RSU OPERATIONS & SECURITY BRIEF

Server and Business PC Maintenance

Why disciplined maintenance, vulnerability discovery, and verified security remediation are essential business controls.

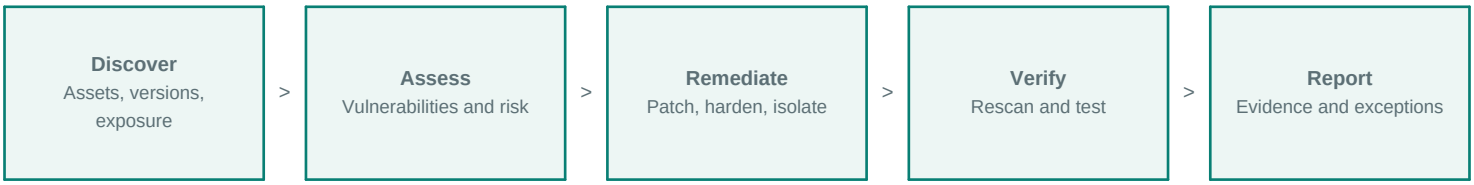
A high-level, public reference for business and technology leaders

Maintenance is a security program

Servers and business PCs continuously change. New vulnerabilities are disclosed, attackers adapt, applications are updated, certificates expire, storage fills, configurations drift, and security agents can stop reporting. A system that worked yesterday is not automatically secure today.

NIST describes enterprise patch management as preventive maintenance: identify, prioritize, acquire, install, and verify patches and upgrades across the organization. Effective maintenance goes further by finding weaknesses, correcting them, and proving that remediation worked.

The closed-loop maintenance model



Why businesses need both server and endpoint maintenance

• Servers concentrate critical applications, identities, files, databases, backups, and administrative privileges.

• Business PCs process email, credentials, browser sessions, documents, remote-access tools, and cloud data every day.

• An unmanaged endpoint can become an entry point; an unmanaged server can turn that entry point into a business-wide incident.

• Maintenance reduces avoidable outages while shrinking the paths an attacker can use to gain access, escalate privilege, or move laterally.

What a security-centered maintenance program covers

Control area	Servers	Business PCs
Asset visibility	Roles, owners, services, ports, dependencies	Owner, location, OS, software, encryption, agent health
Patching	OS, hypervisor, firmware, applications, runtimes	OS, browsers, productivity apps, drivers, firmware
Scanning	Authenticated vulnerability and configuration scans	Endpoint vulnerability, software, and compliance assessment
Hardening	Services, protocols, firewall, admin paths, baselines	Local admin, attack surface, firewall, device controls
Protection	EDR, logging, integrity, privileged monitoring	EDR, anti-malware, web/email controls, disk encryption
Recovery	Application-aware backup and tested restoration	Protected business data and rapid device rebuild

Maintenance must include remediation

• A scan is a measurement, not a fix. Findings need ownership, risk-based priority, a due date, and a documented resolution.

• Patching should prioritize vulnerabilities known to be exploited, internet-facing exposure, privileged systems, and business-critical assets.

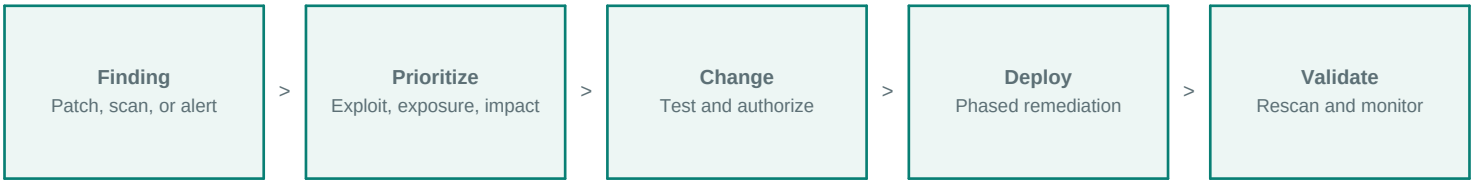
• When a patch cannot be applied promptly, compensating controls may include isolation, access restriction, disabling a vulnerable service, firewall changes, or increased monitoring.

• Every remediation should be verified by installation evidence, configuration checks, rescanning, and functional testing.

A practical operating cadence

Cadence	Representative activities	Evidence
Continuous / daily	Security-agent health, critical alerts, backup failures, capacity and service exceptions	Alerts resolved; exceptions assigned
Weekly	Urgent patches, known exploited vulnerabilities, external exposure review, failed update follow-up	Deployment and rescan results
Monthly	Standard patch cycle, authenticated scans, firmware/app review, local administrator review	Coverage, findings, remediation status
Quarterly	Configuration baseline review, privileged access review, restoration exercise, unsupported software plan	Approved exceptions and test records
Annually	Architecture and lifecycle review, recovery objectives, vendor support status, program effectiveness	Roadmap, budget, and risk acceptance

Risk-based remediation path



Metrics leadership should see

- Asset and security-agent coverage, including unknown or non-reporting systems.
- Patch compliance by severity, age, exposure, and business criticality.
- Known exploited vulnerabilities outstanding and time to remediate.
- Vulnerability recurrence, approved exceptions, unsupported systems, and compensating controls.
- Backup success, restoration-test outcomes, and recovery gaps.

What good maintenance prevents

- Exploitation of known software and firmware weaknesses.
- Credential theft and privilege escalation caused by weak configurations or stale controls.
- Lateral movement from employee endpoints to critical servers.
- Outages caused by capacity exhaustion, failed services, expired certificates, or unsupported software.
- False confidence from security tools that are installed but unhealthy, misconfigured, or no longer reporting.
- Unrecoverable disruption caused by untested or exposed backups.

Public references

NIST SP 800-40 Rev. 4, Guide to Enterprise Patch Management Planning - https://doi.org/10.6028/NIST.SP.800-40r4
CISA Cyber Hygiene Services - https://www.cisa.gov/cyber-hygiene-services
CISA Known Exploited Vulnerabilities Catalog - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
NIST Security Configuration Settings - https://csrc.nist.gov/Projects/risk-management/about-rmf/implement-step/security-configuration-settings

How RSU helps

RSU can establish and operate a maintenance and remediation program for business servers and endpoints, including inventory, patching, vulnerability scanning, configuration review, remediation tracking, monitoring, backup validation, and executive reporting.

Maintenance windows, testing, recovery plans, vendor requirements, and business-critical exceptions should be tailored to each environment. No fixed cadence replaces risk-based prioritization or emergency remediation for active threats.