

# Hygiene & Exposure Management

Strong cyber hygiene is foundational to reducing risk. Unpatched systems, unmanaged assets, misconfigurations, and incomplete visibility create openings attackers can exploit. Brite helps organizations improve security hygiene through vulnerability management, patching support, configuration oversight, endpoint protection, and ongoing monitoring.

By combining assessment, prioritization, remediation tracking, and managed security operations, Brite helps customers focus on the exposures that matter most and close gaps before they become incidents.

## Why Hygiene & Exposure Management?

### Reduce Known Risk

Identify and address vulnerabilities, missing patches, and common configuration weaknesses across the environment.

### Prioritize Remediation

Focus limited IT and security resources on the issues that present the greatest operational or business risk.

### Improve Operational Accountability

Track remediation activity and security posture over time through reporting, reviews, and managed follow-up.



### Vulnerability Management

Use scanning & assessment tools to identify known vulnerabilities across endpoints, servers, applications, and infrastructure.



### Managed Patching Support

Support operating system and application patching efforts to reduce exposure from known exploitable flaws.



### Configuration & Policy Management

Review and manage security policies across endpoint, firewall, email, cloud, and identity environments.



### Asset Context & Prioritization

Map findings to business assets and operational impact so teams can focus on the most important risks first.



### Remediation Tracking

Monitor vulnerability and patch remediation progress to support closure, reporting, and accountability.

