Veritas Cyber Recovery Framework

Ensure Reliable and Trusted Recovery

Executive Summary

Utilize best practices with Veritas' industry-leading cyber recovery capabilities to ensure swift, dependable, and trustworthy recovery from cyber incidents. The Veritas Cyber Recovery Framework offers guidance on the processes and tools necessary for rapid and reliable recovery following a destructive attack.

Organizations must respond swiftly and effectively to malicious cyber-attacks. The Veritas Cyber Recovery Framework, aligned with the NIST Cybersecurity Framework, is structured into three key sections, to guide cyber recovery when a malicious attack is suspected.

Detection:

The initial step in cyber recovery is to confirm the occurrence of an attack and initiate the recovery process.
- Detect the attack through NetBackup Anomaly scanning or security alerts (e.g., SIEM, Anti-Virus, DLP).
- Verify whether the detection is a false positive or an actual threat.
- Assess which resources have been compromised.
- Isolate the affected resources to prevent further damage.

Incident Response:

Once the attack is confirmed, security and IT teams must work to eliminate the threat from the environment.
- Notify relevant stakeholders across IT, security, operations, and management.
- Develop a cleanroom strategy in collaboration with IT.
- Deploy the appropriate incident response playbook.
- Determine which data set is best suited for recovery.
- Conduct forensic analysis to understand the attack's scope.
- Scan backup data for potential threats.
- Confirm the status of critical infrastructure services.
- Remediate identified threats.
- Verify that the incident is fully contained.

Post Incident Recovery:

After eradicating threats, IT and security teams must ensure that applications and services are safe to resume and restore operations.
- Move cleansed data to the staging or recovery environment.
- Verify the integrity of both data and applications.
- Prioritize the resumption of mission-critical applications.
- Monitor restored operations for any lingering threats.
- Conduct a thorough post-incident review.

- Gradually resume remaining applications to restore normal operations.

Supported by Veritas' market-leading capabilities, the cyber recovery framework enables your organization to significantly enhance the speed and reliability of cyber recovery.
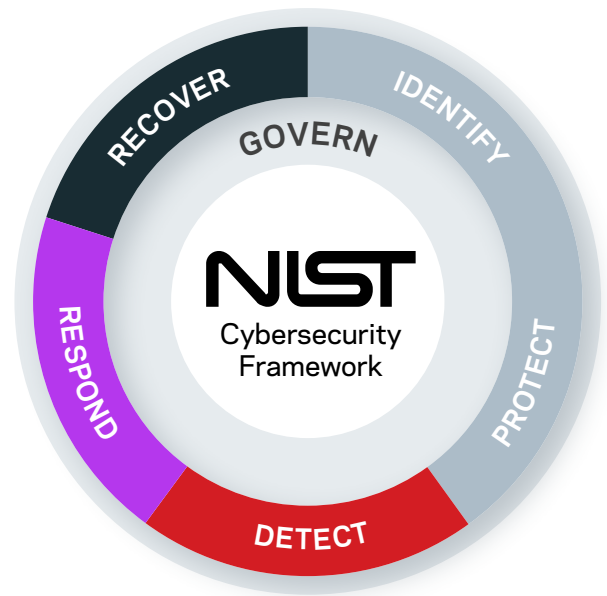
Detection
Did an attack occur?

Incident Response
Is our data, apps and environment clean?

Post Incident Recovery
Are apps and resources ready to resume?

RECOVER • GOVERN • IDENTIFY • RESPOND • PROTECT • DETECT

NIST Cybersecurity Framework

Key Capabilities

- Support for 1,000+ workloads on-premises, cloud and SaaS.
- Veritas cyber recovery services to establish plans and support ransomware recovery.
- Automated detection and remediation of impersonation and hijacking attacks
- In-line, patent-pending anomaly detection
- OCFS support and integrations to SecOps tools
- AI/ML driven data-recovery point analysis and recommendation
- Data recovery from on-premises, remote and cloud
- At-scale IoC scanning, malware and vulnerability scanning.
- Recovery blueprints for orchestrated recovery policies and workflows
- Instant-restore of data, apps and VMs.
- Multi-vendor data-protection monitoring and intelligence.

Learn about your cyber recovery readiness with the Veritas Cyber Recovery checklist.

About Veritas

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers—including 91% of the Fortune 100—rely on Veritas to help ensure the protection, recoverability and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems and 1,400+ storage targets through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on X at @veritastechllc.

VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V2127 09/24