TITAN
CLOUD STORAGE

WHITE PAPERS

DATA SECURITY

In today's digital age, securing data is more crucial than ever. As reliance on digital information grows, so do cyber threats. This whitepaper will guide you through the current cyber threat landscape and highlight the importance of robust data protection strategies.

Introduction

As the digital world continues to expand, your data becomes more valuable and interconnected then before. From medical records and financial statements to confidential employee information and family photos, all of it resides in some form of virtualized environment.

The more data we produce, and the more integral it becomes to our everyday lives, the more imperative it is to keep it safe. Unfortunately, as the amount and value of data increases, so do threats against it—whether physical, technical, environmental, or malicious.

Organizations worldwide experienced heightened security and challenges within their business during the height of the COVID-19 pandemic. As millions of people began to work from home, the risk of cyber threats and system breaches grew exponentially, and continues to rise.

Cybercrime inflicted approximately $6 trillion in damages globally in 2021, making it a significant threat to organizations. Cybersecurity Ventures forecasts this cost to reach $10.5 trillion by 2025, emphasizing the need for a comprehensive approach to defend, protect, and recover data—a playbook, if you will.

For the purposes of this whitepaper, we will imagine modern data protection, and the many threats against it, as a game of football. The attacking team represents cybercriminals delivering sophisticated waves of attacks on your business. They are highly coordinated and advanced. The defense is your organization's cybersecurity strategy, aiming to protect your data netgoal.

Modern attacks are more dynamic and unpredictable, requiring careful game planning and stout defensive alignment. To get your organization's data security strayegy in top shape, we will evaluate the state of cybercrime, the evolving threat landscape, and the key strategies and functions to stay ahead of the competition.

Today's Cyber Threat Offensive

The offensive threats posed by cyber adversaries to businesses and institutions cannot be underestimated. In 2022, ransomware attacks disrupted supply chains, causing widespread downtime, economic loss, and reputational damage. The Colonial Pipeline Co. attack in May 2021 is a prime example, highlighting the impact of ransomware on critical infrastructure and the resulting nationwide fuel shortages.

Ransomware attacked businesses every 11 seconds in 2021, affecting 75% of organizations. Complaints of Ransomware that were reported to the FBI had increased by 82% between 2019 and 2021, costing victims $20 billion in 2021. This figure is predicted to rise to $265 billion by 2031 as cybercriminals refine their techniques.

Organizations must build cyber resilience to remain digitally agile and protect their businesses from increasing cyberattacks. Despite cybersecurity climbing to the top of boardroom agendas, many organizations still lack incident response plans and processes to test their defenses.

KEY STRATEGY

The NIST Cybersecurity Framework

The Five Key Risk Management Functions

Identify:
Managing assests, governance, and risks.

Protect:
Implementing access control, data security, and protective technology.

Detect:
Monitoring and detecting anomalies and events

Respond:
Planning and mitigating responses to security incidents.

Recover:
Planning and improving recovery processes.

The Titan Cloud Storage Difference

Continuous Risk Scanning: Track vulnerabilities and provide deep risk analysis to prioritize remediation efforts.

Backup as a Service (BaaS): Cloud-based backup ensuring 3-2-1 resiliency with encrypted communication and off-site storage.

Disaster Recovery as a Service (DRaaS): Industry-leading disaster recovery software with tight RTO and RPO, ensuring quick recovery from disasters.

Managed Firewall: Gain greater network visibility and protection against attacks with the Fortinet FortiGate platform.

Managed SIEM: Security information and event management (SIEM) solutions for real-time monitoring and threat detection.

Managed Detection and Response (MDR): Proactively identify and respond to threats with a multi-layered security posture.

Object Storage: Secure, manage, and retain data for the long term with comprehensive security and compliance.

Microsoft 365 Backup: Protect Exchange Online, SharePoint Online, Teams, and OneDrive data with flexible restore options.

Summary

All organizations, regardless of size or sector, require a comprehensive data security approach to achieve IT resilience and mitigate cyber threats. Following the NIST CSF framework and partnering with a trusted provider like Titan Cloud Storage ensures a winning defense strategy.

By 2031, a new cyberattack is expected every two seconds. Organizations must have a plan in place to neutralize risks and safeguard their business.