perforce
Puppet

How to Proactively Remediate Security Vulnerabilities

The Top-Line Risks: Breaches, Elevated Costs, and Noncompliance

- **Manual processes waste time, introduce human error, and increase risk** in critical security operations.
- **Failure to meet regulatory and compliance expectations** leads to fines and reputational damage.
- **Scaling hampers innovation and growth** by increasing attack surfaces, introducing new security challenges, and worsening existing ones.

60% of breaches
are attributed to an unpatched vulnerability
Source: Ponemon Institute/ServiceNow

$4.88 million USD
average cost of a data breach, 2024
Source: IBM

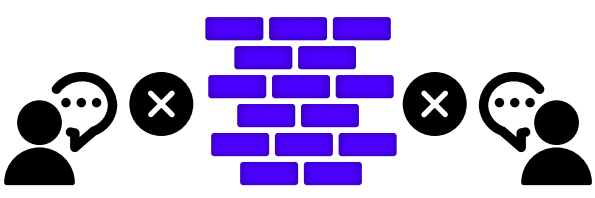
$14.82 million USD
average cost of non-compliance problems
Source: Ponemon Institute/Globalscape

The Source: Disconnected Teams, Procedural Bottlenecks & Inefficient Workflows

Security and operations teams need to work together to proactively address vulnerabilities and maintain secure IT. But a lack of collaboration keeps the ideal workflows — and better DevSecOps — at arm's length.

77% of CISOs struggle to prioritize vulnerabilities
due to lack of information on risks
Source: Dynatrace

Security Team
- Detection
- Assessment
- Prioritization



Platform Team
- Remediation
- Verification
- Documentation

The Future: Unlocking Enterprise DevSecOps

- **Automated processes** speed up detection, remediation, and mitigation.
- **Self-service and enterprise observability** enable informed decision-making.
- **Response time shrinks.**
- **Resilient systems stay prepared.**
- **Teams have more time** to drive business value.

Security is no longer an afterthought.
Secure, compliant configuration policies are enforced throughout the software development lifecycle.

Increased visibility helps teams accurately prioritize risk.
Decision-makers know their exposure, severity, and patch availability.

Automation speeds up response and decreases MTTR.
Scanning, event monitoring, patch testing, and deployment happen with minimal human effort and error.

Improved collaboration lets teams address vulnerabilities together.
Developers, security, and operations teams share critical information and permissions for fast decision-making.

Security Team → **Platform Team**

- **Detection** via automated scanning
- **Assessment** for severity and potential impact
- **Prioritization** based on risk level

- **Remediation** via automated patching and mitigation
- **Verification** via automation
- **Documentation** for auditing and compliance

How Puppet Turns Security Challenges into Business Advantages

Security is integrated from the start to reduce risk and improve compliance.

Development isn't bogged down by infrastructure scaling challenges.

Streamlined collaboration between teams accelerates remediation activities.

Additional use cases increase the utility and value of existing toolsets.

Discover Puppet Enterprise Advanced ▶