

# Continuous Vulnerability Management

See Everything, Secure Everything

Dataprise's Vulnerability Management service delivers extensive identification, assessment, and remediation of vulnerabilities across your entire IT environment through a combination of automated scanning, expert risk analysis, and comprehensive patching. Our proactive approach ensures you have actionable intelligence about current and emerging vulnerabilities, including detailed risk assessments and treatment recommendations tailored to your business operations.

Built on proven frameworks including NIST Risk Management Framework and CISA Cyber Resilience Review standards, our service combines industry-leading automated tools with expert security analysis. This end-to-end approach, enhanced by threat intelligence, ensures vulnerabilities are identified and addressed before they can be exploited.

## You'll Get...



### Fully Automated Patching:

Automated monthly patching for supported operating systems and third-party applications, helping reduce risk at scale with minimal effort for your team.



### Comprehensive Visibility and Protection:

Complete vulnerability coverage across Windows, MacOS, and Linux systems, third-party applications, network devices, IoT equipment, and public-facing IP addresses.



### Expert Risk Advising:

Clear direction on which vulnerabilities to fix first based on actual business impact and current threat landscape, so you can focus on the risks that truly matter to your organization.



### Proactive Threat Response:

Rapid analysis and escalation when new or actively exploited vulnerabilities emerge, helping reduce exposure windows.



### Regulatory Compliance Alignment:

Built-in alignment with major regulatory and industry frameworks, including NIST 800-171, CIS benchmarks, and NYDFS, through endpoint and Microsoft 365 benchmark assessments.





## Our Process:



### Identify:

We perform comprehensive asset discovery and deploy automated scanning tools to identify vulnerabilities, misconfigurations, and security weaknesses. Our tailored approach adapts to your specific operational requirements using both credentialed and non-credentialed methods.



### Assess:

Our security analysts assess identified vulnerabilities to understand severity and relevance within your environment. This assessment incorporates CVSS and EPSS scores, asset criticality, exposure, and threat intelligence to determine potential business impact and escalation needs.



### Prioritize:

We rank vulnerabilities based on real-world risk. Our experts will highlight those that pose the greatest threat to your business or are actively exploited so remediation efforts focus on the greatest risks.



### Remediate:

Our team supports both automated patch deployment and manual remediation, helping ensure high-impact vulnerabilities are addressed quickly and effectively. After remediation activities, we perform validation scans during scheduled scanning cycles to confirm vulnerabilities have been addressed.



### Report:

You'll receive clear, consolidated monthly reports that highlight current vulnerabilities, remediation progress, patching results, trends over time, and alignment with relevant security benchmarks. Each report is reviewed during a monthly meeting with your dedicated security expert to ensure clarity, answer questions, and guide next steps.

