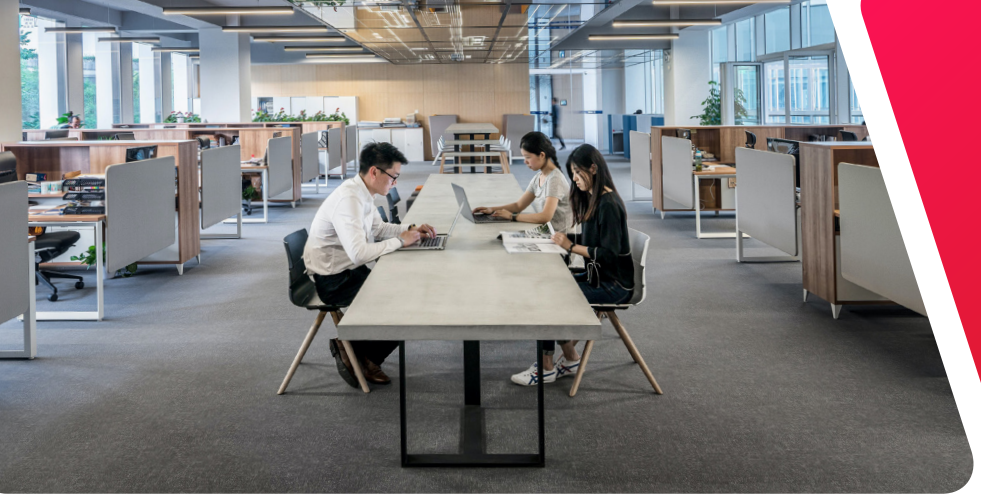
VERITAS

Manage Risk. Build Resilience. Stay Secure.

ENTERPRISE DATA CYBER RESILIENCY GUIDE



Reduce Risks to Your Business

The hardest part of business continuity and cyber resilience is preparing for the unknown. It's not as if anyone is working with you to schedule their attacks.

The safest strategy is to expect the unexpected.

- How do you prepare confidently for ever-evolving threats?
- Do you have a well-thought-out and rehearsed recovery plan?
- How long would you continue to operate your business as usual?
- How long would it take you to identify and recover from an attack?

5.5 Billion

malware attacks in 2022[1]

The Goal of Cybersecurity is to Safeguard Your Data

Becoming the target of a cyberattack is not a question of if, but when. Malware and ransomware —and now ransomware-as-a-service—have become thriving business models.

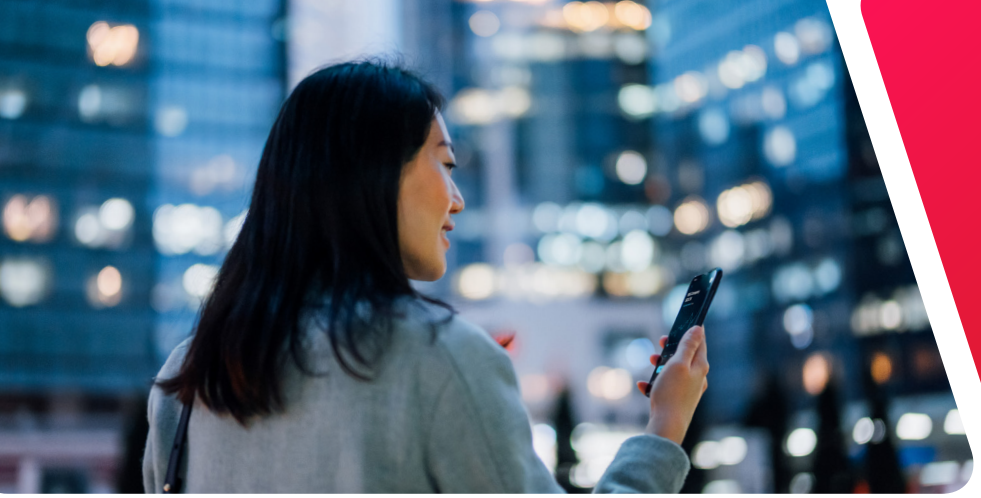
Bracing for a cyberattack can be daunting but the path to protection and recovery doesn't have to be. Explore the essential elements of successful recovery, from establishing a strong foundation and utilizing advanced recovery skills to deploying strategy to minimize the effects of an attack automatically.

6.3 Trillion

intrusion attempts in 2022[1]

$4.35 Million USD

average cost of a data breach in 2022—an all-time high[2]



Prepare for an Evolving Journey

Safeguarding data and maintaining business continuity starts by investing in a dependable platform designed to protect both your on-premises and cloud data.

The key is to protect your infrastructure and establish a secure, indelible, and immutable backup and recovery strategy. Whatever you implement needs to be optimized to support your business operations while protecting your data and providing the ability to recover quickly.

