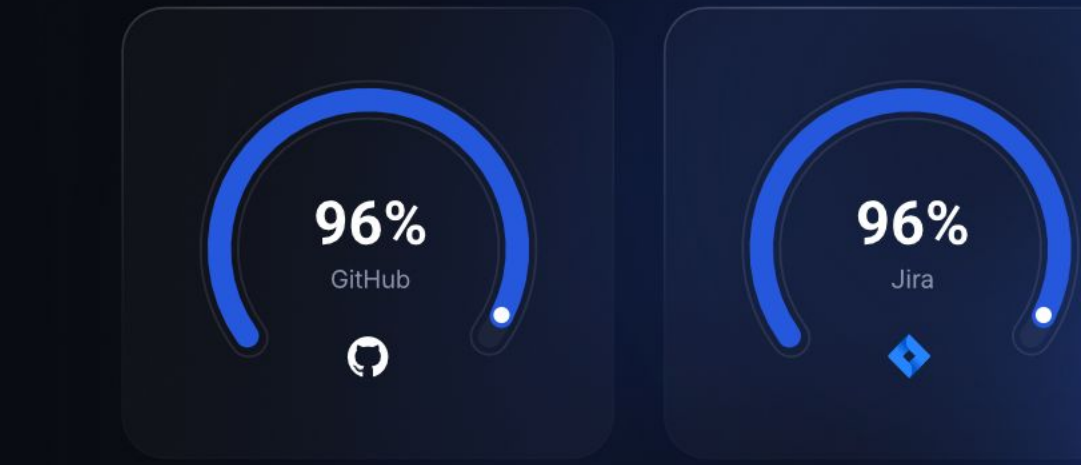
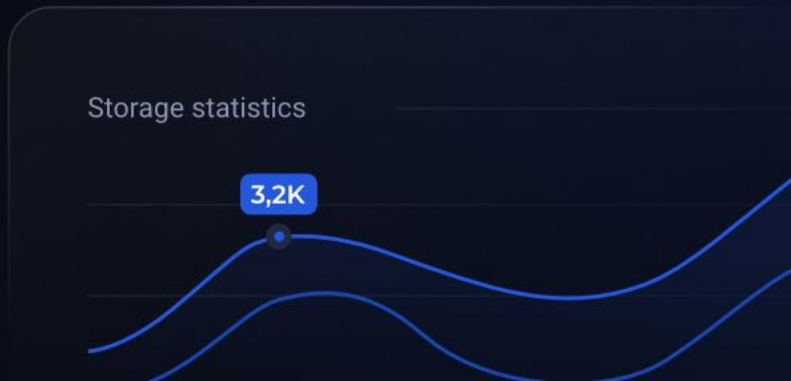
GitProtect.io

State of DevOps Threats 2026

Key Takeaways & Recommendations





The 2025 devops threat landscape

Major development platforms and pipelines are now primary channels for malware delivery and infrastructure control.

Adversaries have pivoted to identity abuse, leveraging stolen tokens to bypass modern defenses at scale.

The cost of fragility

Operational risk is surging: 2025 saw a **40%** rise in platform incidents and **1,750+** hours of high-severity downtime.

Reactive monitoring is obsolete; the **2026** mandate is a total shift toward absolute architectural resilience.

The following pages outline the core mechanics of each threat vector, the hard data behind them, and our strategic recommendations for remediation.

01 AI in DevOps & automation risks

The Productivity Trap

AI tools help developers write code faster and automate repetitive tasks. However, it's important to remember that AI-generated code can accelerate defects rather than reduce them.

The AI Agent Insider Threat

Autonomous AI agents operate with elevated environment privileges. Adversaries exploit the common practice of embedding raw user content into AI prompts without proper sanitization, triggering unauthorized workflows and privileged command execution.

Automation Identity Leakage

Long-lived tokens, often used for automation and continuous deployment, create high-risk non-human identities that can outlast their intended scope, amplifying security fragility and leaving persistent backdoors open.

+65

AI-related incidents analyzed within main DevOps platforms

1.43x

More AI-related incidents in the second half of 2025

65%

Top AI producers leaked secrets on GitHub repos

Source: Wiz

Our Recommendation

- Treat AI tools as untrusted actors by default
- Enforce strict input sanitization and least-privilege access for AI agents
- Require short-lived credentials and human-in-the-loop reviews
- Harden CI/CD workflows and continuously monitor AI-driven actions

02 Software supply chain compromise

Poisoning the Well

During 2025, attackers disguised malware as legitimate security tools and vulnerability scanners, tricking even experienced researchers into executing malicious code within local script execution environments.

