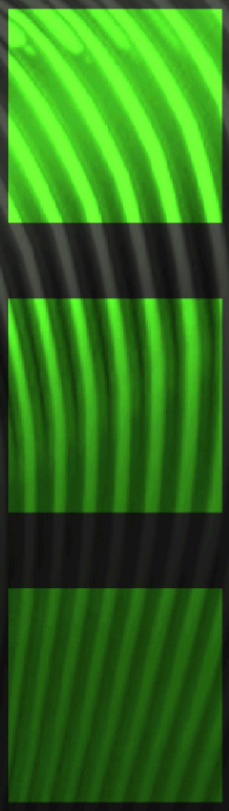
CAYLENT

Idea to Impact. Faster.



Vulnerability Management Plan

Purpose

Caylent takes information security and system protection seriously. Caylent policy requires that:

1. All Caylent production systems must be scanned for vulnerabilities at least daily.
2. All vulnerability findings must be reported, tagged, and tracked to resolution in accordance with the SLAs defined herein. Records of findings must be retained for at least 365 days.

Roles and Responsibilities

1. **General Counsel**: Final approval on new policy creation and/or policy modifications, ownership of overall security posture and programs at Caylent.
2. **Director of Security**:
    a. Monitors of all vulnerability management tools, SLAs, processes, and procedures.
    b. Works with or delegates security tasks to individual team members to achieve desired goals, outcomes, and SLAs.
    c. Oversees policy and process adjustments as necessary.
    d. Tracks SLA progress for events/incidents and maintains documentation for completion or deviations from standard SLA timelines.
3. **Information Technology**: Executes patching of machines according to guidance from the Director of Security. Reviews MDM platforms to ensure endpoints are up to date with most current SLAs as patches are rolled out.
4. **Internal Development Team**: Responsible for patching custom software and cloud infrastructure configurations.

Prioritization of Vulnerability Findings

Caylent reviews and prioritizes vulnerability findings based on multiple facets and data points related to an individual finding. Severity is based on a 1-4 scale or ("S-SEC") with 1 being the lowest priority and 4 being a critical issue. Severity is based on a combination of vendor supplied rankings (CVSS, KEV, EPSS, etc.) and internal data points (system criticality, logging & alerting maturing, presence of a workable exploit, public facing nature of the resource, etc.)

The following guidelines apply for implementing the Caylent rating for Severity (S-SEC). Vulnerability findings are assigned severities, either manually or system-generated, adjusted, and treated according to the associated severity SLA for remediation. Findings are prioritized according to SLAs defined below.

1. *Critical (4):* Vulnerabilities posing a severe risk with large impact have intended remediation SLA of 7 days.Defined as: Anything with a 8.5+ CVSS score and verified real-world plausibility / likelihood of abuse at Caylent and/or:
    a. Any vulnerability that is classified as a 0 Day to critical Caylent systems;

   b. High risk asset(s) based on Caylent's system classification rankings; (I.e.: is resource public?)

   c. Vulnerability is present on KEV;

   d. Affected resource logging and alerting maturity.

2. *High (3):* Vulnerabilities posing a high risk or large impact or categorized as high severity are added to the Security Team task board for immediate adoption into the current sprint and remediated in production within 30 days of findings.

   a. Note: 0 Day laptop patches are always categorized as High with 30 day patch SLA. These are given a P2 or P3 priority depending on the affected system based on Caylent's critical system ranking.

3. *Medium (2):* Vulnerabilities posing a medium risk of measurable impact or categorized as medium are added to the Security Team backlog and–if deemed necessary–remediated in production within 90 days of findings. These are given a P3 or P4 priority depending on the affected system based on Caylent's critical system ranking.

4. *Low (1):* Vulnerabilities posing a low risk of reduced or no immediate impact or categorized as low when received shall be added to the Security Team backlog and prioritized for future work with a 180 day SLA.

   a. Note: If after review the vulnerability is considered not an actual risk or is adequately mitigated, it will be documented and the finding suppressed in the respective system(s).

Caylent maintains a 14-day cool-off period for general patching. That is, patches are approved for release and applied 14-days after the actual patch release in order to lower the likelihood of buggy patches causing production issues. In the event a vulnerability is labeled Critical, the 14-day cool-off will not apply.

Protection Against Malware - End User Devices

1. All Caylent devices will have Anti-virus / Endpoint detection and response (AV / EDR) installed or appropriate mitigation in place where traditional AV installation is not possible.

2. Anti-virus will log to a location that is centrally accessible and retained for at least 30 days Monitors and alerting on anomalous events will be responded to with the SLA for the event severity.

3. All noteworthy findings are tracked in Caylent's ticket systems for historical use and review.

4. End users cannot remove endpoint security features or controls.

5. Contractors, using non-Caylent devices, who may be handling Caylent Restricted or Confidential Information must provide proof of some form of AV / EDR installed within two weeks of starting a contract with Caylent.

6. Any vendor disclosed vulnerabilities (i.e., Apple / Microsoft, Google, etc. announce a patch for a 0-day) will also be addressed as High severity (3+).

7. A partially manual process is required to install some patches and will be addressed by IT team members in accordance with Caylent's documented processes.

AWS / Cloud Infrastructure

1. Managed services are managed / handled by AWS per the Shared Responsibility Model.
    a. In addition to the monitoring that AWS performs as part of the Shared Responsibility Model, Caylent performs additional monitoring and reporting, as specified in this policy.
2. Self hosted products and custom tooling are monitored via a combination of vulnerability scanners, SAST, secrets detection, anomaly detection, and robust monitoring and alerting pursuant to this policy.

Hosted Off the Shelf Software

Caylent hosted off the shelf software (i.e., not SaaS) must have mitigating factors applied in lieu of AV where applicable (i.e., If no AV, firewalls, vulnerability scanners, robust monitoring, etc. must be in use.)

Vendors

Caylent's Third Party Vendor Management Policy outlines specific requirements for Vendors, depending on the Vendor's risk score.

Revision History

Original publication: December 2025