83%

of organizations studied have had more than one data breach[2]

79%

of organizations don't deploy Zero Trust[2]

Create a Flexible Environment

Building an ongoing data-protection strategy isn't cheap. It's far less expensive than the costs that come with unprotected data that you can't easily recover or recover at all. Lost data, damage to your brand reputation, legal fees and repercussions for exposed data, and non-compliance fines from the government are only the start.

Solid strategy and recovery plans need to be a part of the cost of doing business. Besides, it makes budget planning easier.

Break data protection and recovery into buildable blocks to ensure that you are investing in dependable data protection for both on-site and cloud. Ensure that you are maximizing recovery performance and that your investment is flexible enough to shift and scale as regulations and compliance needs change.

19%

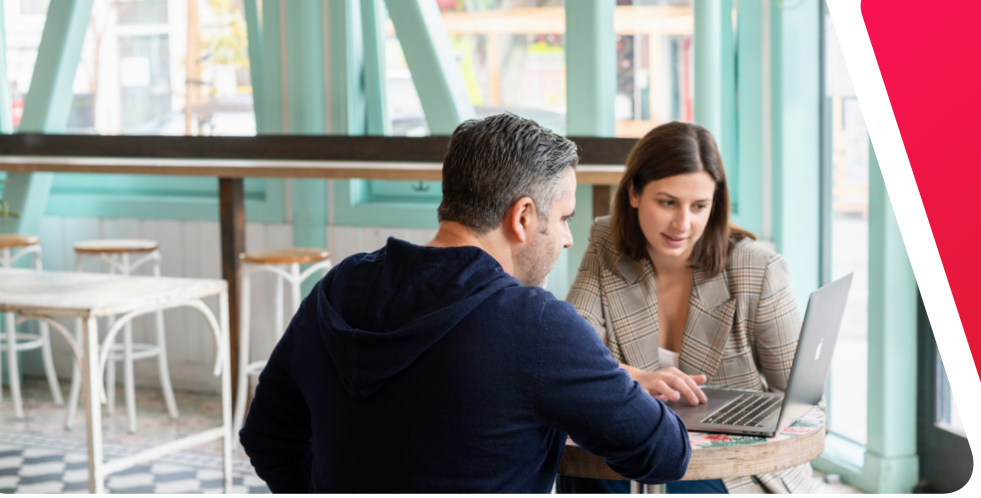
Frequency of breaches caused by stolen or compromised credentials[2]

60%

of encrypted data is restored after paying ransom[3]

4%

of organizations retrieved all of their data after paying ransom[3]



Focus on Process

There's little disagreement about the need for holistic and robust data protection.

Simplifying and centralizing data management to streamline efforts is the first step to preparing your organization against a data breach. Consequences ensue when companies neglect a standardized data management process. The ripple effect of a process breakdown can have huge financial repercussions.

To add to the challenge, your data exists in multiple locations, applications, and formats, which makes it hard to aggregate and analyze data. This disconnection generates inefficiencies, which drive extra costs, hinder visibility of your landscape, and increase security risks.

Have you standardized your process?

- ☐ Strategy and business alignment
- ☐ Risk management framework
- ☐ Resource management
- ☐ Metrics and reporting
- ☐ Vulnerability management
- ☐ Data access, audits, collection, and retention processes

It's challenging to continually optimize your use of data while simultaneously navigating a complex, expensive backup and recovery architecture.

Keeping the business running often relies on replication, snapshots, and deduplication to expand the capabilities of your environment—most likely at extra cost and with limited results. The result can compromise control over data and its protection.

Components to Document

- ☐ Cyber resiliency plan
- ☐ Roles and responsibilities
- ☐ Data access, audits, collection, and retention policies

