Is your agency secure and Resilient?

The 2018 Security Capabilities Benchmark Study found that many government agencies are unprepared for the growing wave of cyber threats.

Only 10% felt extremely effective in determining scope, containing, and remediating a breach.

We found 4 key adversaries using 4 evolving methods.

- **nation states** attack national, utility, and political infrastructure
- **hacktivists** attack political, utility, and services infrastructure
- **insider threats** attack military, political, and services infrastructure
- **for-profit** attack all levels of government for financial gain

Over 53% felt a lack of expertise and trained personnel is keeping them from adopting advanced security processes and technologies.

There is a growing need for cybersecurity that is simple, open, and automated.

- **mass transit** need rate tables, protect revenue, secure equipment and facilities
- **privacy** need secure people data, protect case evidence, and increase visibility into networks
- **energy** need to keep electricity flowing, secure facilities, automate detection and response
- **transportation** need to improve traffic flow, reduce accidents, and enhance real-time notification

Embed security. Embrace resilience.

Learn how in our 2018 Annual Cybersecurity Report: Impacts on Government

Become Cyber Resilient