bacon unlimited

WHITE PAPER

Fix What Others Can't

How to Tackle Vulnerabilities and Compliance Gaps Fast

Today, businesses face an overwhelming number of security vulnerabilities, often due to unpatched software, misconfigured systems, legacy applications, and unsecured endpoints. These vulnerabilities leave organizations exposed to ransomware, data breaches, and regulatory fines. In addition to operational and financial implications, vulnerabilities can also create risks for your reputation.

While many tools focus on patching, they can leave gaps in tackling configuration vulnerabilities, managing legacy systems, and ensuring compliance with regulations like NIST 800-171 and PCI DSS.

Leaders like you must understand how these gaps expose your business to unnecessary risks. More importantly, you need an approach that not only fixes what other tools can't, but also simplifies compliance and operational efficiency, enabling you to achieve a secure, resilient infrastructure.

The Vulnerability Problem

The volume of vulnerabilities reported globally has surged to over 25,000 in 2024, according to the National Vulnerability Database (NVD). Many of these vulnerabilities are being exploited faster than organizations can remediate them. This is particularly alarming given the significant financial, reputational, and operational costs businesses face when vulnerabilities are exploited.

For instance:

- The average cost of a data breach has reached $4.45 million as of 2023, a 15% increase over the last three years.
- Ransomware downtime costs businesses an average of $64,000 per hour, with remediation efforts often taking weeks to complete.
- Cyberattacks resulting from misconfigured systems and unpatched software account for nearly 70% of breaches in hybrid and cloud environments.

Why Business Leaders Should Care: Vulnerabilities are not just a technical issue—they represent a critical business risk. For executives, the stakes include:

Lost Revenue: Downtime or data breaches disrupt operations and drive away customers.

Fines and Legal Costs: Failing to comply with regulatory requirements can result in millions in fines.

Eroded Trust: A single incident can damage or even destroy the reputation a company has spent years building.

Understanding these risks is essential for making informed decisions about your IT and cybersecurity investments. It helps to think of vulnerability remediation as a critical business function, not just an IT task.

Why Traditional Approaches Fall Short: Vulnerability management tools have long been the go-to solution for addressing security risks. However, as IT environments become more complex, traditional tools often struggle to keep pace. They were not built for today's hybrid, multi-cloud world where endpoints span diverse operating systems and configurations.

A Growing Challenge: Businesses need solutions that go beyond identifying vulnerabilities—they need tools that fix them quickly, across all endpoints, while supporting compliance needs. Traditional approaches often fall short because they:

- Over-rely on patching as the only solution, leaving configuration vulnerabilities unaddressed.
- Struggle to provide real-time remediation, leaving organizations exposed for weeks.

The Cost of Vulnerabilities

$4.45 Million
Average cost of a data breach in 2023.

20+ Days
Average MTTR for critical vulnerabilities.

60%
Percentage of breaches linked to unpatched vulnerabilities.

75%
Time saved by automating vulnerability management.

"We caught five bad actors leveraging exploits within 48 hours of their disclosure. Bacon patched us the same day the exploits were made public."

Randall Hayes
Director of IT,
Systems Source.

- Lack visibility into hybrid or remote environments, creating blind spots.
- Fail to streamline compliance processes, forcing IT teams to manually track fixes.

Here's why these limitations put organizations at risk and how they can't keep up with the modern threat landscape.

1. Patching Alone Isn't Enough

- Many vulnerabilities require more than a patch. Misconfigurations, improper permissions, and unsecured endpoints demand attention, but traditional tools rarely address these issues.
- Legacy systems compound the problem, as vendors may no longer provide official patches, leaving critical systems perpetually vulnerable.

2. Slow Remediation Processes

- Mean Time to Repair (MTTR)—the time it takes to fix a vulnerability—often exceeds 20 days, with larger organizations taking even longer. This delay gives attackers ample opportunity to exploit critical weaknesses.

3. Incomplete Coverage

- Hybrid environments, remote work, and bring your own device (BYOD) policies mean IT teams often have limited visibility into endpoints. These blind spots create attractive targets for attackers.

4. Compliance Challenges

- Tracking and enforcing compliance manually is not sustainable, especially in industries like healthcare or finance where regulatory requirements are strict. Traditional tools provide little to no automation for compliance processes, leading to increased workloads and a higher risk of errors.

Fix What Others Can't: The Bacon Unlimited® Advantage

Bacon Unlimited was specifically designed to address the critical gaps left by traditional tools. Recognizing that businesses need a faster, broader, and more flexible approach, it was architected to solve vulnerabilities others can't, delivering real-time remediation, comprehensive endpoint coverage, and seamless compliance integration.

Unlike conventional solutions that rely solely on patching, Bacon Unlimited was designed to manage the full spectrum of vulnerabilities, including configuration issues and legacy systems. Its automation-first architecture minimizes exposure times and empowers IT teams to act decisively, even in complex environments.

Case Study
Systems Source

Challenge

Systems Source needed to meet stringent NIST 800-171 compliance requirements while managing 400 endpoints with a small IT team.

Solution

Bacon Unlimited automated patching, identified vulnerabilities immediately, and freed up 75% of IT staff time for other priorities.

Result

- Remediated critical vulnerabilities within hours of disclosure.
- Achieved compliance milestones efficiently.
- Freed up three weeks of IT staff time each month.

Systems Source.

1. Real-Time Remediation

Bacon Unlimited reduces MTTR to less than a minute:

- Automated Patching: Deploy updates across Windows, macOS, and Linux with zero downtime.
- Configuration Fixes: Securely adjust registry settings or permissions to mitigate vulnerabilities even when patches are unavailable.
- Legacy System Support: Protect unsupported software with virtual patching and proactive monitoring.

2. Comprehensive Endpoint Management

Bacon Unlimited ensures visibility and control across all endpoints, including:

- Hybrid environments with cloud and on-premise systems.
- BYOD endpoints, which often bypass traditional tools.
- Remote work setups that require seamless, secure management.

3. Simplified Compliance

- Automates compliance tracking for frameworks like NIST 800-171 and PCI DSS.
- Generates real-time reports for audits, providing clear evidence of endpoint security.
- Proactively enforces policies to maintain ongoing compliance.

There is an Answer!

The challenges of addressing vulnerabilities and meeting compliance standards are growing, but they don't have to overwhelm your organization. Bacon Unlimited goes beyond traditional solutions to fix what others can't, reducing risks, streamlining operations, and ensuring compliance.

Next Steps

Visit Bacon Unlimited to schedule a personalized demo and see how we can help secure your business.

"Bacon assisted us with NIST and CMMC compliance, increasing our confidence that all systems are secure."

Spencer Furey
Senior Manager,
Rand Worldwide

bacon unlimited

baconunlimited.com

Bacon Unlimited is a real-time endpoint management and vulnerability remediation platform that detects, fixes, and secures Windows, macOS, and Linux devices instantly—reducing risk, closing security gaps, and freeing IT teams from manual patching and configuration tasks.