The Illusion of Trust

Multiple large-scale campaigns demonstrated how stolen tokens and malicious workflows could cascade into thousands of affected repositories. Typosquatting and malicious lookalike packages remain difficult to detect.

Cascading Blast Radius

A single leaked token, combined with permissive CI/CD configurations, enables months-long, multi-project compromises across the software supply chain, leading to complete pipeline takeover.

400K

Dev secrets exposed during the second wave of the Shai-Hulud 2.0 attack

Source: Wiz

3,300+

Exfiltrated keys leaked across hundreds of public and private repositories

Source: GitGuardian

1,750

Poisoned open-source projects hosted on GitHub

Source: Leiden University

Our Recommendation

- Harden CI/CD and developer workflows by enforcing short-lived, least privilege tokens
- Continuously monitor repositories, workflows, and dependencies for anomalies
- Verify all third-party code, PoCs, and tools before using them
- Treat automation, secrets, and open-source trust as critical security boundaries, not defaults

03 Secrets leakage & identity attacks

Identities as the New Perimeter

Attackers systematically shifted focus from traditional perimeter breaches to the software supply chain and cloud identity layer, targeting SaaS platform credentials, SSH keys, and cloud IAM tokens.

MFA Interception & PhaaS

Phishing-as-a-Service (PhaaS) platforms used adversary-in-the-middle techniques to intercept credentials and session tokens in real time, effectively neutralizing common MFA protections.

Stealth Identity Takeovers

Adversaries increasingly abuse legitimate platforms, OAuth flows, and developer infrastructure to blend into normal activity, allowing malicious third-party SaaS extensions to remain completely hidden.

17K

Exposed secrets in public GitLab cloud repositories

Source: Luke Marshall

73%

Organizations that store cloud credentials in GitHub Actions secrets

Source: Wiz

94+

The number of countries where Microsoft credentials were stolen

Source: Microsoft

Our Recommendation

- Enforce least privilege access to protect data
- Rotate credentials frequently
- Continuously monitor CI/CD workflows, repositories, and cloud accounts for anomalies
- Adopt phishing-resistant MFA, secret management, and automated dependency scanning

04 DevOps platform outages & service risks

Centralized Points of Failure

Centralized SaaS and cloud platforms act as single points of failure at a global scale. Repeated failures highlight how configuration changes and maintenance errors can cascade rapidly into operational freezes.

The Automation Cascade

Automated DNS management system defects, database saturation, and bad config deploys recursively shut down downstream developer pipelines, silently halting deployments and CI/CD.

Multi-SaaS Redundancy

Modern software teams face immense cloud concentration risks. Resilience requires designing systems that maintain offline, cross-platform recovery paths and avoid single-provider dependencies.

607

The total number of incidents in 2025 across major DevOps and project management platforms

1,769h

Hours of downtime across major DevOps and project management platforms in 2025

+69%

Year-over-year increase in critical and major incidents compared to 2024

Our Recommendation

- Build a reliable backup and disaster recovery plan to reduce outage impact
- Avoid single-provider dependencies with multi-region and multi-service redundancy
- Test disaster recovery procedures regularly
- Maintain offline access, backup communication paths, and a clear incident response plan

05 Vulnerabilities, exploits, and patches

The Severity Shift

DevOps platforms frequently expose enterprise risk through authentication and CI/CD flaws. Critical flaws increasingly allow for unauthorized access, privilege escalation, or remote code execution.

Third-Party Dependencies

Vulnerabilities stem from weaknesses in third-party components buried inside deeply nested libraries. High-impact flaws in SSO and SAML enable attackers to authenticate as valid users.

Vulnerability Loop

Large language models have been contaminated, with up to 95% of AI-generated file-server code being vulnerable. This reinforces a cycle of insecure code reuse and manual logic defects.

59%

Patched DevOps vulnerabilities in 2025 rated as high or critical severity.

+76%

The increase in patched vulnerabilities from Q1 to Q4 in 2025

+123%

Increase in high-severity vulnerabilities from H1 to H2

Our Recommendation

- Monitor DevOps platforms for vulnerability updates and security recommendations
- Implement on-time patches to reduce the risk from high-severity vulnerabilities
- Audit third-party dependencies and restrict guest access
- Continuously monitor for anomalies to defend against supply-chain exploits

06 Phishing & identity exploits

The Assumption of Trust

Emails masquerading as document shares or security alerts exploit trust in open-source tools and platform notifications. This bypasses human scrutiny to deliver malicious links and attachments.

Turnkey PhaaS Infrastructure

Automated, commercial Phishing-as-a-Service tools render real-time login captures and intercept hardware 2FA workflows instantaneously.

