

» WHITE PAPER

6 ways Flexera reduces cybersecurity risk for government agencies

A comprehensive guide to filling
the security capability void

flexeraTM

6 ways Flexera reduces cybersecurity risk for government agencies

A comprehensive guide to filling the security capability void

» SUMMARY

Rather than merely defending perimeters or offering incident responses, Flexera proactively reduces risk by eliminating blind spots and illuminating the entire attack surface, including vulnerabilities. We fill the capability void left by other cybersecurity vendors and offer unparalleled IT asset and vulnerability intelligence. Our solution enhances the operational effectiveness of government cyber teams by providing detailed data and intelligence, thereby supporting Zero Trust mandates. From identifying assets at or near the end of their support life to prioritizing and accelerating patch deployments, Flexera offers a unified, data-driven approach to managing cyber risk smartly and methodically. Our focus is not just to provide a security solution, but to arm your agency with the actionable insights needed to securely navigate the complex IT environment.

Flexera advances cybersecurity programs, including those supporting Zero Trust mandates, and lowers risk for federal, state and local government agencies by:

Delivering IT Visibility with Flexera One

We show you your entire attack surface—including shadow IT, known cyber vulnerabilities, end-of-support and end-of-life (EOS/EOL) information, interdependencies among IT assets, and service maps that depict how assets work together to support your agency's citizen and business services.

Flexera's IT Visibility solution catalogs your entire IT landscape and enhances that with vulnerability, threat and IT asset market intelligence not available anywhere else, thereby eliminating your blind spots. In addition, Flexera takes this comprehensive security data and consolidates, deduplicates and normalizes it, and makes it available for other systems and automated processes to use.

Alerting you to IT assets at or near EOS/EOL

Only Flexera can show you exactly which assets on your network are—or will soon be—no longer supported by their manufacturers and thus pose significant cyber risks.

That's because Flexera maintains the world's most extensive library of detailed market information about IT assets, including insights from Flexera's Software Vulnerability Research. This information is critical when prioritizing modernization and technology refresh investments and initiatives.

Identifying cyber vulnerabilities with Flexera Software Vulnerability Manager

Flexera presents a clear picture of the vulnerability status of your IT environment, including identifying all Common Vulnerabilities and Exposures (CVEs) for operating systems, apps, virtual machines and containers.

Leveraging Secunia Research, Flexera then automatically delivers links to the relevant patches so they can be deployed manually or automatically. By delivering deep insight into the vulnerabilities themselves through accurate, up-to-date vulnerability research and trustworthy threat intelligence, Flexera significantly accelerates and expands coverage for patch management regimes that employ traditional scanning tools and patch catalogs.

Smartly prioritizing patch deployments

There's not enough time in the day to deploy all the patches needed within a large agency enterprise. Flexera's cyber risk intelligence capabilities help your cyber teams tailor their patch prioritization and remediation efforts based on a wide assortment of factors, including a vulnerability's criticality, its likelihood of exploitation, the impact of a possible exploitation, its Common Vulnerability Scoring System (CVSS) threat score and others.

Flexera's Software Vulnerability Manager provides risk context and information, allowing organizations to leverage threat intelligence, workflows, tickets and alerts to mitigate the risk of costly breaches.

Accelerating patch deployments with Flexera's extensive patch library

Flexera offers the largest set of ready-to-deploy patches that have been thoroughly tested and packaged so your agency cyber teams can deploy them immediately and with confidence. Flexera also simplifies the building of more than 1,700 additional patches.

With Flexera, government cyber teams dramatically reduce time spent on researching, configuring and testing patches and have access to more patches and patch details than with any other solution on the market.

Consider the complete picture



Effectively prioritize software vulnerabilities in your IT estate

Getting you the right data for the right task

Government cyber teams need detailed data to understand their on-premises hardware and software, their cloud-based technology resources, the interdependencies among assets, their cyber risk postures, the status of their remediation efforts and more.

