DELL Technologies

# DDoS: Strengthening Cybersecurity and Resilience with Dell Technologies

## Rising Threat of DDoS Attacks

Distributed Denial of Service (DDoS) attacks have emerged as one of the most pervasive and disruptive threats in the digital era. Leveraging vast networks of compromised devices, DDoS attacks flood targeted systems, servers, or networks with an overwhelming volume of traffic. This relentless surge slows down operations or brings them to a grinding halt, often crippling a business in the process.

From startups to multinational corporations, no organization is immune to the rising specter of DDoS attacks. As businesses grow increasingly reliant on digital infrastructure, these attacks have devastating consequences, ranging from financial loss to reputational damage. Dell Technologies acknowledges the criticality of this challenge and delivers scalable, innovative solutions that help businesses bolster their defenses and weather the storm.

## What Are DDoS Attacks?

A DDoS attack seeks to disrupt the normal functioning of a network, service, or server by overwhelming it with a massive volume of traffic from multiple sources. These attacks are executed by exploiting botnets, which are networks of infected devices controlled remotely by attackers.

## How DDoS Attacks Work

1. **Botnet Recruitment:** Cybercriminals infect thousands or millions of devices with malware, forming a botnet that can be mobilized for an attack that makes your business inoperable.
2. **Traffic Flooding:** Attackers direct the botnets to send a flood of requests to the targeted server, causing the system to slow down, crash, or become unavailable to legitimate users.
3. **System Overload:** The system, overwhelmed by illegitimate traffic, becomes incapable of fulfilling legitimate requests, resulting in service outages or severe delays.

## Common Techniques

- **Volume-Based Attacks** leverage sheer traffic volume to exhaust a network's bandwidth.
- **Protocol Attacks** exploit vulnerabilities in protocols such as TCP/IP to consume resources.
- **Application-Layer Attacks** target specific applications, such as a website or database, to disrupt functionality.

These attacks evolve constantly, making them a formidable challenge for businesses attempting to safeguard operations.


© 2025 Dell Inc. or its subsidiaries.

## The Impact on Businesses

### Financial Fallout

A single DDoS attack can cost millions of dollars in lost revenue, downtime, and recovery expenses. Even minutes of service unavailability can significantly impact businesses reliant on real-time transactions, such as e-commerce platforms and financial services.

### Operational Disruption

Interruptions caused by a DDoS attack reduce productivity, delay critical processes, and hinder access to essential services. For industries such as healthcare or manufacturing, operational downtime can result in far-reaching consequences.

### Reputational Damage

When customers or clients experience service disruptions, trust weakens. Prolonged or repeated incidents can result in long-term damage to an organization's reputation, leading to customer attrition and reduced market confidence.

## Real-World Example

One high-profile instance occurred in 2020, when a large financial institution fell victim to a sustained DDoS attack that shut down its online banking services for several hours. The direct revenue losses, combined with a tarnished reputation, resulted in damages exceeding **$50 million.**

## Alarming Statistics

Zayo Group's DDoS Insights Report (Feb 2024) indicates that unprotected organizations averaged **$6,000** per minute, leading to an average cost of about **$408,000** per incident in 2023. Furthermore, the frequency of such attacks is escalating, with over **10 million attacks reported annually**. These stats highlight the urgent need for robust preventive mechanisms.

**20.5 Million**

DDoS attacks were blocked in Q1 2025

Source: 2024: Cloudflare DDoS Threat Report

## Combating DDoS Attacks with Dell Technologies

Dell Technologies provides an advanced suite of solutions to help businesses preempt, detect, and recover from DDoS incidents.

### Fortified Endpoints with Dell Trusted Workspace

Endpoints are crucial entry points for DDoS-related threats. Dell Trusted Workspace offer robust security features built into the hardware, such as Secure BIOS and SafeID, which protect against unauthorized access and maintain system integrity.

### Server Security

Dell's server solutions, equipped with embedded security measures like Dell Trusted Server technology, which includes:

- **Hardware Root of Trust:** This feature ensures that the hardware components of the server are verified at boot time, thereby providing a foundational layer of security against tampering or unauthorized modifications.
- **Built-in Security Features:** Dell servers come with self-encrypting drives and end-to-end boot verification, which protect against unauthorized access and instill confidence in data integrity.
- **Cyber Resilience:** The approach includes capabilities for detecting anomalies, breaches, and unauthorized operations, allowing organizations to recover from cyber incidents swiftly.
- **Comprehensive Data Protection:** Dell's Trusted Server solutions feature integrated security mechanisms that safeguard data at rest and in transit. This includes advanced encryption techniques and automated recovery options to ensure business continuity.

 © 2025 Dell Inc. or its subsidiaries.

These capabilities ensure servers can withstand traffic surges while maintaining operational stability. Storage solutions protect critical data availability and integrity during an attack, minimizing disruptions.