Token & Cookie Hijacking

Adversaries capture credentials and session cookies to bypass MFA protections. Attackers abuse legitimate infrastructure like ADFS to make malicious links appear fully trustworthy.

1M

Phishing attempts powered by the Whisper 2FA platform by October 2025

Source: Barracuda

5,000

Downloads of malicious releases before removal

Source: The Hacker News

50%

Success rate of attempted Microsoft 365 account compromises

Source: Proofpoint

Our Recommendation

- Restrict OAuth device code flows with Conditional Access
- Enforce app consent approvals and continuously audit authorized applications
- Combine phishing-resistant MFA with behavior-based detection
- Focus user training on device codes and trusted platform abuse

07 APT campaigns & targeted operations

Dev Platforms as C2 Infrastructure

Multiple groups leverage GitHub repositories as command-and-control infrastructure and malware hosting platforms to bypass standard web filtering.

The Open-Source Arsenal

Modern ransomware operators build up to 80% of their toolkits from modified, public open-source tools. They use Bring Your Own Vulnerable Driver (BYOVD) to disable local antivirus defenses.

Infiltrated Workflows

Operatives secure remote positions by fabricating histories and coordinating commits to manage platform credibility, embedding rogue IT workers inside enterprise networks for espionage.

+1,600+

Victims infected by a single targeted APT campaign

Source: Check Point

30min

Interval at which malware, deployed during a spearphishing campaign

Source: Cyber Security News

233

Confirmed victims across the US, Europe, and Asia targeted by a cryptocurrency theft operation

Source: Strike

Our Recommendation

- Monitor and restrict the use of public repositories for internal workflows
- Enforce strict access controls on API tokens
- Validate code from third-party sources
- Deploy behavioral detection to flag unusual repository activity and prevent the impact of malware, ransomware, and APT campaigns

08 DevOps breaches & enterprise risks

Targeting the Blueprint

Attackers prioritize repository and ticket environments yielding cloud access keys and API logic. Lateral movement enables shifts from developer environments into production systems.

The Lateral Pipeline Shift

By infecting endpoint workstations with lightweight infostealers, attackers harvest persistent cookies to move directly from QA and dev systems to live production environments.

Persistent Stale Credentials

Unrotated, long-lived credentials remain valid for years after employees leave. This highlights the long-term risk posed by unrevoked root AWS credentials and exposed GitHub tokens.

21K

Nissan customers whose personal information was exposed in a third-party data breach

Source: Bleeping Computer

$890M

Financial shortfall caused by a cyberattack on Jaguar Land Rover

Source: Security Week

1.1TB

Internal data stolen from Disney's Slack channels

Source: The Register

Our Recommendation

- Enforce strict credential hygiene
- Rotate and revoke old access tokens, and implement least-privilege access across DevOps platforms
- Utilize continuous monitoring and repository audits
- Implement employee security training to prevent unauthorized access, insider threats, and supply chain abuse

09 Malware hosting on dev platforms

Safe-Haven Illusion

Malware distribution networks host malicious binaries directly inside public Git repositories to bypass corporate web content filtering policies and DNS blocks.

Evasion Bloating Architecture

Downloaders artificially inflate executable sizes to 500MB+ using meaningless padding bytes. This makes detection and mitigation difficult while stolen data is sold on the dark web.

Target System Scavenging

Modular payloads with anti-analysis checks target browser credentials and financial access data. Attackers deceive developers with polished README files and inflated commit histories.

1M

Devices hit worldwide in a GitHub-linked malvertising attack

Source: Bleeping Computer

76

GitHub accounts linked to a campaign distributing multi-stage malware via fake open-source projects

Source: Trend Micro

$5K

Price Per Stolen Digital Identity Package

Source: Trend Micro

Our Recommendation

- Enforce strict code vetting and limit access to repositories
- Scan third-party projects for malware before use
- Combine repository monitoring, behavioral analysis, and credential hygiene
- Increase employee awareness to prevent attacks exploiting fake or trojanized dev projects, malvertising, and supply chain abuse

10 Compliance, privacy & governance

Inaccurate Compliance Claims

Falsified security statements lead to immediate federal enforcement. Organizations are penalized for inaccurate certifications and weak internal controls, even without confirmed breaches.

Non-Consensual Data Processing

Enterprise data controls cannot be delegated. Regulators hold enterprises legally responsible when cloud platforms track data or set cookies without explicit transparency or user consent.

Negligent Threat Patching

Failing to patch known vulnerabilities and ignoring audit warnings are primary drivers for maximum regulatory penalties. Organizations must isolate compromised devices quickly.

