UPRITE SERVICES

Uprite Recommended Security Standard

Published at uprite.com/ss

Revision 1.0 — April 2026

Purpose

This document defines the Uprite Recommended Security Standard — the minimum set of security capabilities required for full incident response coverage under the Uprite Services Catalog. It identifies the required capability categories and the currently approved technologies fulfilling each category.

The approved technologies listed in this document may be updated over time as the threat landscape evolves and Uprite's vendor relationships change. Clients will be notified of material changes. The capability categories themselves are updated less frequently and are governed by the Services Catalog.

Required Capability Categories and Approved Technologies

Capability Category	Description	Currently Approved Technology	Required for Full Coverage
Managed Detection & Response (MDR)	24/7 SOC-based monitoring, alert triage, threat hunting, and guided response	Huntress MDR	**Yes**
Identity Threat Detection & Response (ITDR)	Monitoring and response for identity-based attacks including credential compromise and lateral movement	Huntress ITDR	**Yes**
Endpoint Protection	Next-generation, behavior-based prevention and response for servers and workstations	SentinelOne	**Yes**
Multi-Factor Authentication (MFA)	Enforced MFA on all accounts and systems managed by Uprite, including email, servers, and cloud services	Microsoft Entra ID / Conditional Access (or Uprite-approved equivalent)	**Yes**
Offsite and Immutable Data Backup	Managed backup solution stored offsite and protected against modification or deletion	Uprite-approved immutable backup solution (current approved vendor published separately)	**Yes**

Deployment Requirements

To qualify for full incident response coverage under the Services Catalog, all five capability categories must be:

1. Active on the Client's current Service Order
2. Confirmed as deployed by Uprite on all applicable devices and accounts
3. Actively managed by Uprite at the time of the incident

Coverage is based on actual deployment status, not Service Order enrollment alone. Clients who have agreed to the full standard but have not permitted deployment of one or more capabilities will be treated as Partial Deployment clients for incident response purposes until full deployment is confirmed.

Partial Deployment

A client is considered to be in Partial Deployment status if one or more capability categories are not deployed at the time of an incident, for any reason including:

- The capability is not included on the Service Order
- The Client has declined or deferred deployment of an approved technology
- The technology has not yet been deployed to all applicable devices or accounts

Clients in Partial Deployment status receive limited incident response coverage and are subject to premium billing rates as described in the Services Catalog. See the Cybersecurity Incident Response section of the Services Catalog for full details.

Achieving Full Standard Deployment

Clients wishing to achieve Full Standard Deployment status should contact their Uprite Client Success Manager. Uprite will assess current deployment status, identify any gaps, and provide a remediation plan. Once all capability categories are confirmed as deployed, the Client will be eligible for full incident response coverage at standard rates.

Revision History

Version	Date	Summary of Changes
1.0	April 2026	Initial publication. Establishes five required capability categories: MDR, ITDR, Endpoint Protection, MFA, and Offsite Immutable Backup.

> **Note:** *This document is maintained by Uprite and updated as approved technologies change. Clients are encouraged to confirm their current deployment status with their Client Success Manager at least annually.*