IBM **Security**

## Implementing OMB M-21-31 using IBM Security solutions

Federal government agencies clearly have complex, hybrid and multi-cloud, multi-vendor cybersecurity environments to manage. While threats continue to increase and skill gaps grow, leaders tasked with navigating these challenges also need to address government mandates and timelines, including Executive Order (EO) 14028 from May 2021.

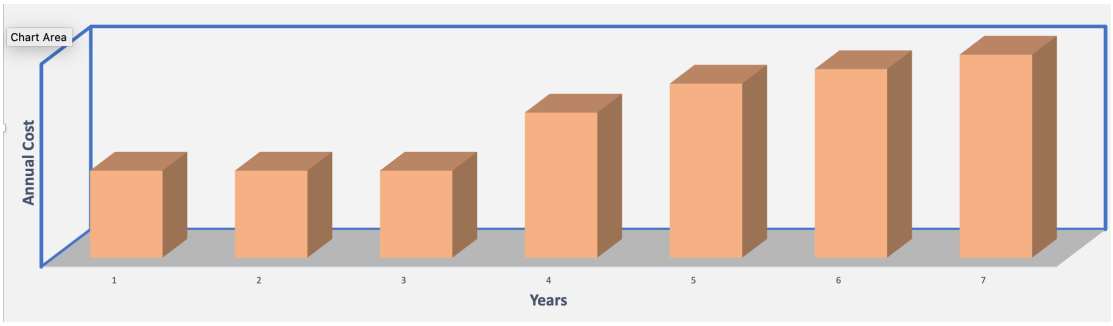
OMB memorandum M-21-31, *"Improving the Federal Government's Investigation and Remediation Capabilities Related to Cybersecurity Incidents"*, August 2021, mandated agencies meet specific logging of IT activity, with specific log retention and log management requirements. The order ensures a progression towards uniform log management.

There is a compelling need for a robust and flexible logging solution to address struggles such as an expanded attack surface caused by **growing complexity and unknown assets on the network**, security risks with increased volume of remote users, and spiraling and unpredictable costs.

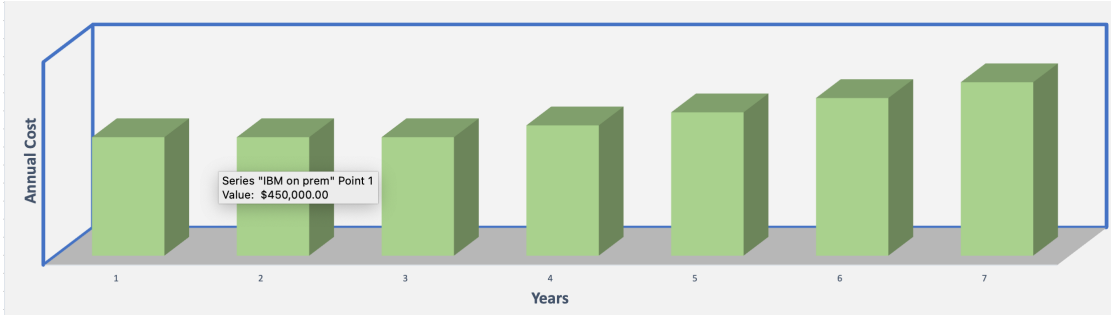
As you consider going forward solutions to predict, prevent and respond to modern threats and protect your data, two major considerations include:

- how to achieve fast time to value and compliance - meeting M-21-31 requirements, and
- how to assess total cost of computing, including infrastructure, and stabilize long term costs.

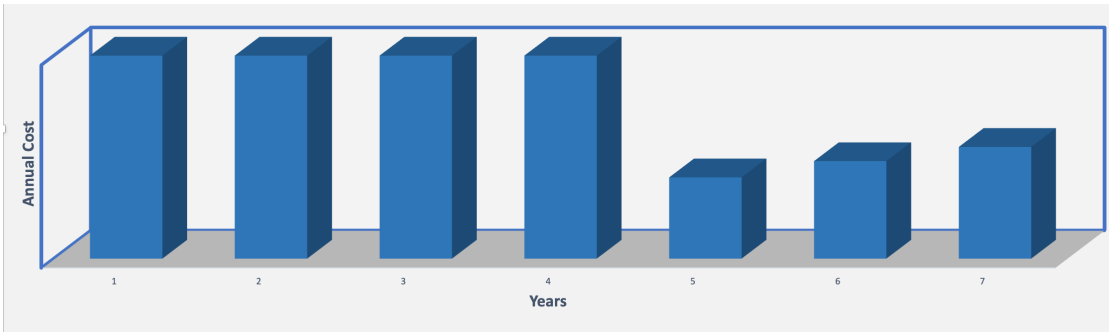
What do your costs look like today? Do you have unpredictable or less unpredictable costs with potential large increases over time depending on volume of data?




Are you aiming for more predictable costs, linear over time? Or as an alternative, more predictable costs with up-front perpetual licenses purchase yet lower ongoing costs in out years?



IBM **Security**



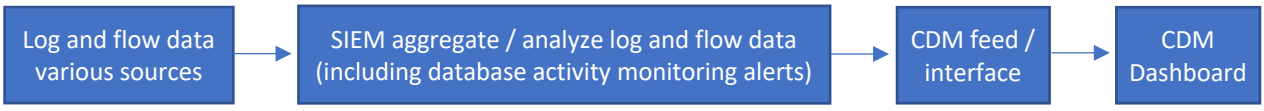

IBM Security offers an advanced and integrated portfolio of enterprise security products and services with predictable costs. An extensive range of cybersecurity capabilities is also provided through our business partner ecosystem. **IBM cybersecurity solutions for U.S. Federal** offer an open and unified approach to Zero Trust that puts security everywhere, so an organization can thrive everywhere.

**IBM Security QRadar** is a robust, next generation SIEM solution to help security teams detect, prioritize, and respond to threats across the organization. QRadar automatically aggregates and analyzes log and flow data from the devices, endpoints and apps across your network. It offers advanced analytics such as user behavior analytics (UBA), network flow insights and artificial intelligence (AI) to accelerate detection, and the solution integrates seamlessly with security orchestration, automation, and response (SOAR) platforms for incident response and remediation. **Logging yet much more!** Licenses are available both as a Software as a Service/SaaS subscription (like the model in "green" above) or on-premises, perpetual licenses (similar to "blue" model).

**IBM Security Guardium** is a modern, scalable data security platform to protect what matters most – your agency's data – whether in the cloud or on premise. Its end-to-end security framework includes discovery and classification, vulnerability management, protection and encryption, privacy and compliance, threat detection, and response. In 3Q21, IBM Guardium Data Protection offering added an **"out of the box" policy to map the requirements in M-21-31**, focused on database level logging. Logging yet much more! Guardium licenses are available as on-premises, perpetual licenses.

Why IBM? We offer **market-leading, SaaS and on-premises** solution options. IBM solutions help you **meet EL0-EL3 mandates under M-21-31,** achieve fast time to value and **better predict long-term costs** over 5-7+ years with server / resource-based, not workload / data volume-based, pricing.

IBM Security **offers a no-fee workshop option and financing** through IBM Global Financing for initial, up-front charges, as applicable. Let's explore how we can provide the lowest multi-year cost for performance, helping you save on logging costs and potentially fund other projects. Might an architecture approach that adds QRadar and other IBM Security offerings work in your environment?




To learn more about how our solutions might address your requirements, fit into your cybersecurity architecture and complement your existing environment, please check out our **IBM cybersecurity solutions for US Federal web page** at https://www.ibm.com/industries/federal/security or reach out to an IBM contact.