Start with Users and Data

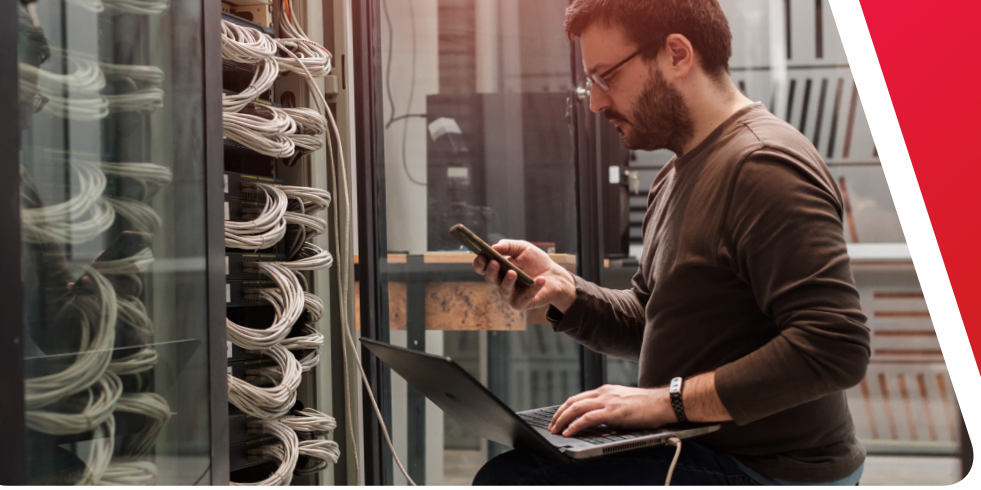
A simple and critical step in reducing vulnerabilities is to enact robust password policies to guarantee users are accessing data securely. Prime examples of successful attacks resulting from ineffective access-control and authentication procedures appear in the news on a regular basis.

You can bolster both on-site and cloud-based security significantly by implementing strong credentialing, multifactor authentication, and approaches including role-based access control. Use a Zero-Trust framework to enforce identity, segmentation, and privileges as a first step toward decreasing the fallout of a potential attack.

Recording and monitoring user access privileges within your environment is particularly important for mailboxes and shared folders for software-as-a-service platforms like Salesforce, Microsoft 365, SharePoint, and others. Continual review and auditing access is also necessary to ensure authorization is justified for specific roles.

Use Access Controls

- Credentialing
- Account creation/deletions
- Authentication
- MFA w/SAML 2.0 IDP
- SmartCards
- One time passcodes
- Authorization: role-based access control
- Repository (LDAP/active directory)
- Federation
- Self service password resets
- Integration of cloud-based identities
- DNS
- NTP (network time protocol)



Prevent a Data Breach

Securing data is at the heart of any security architecture, especially in the cloud. Ensure that your data security strategy addresses confidentiality, integrity, and data availability. Set consistent processes for the usage, storage, sharing, archiving, and destroying of information.

Multilayered data security addresses the reality that your data resides and travels through multiple applications and connections, which creates a wide surface area vulnerable to attack. Multiple migrations further increase the attack surface. Meanwhile, malware and intrusions can breach a vulnerable gap and sit quietly undetected, roaming your network for weeks or even months before they're detected.

Security Architecture

- ☐ Immutability
- ☐ Long term retention
- ☐ Privileged access management (PAM)
- ☐ Local identities
- ☐ Network identities
- ☐ Least privilege
- ☐ Role based access
- ☐ Just-in-time provisioning
- ☐ Password vaults
- ☐ Password rotation
- ☐ Auditing/monitoring
- ☐ Alerting
- ☐ Provision
- ☐ Portable token
- ☐ Static ACLs
- ☐ Licensing

Define Backup Strategy

A comprehensive data protection strategy includes backing up all types of data, securing storage, and recovering data in the event of any type of disaster. Your strategy should address how you manage data, including:

- Data availability, which centers on ensuring systems are running.
- Data durability, which refers to how you safeguard data against corruption and degradation over its lifetime.
- Data retention, which deals with policies and compliance surrounding where and how long data is stored.

It's important to define goals related to recovery of data, including RPO and RTO:

- Recovery-point objectives (RPO) dictate the point in time of the backup to which you want to fall back. Can you recover with data from one week ago or do you need it to be less than one hour?
- Recovery-time objectives (RTO) refer to how long it takes to get up and running again. Tape is incredibly secure, but it might take a week for you to get to restore. Can you wait that long?

An essential element for backup is ensuring that data is continuously replicated to another system and tested regularly. Testing is critical to identify and mitigate any issues with configuration, software, or equipment that would prevent successful recovery.

