest level of network protection.

2 Parties Responsibilities

The following contains a non-exhaustive list that describes the responsibilities for both DoIT and the subscribing entity and may be updated periodically. Updates will be considered effective 14 calendar days from the posting date of the new service agreement.

2.1 Service Initiation and Onboarding

The parties agree to the following delineation of activities during the onboarding and implementation of the managed firewall service:

2.1.1 DoIT will:

1. Provide an initial Managed Firewall Service consultation to evaluate the product's suitability and estimate price and schedule.
2. Develop a high-level migration strategy and plan.
3. Migrate firewall configurations in an agreed-upon and appropriate for the environment manner, such as:
    a. 1:1 migration;
    b. New instance; and
    c. Migration with updated rules.
4. Assist in the planning for network design and transition to support integration.
5. Complete migration activities in a mutually agreeable, scheduled window.

2.1.2 The Subscribing Entity will:

1. Provide an executive sponsor who can make organizational decisions regarding strategy, approach, and implementation plans.
2. Support migration by providing technically competent resources.
3. Develop and maintain test plans for systems supported by the managed firewall service, following:
    a. Migration activities;
    b. Code upgrades; and
    c. Baselining Efforts.
4. Agree to system rules of behavior before accessing system components.

2.2 Operations

2.2.1 DoIT will:

1. Maintain documented baseline standards for the firewall and customer virtual systems.
2. Utilize the DoIT change management policies for updates to the baselines, deployment of the baseline, and any other changes to the customer's virtual system.
3. Utilize a formal change management process for all system changes, including the managed platform and management systems.
4. Ensure compliance with State IT policies and standards.
5. Perform system software upgrades when:
    a. required to address system vulnerability or flaws;
    b. to maintain alignment with the vendor recommended code revisions;
    c. to support new features, performance enhancements; and
    d. other circumstances that arise, necessitating the upgrade of the system software.
6. Manage automatic security content updates, including:
    a. monitoring issues caused by updates; and
    b. investigating and resolving problems with automatic updates.
7. Notify customers of service impacting changes in accordance with SLAs and maintenance schedules.
8. Support external audits by providing:
    a. Managed service processes, plans, and procedures, and;
    a. Firewall configurations.
9. Update dynamic block lists to prevent traffic transactions with known malicious hosts, networks, and URLs.
10. Notify the customer's technical contacts of credible security events detected through SOC monitoring, including detection of:
    a. malicious traffic based on signatures;
    b. malicious files based on signatures and 0-day threat detection;
    c. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks;
    d. Notable unusual activity detected by the IDP/IDS systems; and
    e. unusual activity detected by auxiliary sensors.

2.2.2 The customer will:

1. Use the operational processes and documents provided on the DoIT website for changes and reporting service and security issues.
2. Maintain system components under its management (e.g., User-ID server agent).
3. Notify DoIT of changes to its infrastructure that transact with the firewall, including
    a. Active Directory Servers; and
    b. SSL Certificates.
4. Review their ruleset, at least annually, to ensure that rules still have a business purpose and that configurations are aligned with organizational objectives.
5. Determine the business suitability and risk of requested policies and rule sets.
6. Notify DoIT of security issues and administrative changes, including changes in:
    a. Customer authorized system users;
    b. Customer change approvers; and
    c. Service delivery contacts.
7. Assume responsibility for:
    a. Rule changes and the impact of such changes (DOIT will provide a basic review of requested rule changes, but the ultimate responsibility is the customer).
    b. Audit findings related to the configuration of the customer's virtual system (DOIT will assist customers in responding to audit findings regarding the process).
8. Respond promptly to notifications of detected security issues, conduct a prompt and thorough investigation, and report findings to the SOC.
9. Provide an organizational reporting structure to escalate detected incidents and events.
10. Notify DoIT through an intake request as soon as practicable, but no less than 45 days before resources are needed for an audit.

3 Service Level Agreements

3.1 Availability

DoIT defines service availability for the managed firewall service as the system components being up and passing traffic with less than 10ms of delay.

3.1.1 Availability Target: 99.9%, measured monthly

The availability target excludes planned maintenance windows.

3.2 Incident Handling

3.2.1 Priority 1: Response time 30 minutes, resolve time 2 hours

Priority 1 incidents include any issue that results in a total cessation of service or the partial cessation of service impacting a customer application categorized as business-critical.

3.2.2 Priority 2: Response time 2 hours, resolve time 2 days

Priority 2 incidents include any issue that results in a partial cessation or disruption of service, administrative access issues, and other important business issues.

3.2.3 Priority 3: Response time 2 business days, resolve time 5 business days

Priority 3 incidents include service questions, reporting, and other administrative issues.

3.3 Changes

Change SLAs are measured from the time that a valid and complete request is received in the ticketing system until the confirmation from the requestor that the change was successful. Change SLAs exclude any time required to get formal approval, requestor time spent validating, and rework due to incomplete and inaccurate customer requests.

DoIT uses ITIL processes, including peer reviews, to ensure change consistency and alignment with configuration standards. All changes are logged in the ITSM, including the authorization for change, configuration changed, approvals, requestor, implementer, and outcome.

3.3.1 Substantial Changes: 7-30 Days

Changes that require significant engineering and coordination activities, such as establishing new security zones, substantial migrations, or implementation of new services and features.

3.3.2 Regular Changes: 4 Hours

Non-urgent changes that are defined in the standard change catalog, and occur as part of normal operational activities, such as website whitelisting/blacklisting, adding new ports to existing services, or adding new servers.

3.3.3 Urgent Changes: 2 Hours

Urgent changes that are defined in the standard change catalog and occur as part of normal operational activities where a service interruption has occurred, such as website whitelisting/blacklisting, adding new ports to existing services, or adding new servers.

4 Maintenance Schedules

Maintenance of the managed firewall will typically occur on Tuesday and Thursday nights starting at 11:00 PM EST and ending at 05:00 AM EST the following day. Except in instances where an emergency maintenance is required, DoIT will provide 48-hour notice and will make every effort to leverage the redundancy of the service to limit any service interruption.

5 Support and Service Outages

Service requests and security issues should be reported to the security operations center.

6 Costs for Services

Costs for the service are based on managed firewall size. Sizing is typically aligned with the number of users behind the customer's instance. Details on the pricing are agreed to in the initial service consultation.

- Small: $5,000 (1-49 PINs)
- Medium: $20,000 (50-499 PINs)

- Large: $50,000 (500-4999 PINs)

Security Operations Center Monitoring

- $100 per PIN

7 Termination of Services

The subscribing entity must provide 60 days advance written notice to terminate services. Termination of services will be effective at the end of the fiscal year following the conclusion of the 60 day notice period.

8 Warranty

While DoIT strives to provide a secure service, no service can guarantee that all network and system intrusions, compromises, or other unauthorized activity will be detected and prevented. Examples of items with limited detection capabilities include, but are not limited to:

1. Detection of malicious activity that occurs in encrypted tunnels and sessions (e.g., SSH, HTTPS, LDAP-S, Gmail);
2. Detection of unauthorized access using valid accounts;
3. Blocking of unseen and bespoke 0-day payloads; and
4. Attacks using expected and unusual mechanisms (e.g., detection of SQL injection on websites that use SQL coding in URLs).