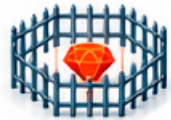


What Every Government Needs To Contain AI Cyber Threats



Zero Trust

All systems need this architectural and policy framework, which assumes everyone is a threat unless a user has explicit permission to access a particular segment of a system.



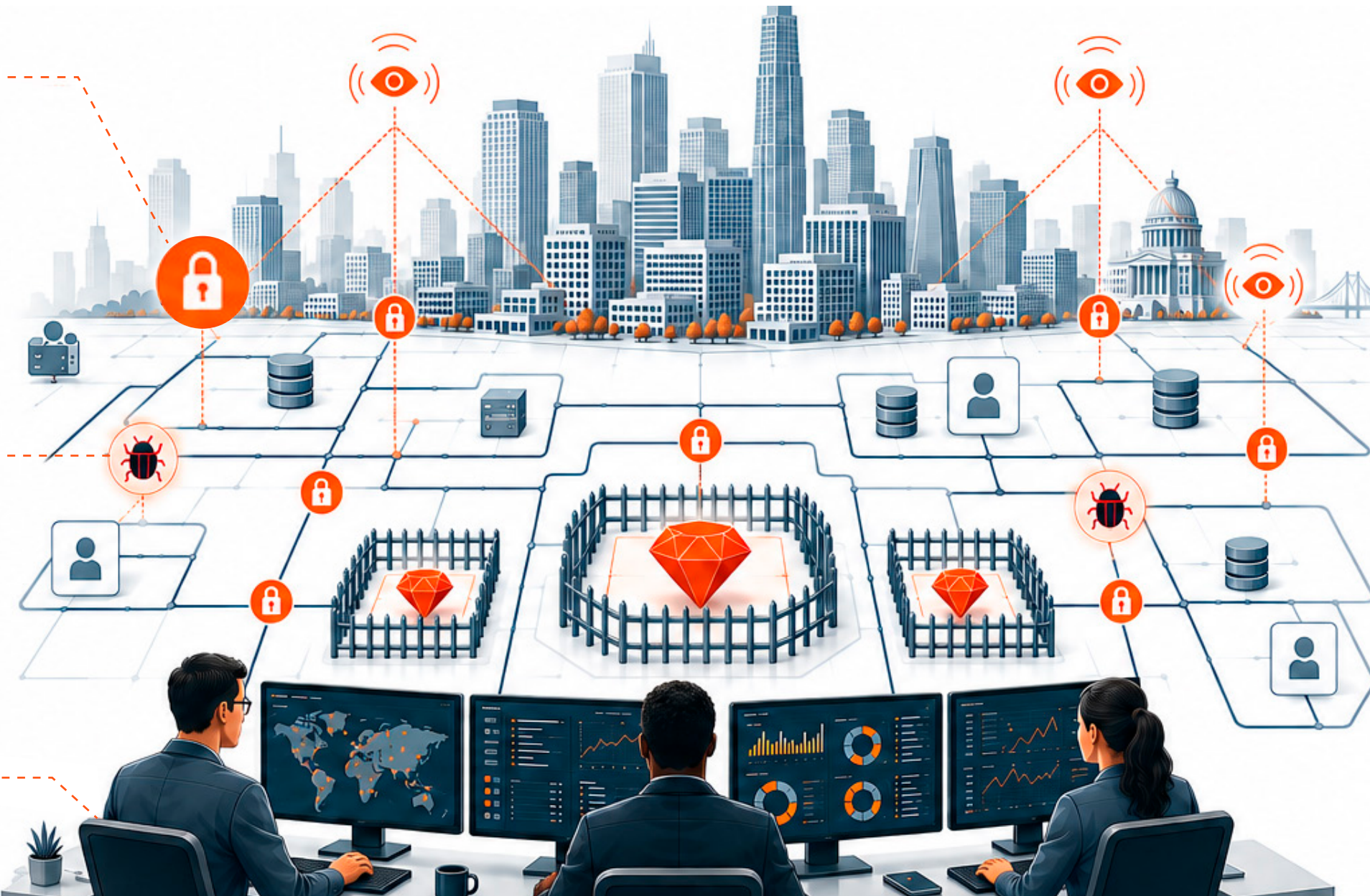
Micro Segmentation

Organizations must assume they will be breached given the speed of frontier AI. But with micro segmentation, valuable data remains outside of the reach of cybercriminals — fenced off from any breaches.



Real-Time Visibility

The sheer number of potential threats that could occur at any given moment means real-time visibility across every part of the system is essential.



ZERO TRUST
(Access Controls)



MICRO SEGMENTATION
(Data Protection)



REAL-TIME VISIBILITY
(Threat Detection)



THREATS/BREACHES
(Detected)

5 Steps to Zero Trust

1



Define protect surface.

2



Map transaction flows.

3



Architect a Zero-Trust environment.

4



Create a Zero-Trust policy.

5



Monitor and maintain.