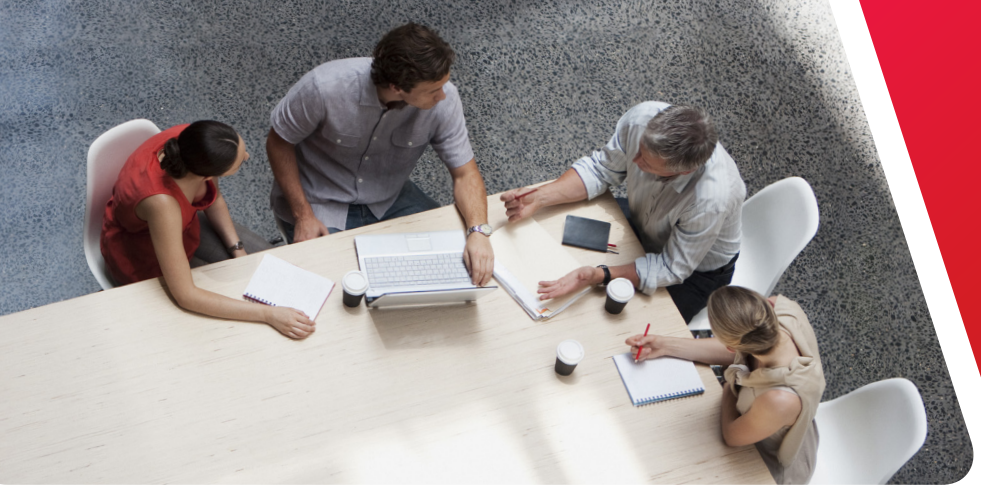
Defend Against a Breach

It's critical to protect data and systems from both external and internal threats. Reliable encryption, access management, anomaly and malware scanning, and immutability are paramount to your prevention efforts.

- **Gain insight** into your data assets to construct an understanding of resources, trustworthiness, potential risks, and inherited susceptibilities.
- **Increase oversight** not only to facilitate better audit and inspection processes, but efficiently identify potential risks within your enterprise.
- **Incorporate anomaly** and malware scanning to identify fraudulent transmissions.
- **Set up policies** to collect and retain system logs from multiple sources for evaluation.

Infrastructure Components

- ☐ Isolated Recovery Environment (IRE)
- ☐ Air Gap
- ☐ Recovery Vault
- ☐ WORM Immutability
- ☐ Anomaly Detection
- ☐ Malware Detection
- ☐ 3-2-1 Backup
- ☐ STIG Hardened Appliances
- ☐ FIPS 140-2
- ☐ Built-in / External KMS Encryption
- ☐ Built-in / External Certificate Authority
- ☐ TLS v1.2 or better



Evaluate and Adapt

It's important to prioritize, define, and adopt a strategy of operational resilience with risk tolerances. But it's not a one-and-done proposition: the business environment is always in a state of evolution, as is the threat landscape.

- **Prioritize**: Consider which individual processes, systems, and workloads are essential.
- **Define:** An effective strategy addresses core business systems and processes. It mitigates risk by ensuring that backups are not hosted in any one location. And it considers how the organization and stakeholders are affected by interruption, both in service and monetary consequence.
- **Adopt:** Leaders of successful data-protection programs take the lead in understanding, communication, and implementing compliance, governance, and risk assessment in effort to decrease the surface attack area and increase visibility into the data infrastructure.

Do You Have These in Place?

- ☐ Network Segmentation
- ☐ Application Protection
- ☐ Defense in Depth
- ☐ Remote Access
- ☐ AES 256-bit Encryption Technology
- ☐ SIEM/SOAR
- ☐ Cyber Resiliency Plan
- ☐ Disaster Recovery Plan
- ☐ Data Recovery Rehearsal
- ☐ Orchestration

Why Veritas?

Malicious attacks are an omnipresent threat with the potential to wreak havoc on your operations. Examples of their devastating effects make the news. Many vendors promise solutions, while CEOs and board members demand comprehensive strategies—usually within budget constraints.

Veritas can help you establish foundational safeguards so that you safeguard your data and recover faster than ever before. With this advice, you'll be able to craft a reliable data protection plan and prevent future disruptions as much as possible.

Resilience and protection are our highest priorities. We help secure systems and preserve data integrity with a broad array of Zero-Trust security measures, workload support, and immutable storage alternatives—whatever your requirements may be. Our tools grant you full transparency into all parts of your environment, whether cloud, on-premises, virtual, or managed by third-party backup vendors and services too. Nothing gets overlooked.

We use AI-assisted detection capabilities to monitor for strange behaviors associated with both user and data activity. And our automated and on-demand malware scanning will notify you about high-risk areas, helping to guarantee that nothing slips through the cracks and your data stays clean.

At Veritas, we design solutions with maximum resiliency and robust security in mind so you can trust that your business remains operational without prolonged disruption. Our wide range of Zero Trust controls keep IT systems safe and data secure, while providing the indelible storage solutions required. We'll provide you full visibility of your entire environment—from physical to virtual to cloud workloads—and even beyond, making sure no stone is left unturned. Plus, AI-driven detection of anomalies in user behavior or data activity means you're one step ahead in fending off potential threats. Plus, automated and on-demand malware scanning will provide impartial monitoring of high-risk areas as well as recovering clean data when needed.

Close the Gaps in Your Cybersecurity Strategy. Learn more >

[1] 2023 Sonicwall Cyber Report

[2] 2022 Cost of a Data Breach

[3] assets.sophos.com

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent 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, 1,400+ storage targets, and 60+ clouds 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 veritas.com. Follow us on Twitter 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

V1811 04/23