335

The number of GDPR-related compliance incidents recorded by regulators in 2025

Source: Enforcement Tracker

$11.25M

Settlement paid to resolve allegations of falsely certifying cybersecurity compliance

Source: SC Media

£14M

Penalty for failing data protection requirements

Source: The Guardian

Our Recommendation

- Enforce strict compliance requirements to ensure transparency, consent, and clear data handling with cloud providers
- Maintain regular vulnerability management and rapid incident response procedures
- Implement continuous monitoring to prevent data exposure and protect sensitive information
- Assign clear accountability metrics across all involved parties

What you'll get with GitProtect

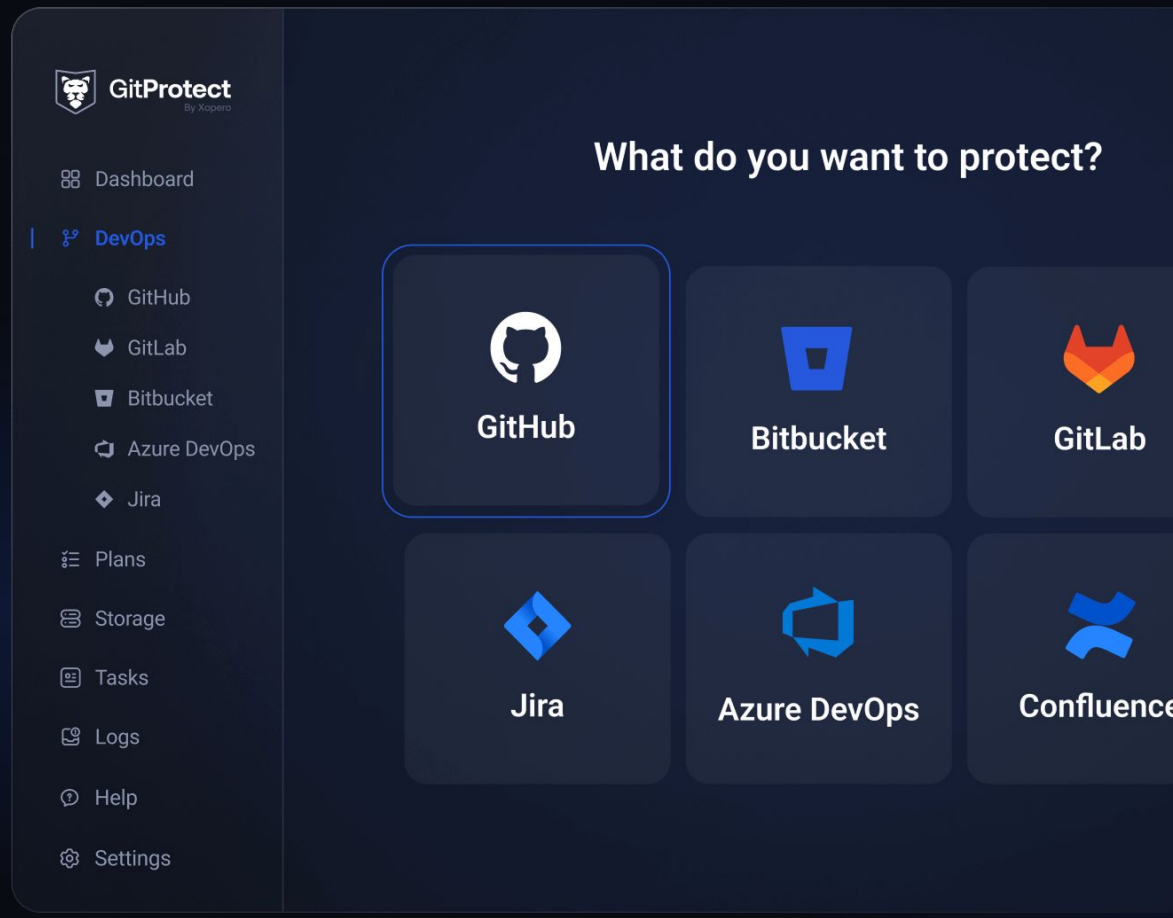
GitProtect is an automated backup and disaster recovery solution built for DevOps environments, including GitHub, GitLab, Bitbucket and Jira.

It protects source code and DevOps metadata from accidental deletion, ransomware, and service outages, so teams can restore quickly and keep delivery moving.

GitProtect helps you reduce backup-and-recovery risk and prepare the documentation needed for certification and ongoing audits.

Ready to see it in action?

Book a demo



GitProtect.io