

The Application Iceberg

The Hidden 80% of Enterprise Risk

Vulnerability lives above the waterline.
Remediation happens below it.

What IT Sees



Windows Updates



OS Compliance



Security Baselines



Patch Tuesday



Endpoint Health



Vulnerability Dashboards

48% of breaches involve vulnerability exploitation

What You Measure Isn't Always What Attackers Target

The Hidden Operational Risk – Third-Party Applications

- Hundreds of third-party applications
- Different vendors
- Different release schedules
- Different installers
- Different packaging requirements
- Testing processes
- Approvals
- Deployment mechanisms
- Maintenance windows
- Limited reporting

Operational Complexity Slows Remediation

Manual processes, security reviews, packaging, testing and deployment all create downstream bottlenecks that delay rollout.

Discovery is fast.
Remediation takes weeks or months.

Enterprise Risk by the Numbers

48%
of breaches involved
vulnerability exploitation

Hundreds
of third-party apps
per enterprise



429
security fixes in one
Chrome Stable release

55 Days
typical enterprise
remediation time

Reduce Risk Faster

Visibility alone doesn't reduce risk.
Faster remediation does.

Automate Third-Party Patching

Patch My PC operates within existing Microsoft management tools to identify third-party application updates quickly, download and test content centrally, and automate packaging and deployment tasks.

Click below to download our white paper:
[The Application Iceberg: The Hidden 80% of Enterprise Risk](#)