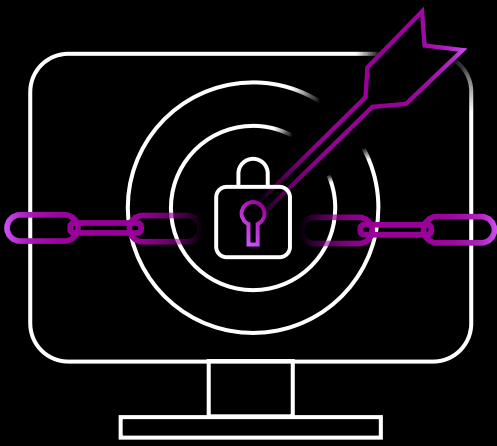


Open-Source on the Mainframe: Are You At Risk?

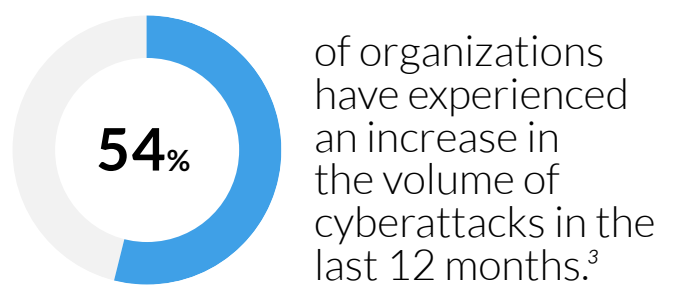
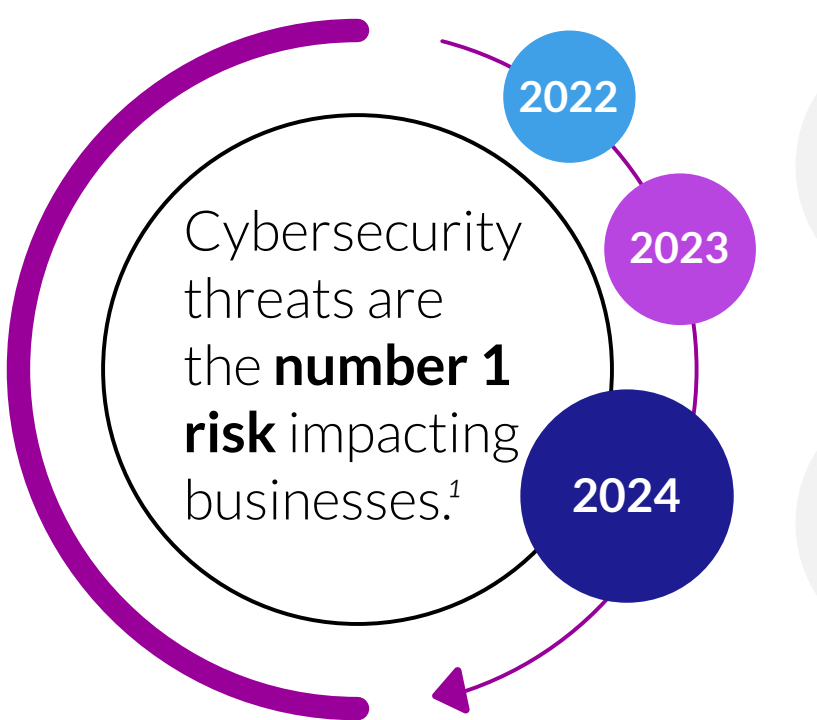
There is a misperception at the C-suite level that the mainframe is immune to cyberattacks. But due to the proliferation of open-source software, that perception is false.

Protect your organization with Rocket® Open Source Solutions for z/OS®



Ransomware is the biggest cyberthreat for organizations.

Cyberattacks are growing in volume, variety, complexity and precision.



63% of IT leaders measure success by their ability to reduce risk.⁵



\$10.5 Trillion is what cybercrime will cost the world annually by 2025, up from \$3 trillion in 2015.⁵

300% increase in cyber attacks on small and medium sized businesses in 2020 compared to the previous year.⁶



67% of companies have experienced an open source security vulnerability in the last 2 Years.⁷

Are you asking the right questions about open-source software?

Do you know if you're using open-source software on z/OS?

Do you know the risks that open-source vulnerabilities pose to your mainframe and business?

Do you know who is writing the open-source code that is already implemented on your mainframe?

Do you know that open-source vulnerabilities may be lying dormant in your business?

Do you know that it can take months to implement fixes to open-source security vulnerabilities without vendor support?

Do you know unsupported open-source software puts you at risk of not meeting regulatory compliance requirements for your business and industry?

Rocket Software can fix critical vulnerabilities and deliver currency updates for open source for z/OS within days.

Rocket Software has ported over 20 open-source languages and tools to z/OS and offers full security and support for Open Mainframe Project's Zowe open-source framework.

Secure your mainframe without losing the benefits of open-source software.

[Talk to an expert](#)

Visit RocketSoftware.com >