Qualys

SUCCESS STORY



Closing Security Gaps with Fast, Comprehensive Patching

Imperial Brands Streamlines Remediation of Vulnerabilities in Third-Party Applications with Qualys Patch Management

Consumer Products

25,000
Employees

Inter-national

Business

Headquartered in Bristol, UK, Imperial Brands is an innovative global FMCG business. Operating a portfolio of brands including Davidoff, JPS and West cigarettes across 120 markets, the company generates £30bn in annual revenues.

Executive Summary

Thousands of Imperial Brands employees around the world rely on third-party applications to do their work. To rapidly act on vulnerabilities across thousands of endpoints, Imperial Brands is laying the foundations for automated patching with Qualys—cutting mean time to remediate by 20%.

Working with Qualys has been one of the best experiences we've ever had with a vendor. From the very beginning, the Qualys team was fully engaged with our cyber security goals—and we consider them a true partner."



TOM BLANE
Head of Cyber Security, Imperial Brands



Business Background

With thousands of employees working around the world, information security is a key requirement for Imperial Brands. The company operates an estate of approximately 14,000 workstations and around 4,000 servers—and to comply with stringent operational level agreements and external regulatory requirements, Imperial Brands aims to rapidly identify and remediate vulnerabilities. While the organization had mature scanning capabilities, its lean teams struggled to keep pace with a constant stream of remediation work.

Customer Environment



Hybrid cloud environment comprising Microsoft Windows workstations, on-premises servers and Microsoft Azure instances



Third-party collaboration and productivity applications for employees, including Google Chrome, Notepad++, 7-ZIP, and Zoom

Business Challenge



Streamline and accelerate the patching of third-party applications installed on employee devices



Prioritize remediation activities across thousands of on-premises and cloud systems



Strengthen security posture by reducing the total number of active vulnerabilities



Secure buy-in from system owners across the organization

Qualys Solution

By replacing its previous tools with Qualys Vulnerability Management, Detection and Response (VMDR®) and Qualys Patch Management, Imperial Brands is transforming its approach to remediation.

"In the past, we relied on Windows Server Update Services [WSUS] to patch our servers and Microsoft Intune to patch our workstations," explained Blane. "One of the big challenges of this approach was that it did not cover the breadth of third-party applications in use across the business, including Zoom and Google Chrome. With Qualys, we can extend our patching capabilities to cover those applications and more from a single point of control."

Working with Qualys, Imperial Brands rapidly configured network and agent-based scans across its 200 office and factory locations around the world. As an existing user of Microsoft Defender for Cloud, the company already had lightweight Qualys Cloud Agents deployed across its estate, further accelerating the deployment process.

"The team helped us to update our agents, automatically tag our endpoints, and scan our entire environment to establish a baseline vulnerability assessment. Next, we will explore the automation capabilities of Qualys Patch Management."

In the past, we relied on Windows Server Update Services [WSUS] to patch our servers and Microsoft Intune to patch our workstations. One of the big challenges of this approach was that it did not cover the breadth of third-party applications in use across the business, including Zoom and Google Chrome. With Qualys, we can extend our patching capabilities to cover those applications and more from a single point of control."

TOM BLANE
Head of Cyber Security, Imperial Brands

Qualys Difference



Enables Imperial Brands to manage remediation work for Microsoft Windows systems and third-party applications from a single platform



Augments Common Vulnerability Scoring System (CVSS) metrics with Qualys TruRisk scores, providing valuable decision-making context



Automatically determines the appropriate patches for vulnerabilities detected by VMDR



Offers zero-touch patching capabilities, powered by smart automation from Qualys



Provides **access to responsive** support services from Qualys experts

> It was really easy and quick to get started with Qualys”

TOM BLANE

Head of Cyber Security, Imperial Brands

Business Benefits

Reduced the number of critical/high **vulnerabilities by 68.4%** within 6 months

Projected to **cut mean time to remediate (MTTR) by 20%** within 12 months

Supports **automated patching** for Microsoft Windows as well as third-party applications

Delivers **deep insights** into vulnerabilities, including filtering by machine and software

Helps to **shrink the attack surface,** reducing the risk of a data breach

Schedule a demo with one of our technical account representatives.

Request a Demo

Qualys®

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. For more information, please visit qualys.com.

Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

For more information, please visit **qualys.com**

v250128

©2025 Qualys, Inc. All Rights Reserved.