

DATA SECURITY



DATA SHEET

INTRODUCTION

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

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

Organizations worldwide experienced heightened security & 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 & system breaches grew exponentially, & 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 & recover data - a playbook, if you will.

For the purposes of the 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 & advanced. The defense is your organization's cybersecurity strategy, aiming to protect your data net-goal.

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

TODAY'S CYBER THREAT OFFENSIVE

The offensive threats posed by cyber adversaries to businesses & 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 & 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 & 2021, costing victims \$20 billion in 2021. This figure is predicted to rise to \$265 billion by 2031 as cybercriminals refine their technique.

Organizations must build cyber resiliance to remain digitally agile & protect their businesses from increasing cyber-attacks. Despite cybersecurity climbing to the top of board-room agendas, many organizations still lack incident response plans & processes to test their defenses.

THE NIST CYBERSECURITY FRAMEWORK

The Five Key Risk Management Functions



Identify:

Managing assests, governance, & risks.



Protect:

Implementing access control, data security, & protective technology.



Detect:

Monitoring & detecting anomalies & events.



Respond:

Planning & mitigating responses to security incidents.



Recover:

Planning & improving recovery processes.

THE TITAN CLOUD SOLUTIONS DIFFERENCE

Continuous Risk Scanning:

Track vulnerabilities & provide deep risk analysis to prioritize remediation efforts.

Backup as a Service (BaaS):

Cloud-based backup ensuring 3-2-1 resiliency with encrypted communication & off-site storage.

Disaster Recovery as a Service (DRaaS):

Industry-leading disaster recovery software with tight RTO & RPO, ensuring quick recovery from disasters.

Managed Firewall:

Gain greater network visibility & protection against attacks with the Fortinet FortiGate platform.

Managed SIEM:

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

Managed Detection & Response (MDR):

Proactively identify & respond to threats with a multi-layered security posture.

Object Storage:

Secure, manage & retain data for the long term with comprehensive security & compliance.

Microsoft 365 Backup:

Exchange Online, SharePoint Online, Teams & OneDrive data with flexible restore options.

Summary

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

By 2031, a new cyberattack is expected every 2 seconds. Organizations must have a plan in place to neutralize risks & safeguard their business.