

Safe Deployment Practices for Endpoint Security at Scale

Cynet's Safe Deployment Practices (SDP) align with Microsoft Virus Initiative expectations for endpoint security solutions, including those operating with kernel-level components on Windows. Every update is deployed in a controlled, observable, and reversible manner — minimizing customer risk while maintaining rapid delivery of security protections.

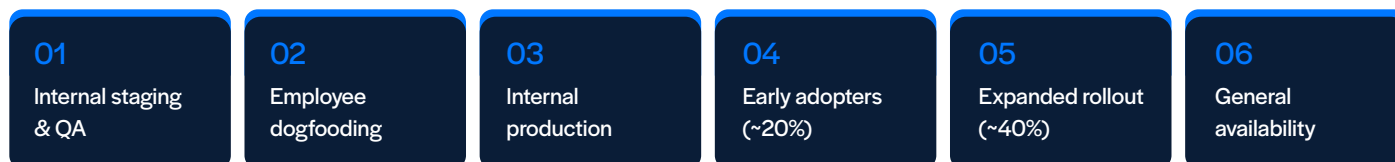
OVERVIEW

- | | |
|----------------------------------|----------------------------------|
| 01 Staged Rollout | 05 Rollback & Containment |
| 02 Kernel-Level Safety | 06 Incident Response |
| 03 Pre-Release Validation | 07 Customer Transparency |
| 04 Telemetry & Monitoring | 08 Governance |

01 Controlled and Staged Deployment

All Cynet updates agent software, Windows drivers, and cloud-delivered configuration or detection content—are deployed through a multi-stage rollout process designed to limit blast radius and detect issues early.

DEPLOYMENT STAGES



Each stage includes:

- Defined success criteria (stability, performance, error thresholds)
- Mandatory monitoring periods before advancement
- Explicit human approval gates

No update is deployed globally without successfully progressing through all prior stages.

02 Windows Driver and Kernel-Level Safety

For Windows agent updates, particularly those involving kernel-mode components:

- Releases are tested across supported Windows versions and representative enterprise configurations
- Customer environments are monitored for anomalies or operational issues during rollout
- Driver releases follow Microsoft signing and release requirements where applicable

Additional safeguards include:

- Health telemetry monitoring during rollout
- Deployment halt and rollback capabilities when significant issues are detected
- Monitoring for crashes, performance degradation, and operational instability

03 Comprehensive Pre-Release Validation

Before deployment, updates undergo validation processes intended to identify operational or security issues prior to release.

Validation activities include:

- Automated and manual testing performed by QA and engineering teams
- Internal bug-hunt and validation activities prior to release advancement
- Compatibility and operational validation in staging and internal production-like environments
- Malware detection and prevention validation against real-world threats

Testing scope and duration are adjusted according to the nature of the release.

04 Deployment Telemetry and Monitoring

Cynet maintains continuous monitoring throughout deployment stages.

Monitoring include:

- Endpoint telemetry related to deployment success/failure
- Operational health and stability monitoring
- Visibility into crash reports, exceptions, and connectivity issues
- Automated alerting when predefined thresholds are exceeded

Alerts are routed to on-call personnel responsible for assessing the situation and initiating response actions where necessary. Customer-reported issues are also incorporated into deployment health evaluation.

05 Rollback and Containment

Cynet maintains rollback and containment mechanisms intended to minimize customer impact from problematic releases.

Capabilities include:

- Emergency stop functionality available during all rollout stages
- Rollback to previously stable versions where applicable
- Automated and manual recovery procedures depending on deployment conditions

Rollback actions may be initiated in response to:

- Elevated error or crash rates
 - Endpoint instability
 - Significant performance degradation
 - Critical operational or security issues identified during rollout
-

06 Incident Response and Operational Readiness

Cynet maintains formal incident response procedures specifically for deployment-related issues:

These procedures include:

- Escalation paths for operational and engineering teams
- Coordination between engineering, operations, support, and customer-facing teams
- Root Cause Analysis (RCA) processes following significant incidents
- Ongoing review of deployment outcomes and lessons learned

Deployment-related incidents may be identified through telemetry, internal monitoring, automated alerting systems, or customer reports.

07 Customer Transparency and Deployment Control

Cynet provides customers with visibility and control over updates through:

- Advance notification of major releases
- Release notes and deployment communications
- Customer portal visibility into rollout status where applicable
- Support channels for issue reporting and escalation
- Early-adopter participation and supported deployment deferral options

Customers are encouraged to remain on supported versions to ensure access to the latest security improvements and operational enhancements.

08 Governance & Continuous Improvement

Deployment processes are reviewed regularly and updated as practices evolve. Continuous improvement activities include:

- Post-release reviews
- Analysis of deployment issues and near-miss events
- Incorporation of customer feedback
- Alignment with evolving industry guidance and best practices

Cynet continues to evolve its deployment practices in alignment with guidance from Microsoft and broader industry security recommendations.

SUMMARY

Cynet's Safe Deployment Practices combine staged deployments, pre-release validation, deployment monitoring, rollback mechanisms, and customer communication processes intended to reduce operational risk and support reliable delivery of endpoint security updates.

These practices are designed to support alignment with Microsoft MVI Safe Deployment Practice expectations while remaining grounded in Cynet's current operational processes.

About Cynet

Cynet's Unified, AI-Powered Cybersecurity Platform unifies a full suite of security capabilities on a single, simple solution, backed by 24x7 expert support. Cynet is purpose-built to enhance protection for small-to-medium enterprises and to maximize margins for MSPs.

Learn more at www.cynet.com