### Storage Security

Dell Storage helps protect against DDoS attacks through various integrated security measures and advanced technologies designed to minimize vulnerabilities, detect threats early, and ensure rapid recovery if an attack occurs. Key methods include:

- **Proactive Threat Detection:** Dell storage solutions employ intelligent monitoring and AI-driven anomaly detection to identify unusual access patterns that might indicate a DDoS attack. These tools provide real-time security insights and can trigger automated threat responses to mitigate the impact of an attack
- **Root of Trust Architecture:** Integrated into storage controllers, this architecture ensures firmware authenticity and prevents unauthorized modifications, thereby enhancing the security of the storage hardware and reducing the chances of compromise during a DDoS attack
- **Multi-Factor Authentication (MFA) and Access Controls:** Implementing MFA and Role-Based Access Control **(RBAC)** helps prevent unauthorized access to storage systems, further protecting against threats associated with DDoS attacks
- **Micro-Segmentation and Network Isolation:** By isolating storage systems and restricting access between workloads, Dell minimizes potential attack vectors and protects storage systems from lateral movement in the event of a breach
- **Secure Snapshots and Immutable Logs:** Dell's storage solutions provide secure snapshots and immutable logs that ensure data integrity and help organizations recover swiftly from DDoS attacks. These features facilitate forensic analysis and incident investigation, allowing IT teams to detect and analyze attack vectors
- **Cyber Recovery Vault:** Solutions like Dell PowerMax and PowerProtect Cyber Recovery Vault create air-gapped backups that are immutable and safeguarded against ransomware and other attacks. These backups can be restored to ensure business continuity without risk of reinfection

By integrating these comprehensive security features and technologies, Dell Storage and Cyber Resilience effectively help organizations defend against DDoS attacks and maintain resilient and secure IT environments.

### Proactive Monitoring with CrowdStrike

Real-time monitoring and advanced analytics are vital to detecting abnormal traffic patterns before escalation. CrowdStrike integrates with Dell's ecosystem to use behavioral analysis and AI-powered insights to differentiate legitimate activity from attack traffic, enabling swift remediation.

### Dell PowerProtect for Data Integrity

Dell PowerProtect ensures critical data remains secure and accessible amid a DDoS attack. Immutable backup capabilities and isolated recovery environments allow businesses to restore systems and minimize downtime after an incident.

### Advanced Network Security and Micro-Segmentation with Dell PowerSwitch Networking & SmartFabric OS

Strengthens defenses against DDoS attacks by delivering advanced network segmentation, strict access controls, and real-time traffic analytics across your infrastructure.

## Real-World Implementation

A global e-commerce platform recently leveraged Dell PowerProtect solutions alongside proactive detection capabilities to fend off a sophisticated DDoS attack. By isolating critical systems and deploying emergency recovery processes, the business resumed full operations in record time, mitigating financial losses and preserving client trust.

## The Multi-Layered Security Approach

Success against DDoS attacks stems from layered and adaptive defenses. Dell advocates for the following strategies to complement its technological offerings:


2025 Dell Inc. or its subsidiaries.

### Key Steps to Enhance Defense

- **Zero Trust Architecture** Implement a “never trust, always verify” model to scrutinize each user and device.
- **Advanced Encryption** Encrypt communication across all layers to protect sensitive data transmitted during potential attack attempts.
- **Employee Training** Educate employees on identifying suspicious activity and following secure protocols to prevent inadvertent breaches.
- **Regular System Testing** Conduct routine assessments, including penetration testing and load testing, to evaluate system preparedness for high traffic volumes.

These actions, combined with Dell Technologies solutions, create a robust defense mechanism against sophisticated threats.

## Partnerships that Strengthen Cybersecurity

To extend its capabilities, Dell Technologies collaborates with industry leaders such as **Microsoft**, **CrowdStrike** and **Secureworks** for example. These partnerships provide additional layers of protection, incorporating the best threat intelligence and advanced detection methodologies into Dell’s comprehensive framework.

## Leveraging Dell Professional Services

Beyond technology, Dell’s Professional Services offer expert guidance to businesses facing DDoS challenges. From incident response to tailored security architecture consultations, Dell’s team ensures organizations can quickly recover and reinforce future defenses.

## Build a Resilient Future

Dell Technologies is more than a technology provider; it’s a partner committed to safeguarding your business against the evolving threat of DDoS attacks. By combining cutting-edge technology, in-depth partnerships, and actionable insights, Dell helps businesses protect operations, maintain client trust, and actively pursue growth.

Take the first step toward a resilience today. Contact Dell Technologies to fortify your business against DDoS threats and secure your future.

Dell Technologies empowers businesses to rise above the challenges of DDoS cybersecurity, proving that a secure foundation is the key to success in an interconnected world.

Learn how to address some of today’s top cybersecurity challenges at **Dell.com/SecuritySolutions**

---

Learn more about Dell solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation with #DellSecurity

© 2025 Dell Inc. or its subsidiaries. All Rights Reserved. Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

DELL Technologies