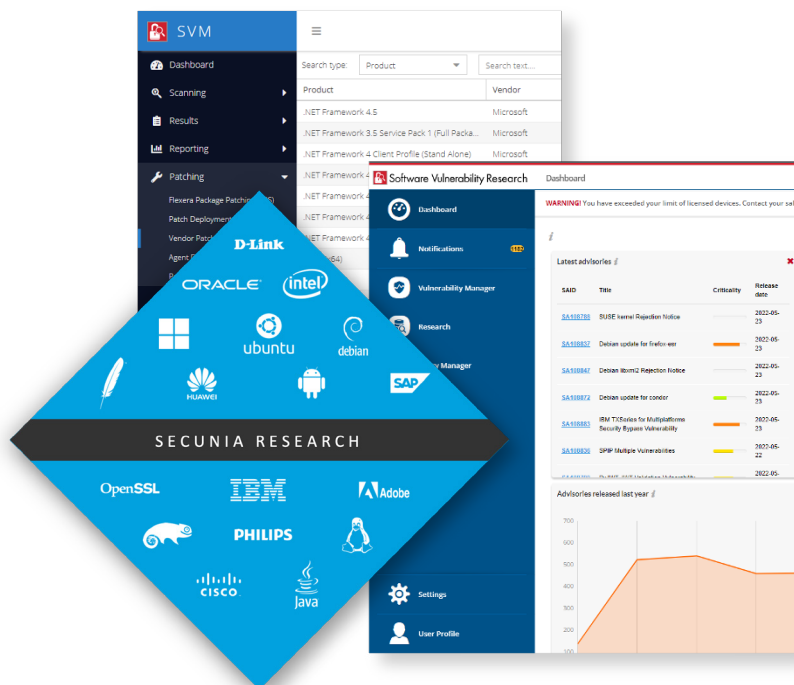
Flexera automates all aspects of data capture, consolidation and analysis, and presents an easy-to-navigate, unified view of the entire technology landscape. Moreover, we can help you leverage your cyber data to derive maximum value from it.

Why Flexera

Only Flexera delivers government cyber teams the trusted, accurate, complete vulnerability intelligence, threat intelligence, vendor patch data, reliable research and effective assessment they need to reduce risk and remove blind spots significantly beyond the capabilities of their existing cybersecurity architectures.

With Flexera, federal, state and local government agencies can bring order to the chaos of vulnerability management with an intelligent, prioritized approach based on deep insight into the vulnerabilities they face.

Software Vulnerability Management and Software Vulnerability Research empower IT professionals to identify, prioritize and remediate vulnerabilities



- **Vetted vulnerability and threat intelligence** for over 69,000 product versions
- **Largest patch catalog** on the market with updated detail on over 5,800 installers
- **95% of security advisories issued within 1 day**
- **20+ years as market leader**, powered by Secunia Research

SVM, SVR and Secunia Research combine to get you the data you need to stay secure and up to date

And because Flexera is continuously enhancing our vulnerability management technologies and updating our extensive IT asset knowledge base, our government clients can keep their IT environments safe now and into the future.

Conclusion

In the cyber arena, our lane is narrow but critical. You can't address the vulnerabilities you can't see. Flexera arms your cyber teams with the data and intelligence they need to eliminate blind spots and manage cyber risk smartly and methodically, no matter how large or complex the IT environment may be.

To find out more about how Flexera can improve your agency's cybersecurity posture, contact Michael Anthony, Vice President, Flexera Public Sector at 703-509-2472 or manthony@flexera.com.

About Flexera

Flexera saves customers billions of dollars in wasted technology spend. A pioneer in Hybrid ITAM and FinOps, Flexera provides award-winning, data-oriented SaaS solutions for technology value optimization (TVO), enabling IT, finance, procurement and cloud teams to gain deep insights into cost optimization, compliance and risks for each business service. Flexera One solutions are built on a set of definitive customer, supplier and industry data, powered by Technopedia, that enables organizations to visualize their Enterprise Technology Blueprint™ in hybrid environments—from on-premises to SaaS to containers to cloud.

More than 50,000 customers subscribe to Flexera's technology value optimization solutions, delivered by 1,300+ team members worldwide. Learn more at flexera.com

» NEXT STEPS

Fill the security gap
in your IT estate

CONTACT US