Manage security risks and remediate vulnerabilities faster

You have to protect your organization and its reputation like never before — particularly as your infrastructure grows and diversifies, presenting a broader front for attackers. That means Security teams must work closely with IT Ops counterparts to understand the risk of ever-changing infrastructure, rather than in silos.

Vulnerability management can be a long, painful and inefficient process

Today, the vulnerability management process, from vulnerability scan reports run by InfoSec to vulnerability remediation done by IT Ops, is segregated and inefficient. The InfoSec team uses sophisticated scanning tools to identify vulnerabilities, then emails the scanning data to IT Ops.

IT Ops then manually tries to determine what resources are affected, prioritizes resources to fix, then remediates them. How do they quickly determine what is important to fix out of thousands of vulnerabilities?

Number of known vulnerabilities reached almost 15,000 in 2017

IT Ops spends on average 320 hours per week on a single vulnerability remediation

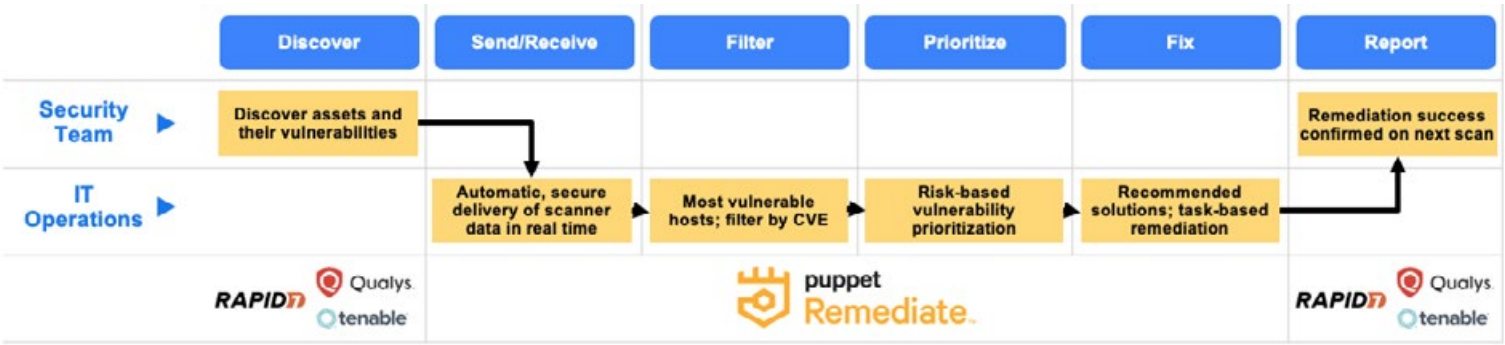
Average total cost of a data breach was $3.86M in 2018

The lack of parity between tools and teams also means there is no control or visibility over who does what and when. This leads to delays and negatively impacts the ability to reduce vulnerabilities present in your systems, leaving your organization exposed to external attacks and the potential for hefty financial losses.

Puppet Remediate helps IT organizations mitigate security risks, enabling them to reduce the number of vulnerabilities faster. It integrates with the leading vulnerability scanners commonly used by InfoSec teams, such as Tenable, Qualys and Rapid7. This integration helps facilitate risk-based prioritization, so IT Ops has context about what to remediate and can take action within the same tool. Simply put, vulnerability scanners **FIND** the vulnerabilities, Puppet **REMEDIATES** them.

Efficiently manage vulnerabilities with Puppet Remediate

With Puppet Remediate, InfoSec runs scans, but instead of manually exporting them into spreadsheets and emailing them, IT Ops receives read-only scanning data automatically with Puppet Remediate. IT Ops has everything they need to quickly filter, prioritize and remediate vulnerabilities in a standardized, trackable, and easily auditable way.



With Puppet Remediate you reduce the risk of external attacks and data breaches by eliminating manual handovers in the vulnerability management process — scan, find to fix. This means vulnerabilities are remediated days/weeks faster than ever before all the while reducing the number of vulnerabilities present in your infrastructure.

If you'd like to learn more about Puppet's capabilities for vulnerability management, contact us.