CyberRes

Flyer

Resilient Digital Public Sector and Government Services

Governments are being driven to rapidly expand digital services to their citizens, reduce cybersecurity incidents and breach impacts, and lower operating costs. Implementing the right technologies to achieve these goals can dramatically improve overall services' resilience at no additional cost.

Achieving Resilient Government

The 2017 National Security Strategy has driven the Federal government to invest heavily in cybersecurity defenses, reporting, and remediation. Aligning the defensive posture with increasing citizen expectations for digital services can put responsiveness and resilience at odds. CyberRes solutions help strengthen government resilience in four key areas.

Data Exfiltration Mitigation

Data security controls embedded within existing IT applications are proving increasingly ineffective as data has become more pervasive, mobile, and cross functional. Governments must now assume that data will be stolen, so the goal is to reduce or eliminate the value of the stolen data.

Zero Trust through TIC 3.0

TIC 3.0 is requiring least-privileged access, data protection, and resilient and automated incident response. CyberRes delivers zero trust to reduce risks, speed deployment, and lower costs.

Continuous Diagnostics and Mitigation

Insider threats (insiders, third parties, entities, malicious code resources, digital supply chain, etc.) are the primary threat risk to federal data security and mission readiness. Dynamic user behavior analysis with real-time responses to breaches and attempts is the key to successful continuous diagnostics and mitigation.

Zero Outage

By moving security to the left in the system development process, governments can accelerate delivery timelines, dramatically increase system availability, reduce recovery timelines, and reduce rework costs related to security issues in software.

Data Exfiltration Mitigation

As recent cybersecurity incidents have shown, data protected only by disk, database, and application encryption is still very vulnerable to exfiltration. With most organizations now using multiple cloud providers, protecting sensitive data across hybrid IT is increasingly challenging.

Unlike traditional encryption, which tends to mask data to the point where it is no longer usable and appears like a long string of nonsensical characters, FPE and FPH maintain the format and structure of data so that it appears like real data to machines that are using it.

NIST-compliant format-preserving encryption solutions ensure that even stolen data has no value. They streamline information classification by automatically identifying critical and sensitive data, applying governance policies, and enabling the appropriate controls on data to move, govern, dispose, protect, and encrypt—enabling the safe use of data in analytics and applications and, ultimately, protecting data in use, in transit, and at rest.

This enables governments to:

- Protect sensitive production data at the field level, regardless of the privilege of the user or system service.
- Greatly reduce the impact of any data exfiltration by anonymizing segments of data fields without altering the value of the data in data analytics efforts.
- Automate extraction, encryption, hashing, or masking and archiving of test data as needed across use cases.

Zero Trust through TIC 3.0

Zero trust, like TIC 3.0, recognizes that perimeter-based security is no longer sufficient. This is due in part to so many users or systems working outside the perimeter. In addition, malicious actors have become much more proficient at stealing credentials and getting inside the perimeter. Consequently, zero trust assumes there is no implicit trust granted to assets (such as data) or user accounts based only on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).

Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary.

Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), rather than network elements, because network-centric security is no longer sufficient to ensure the security posture of data. While it’s a large effort in total, beginning to address zero trust with practical, tactical investments can yield significant reductions in both the frequency of breach and breach impacts.

> “NetIQ meets our organization’s current and future requirements. We have found the solutions very reliable. We are set for future growth and are very confident that the system will grow with us.”
>
> Chief Technology Officer
> Civilian Government Agency

Continuous Diagnostics and Mitigation

Government agencies continue to invest in the Continuous Diagnostic and Mitigation (CDM) program, although there is a significant gap in recommended approaches and actual implementation by agencies.

The CDM program has emphasized automating network monitoring and incident reporting and roll-up. While these are critical steps, the real improvements in cyberdefense and response will require improved correlation of critical security-related information, automation of standard responses to decrease workload on SOC personnel, continuous user and entity behavior analysis, and enhanced risk-based decision-making.

Advanced CDM solutions from CyberRes enable administrators and leadership to know the state of their respective networks at any given time and enable SOC personnel and management to focus on the largest and most risky threats on a real-time basis.

This enables governments to:

- Improve security analyst efficiency 10x-15x by correlating events, organizing related events, and automating typical responses.
- Improve response and efficiency as AI and ML improve user, entity, and application behaviors over time.
- Increase automation to identify assets.
- Improve accuracy, reporting, risk management decision-making, and incident response.
- Enhance near real-time monitoring and risk response.

Zero Outage

Outages of IT services are most often associated with the misbehavior or errors of operating personnel, or with technical problems—which might, for example, be attributed to errors in the design. Analysis has shown that over the past five years, 76 percent of all published vulnerabilities were from applications. Given this radical shift in attacker focus, it's time to embed security from design, through development, and into production. The best way to do this is to focus on building safer code during initial development, rather than waiting for a security acceptance test late in the development cycle.

Zero outage is a growing global approach and framework that emphasizes standardization in the quality of IT platforms, people, processes, and security throughout the whole lifecycle. Doing this will enable organizations to minimize errors, increase availability, ensure security, and operate more cost-effectively.

This enables governments to:

- Reduce the cost of fixing security issues by 90%.
- Reduce incident recovery times by over 50%.
- Reduce the time-to-effective for new IT personnel.

CyberRes Capabilities for Resilient Government Services

CyberRes is a Micro Focus line of business. We bring the expertise of one of the world's largest security portfolios to helping our customers navigate the changing threat landscape by driving both cyber and business resiliency within their teams and organizations. We are here to help enterprises accelerate trust, reliability, and survivability through times of adversity, crisis, and business volatility.

Our products have delivered trusted and proven mission-critical software for government and public-sector organizations for more than 40 years.

We are part of a larger set of digital transformation solutions that fight adverse conditions so businesses can continue to run today to keep the lights on and transform to grow and take advantage of tomorrow's opportunities.

CyberRes capabilities for resilient government services include:

- AI-driven monitoring of user behavior and potential insider threats, assigning risk scores to users and services real-time, and adjusting the access to data accordingly.
- Centralized identity and access management to ensure least-privileged access to all managed systems, helping agencies digitally transform their environment and build a solid security foundation for the zero trust methodology.
- Automated incident response and escalation, reducing the event noise that front-line security personnel need to address.
- Format-preserving encryption that ensures even stolen data has limited or no value.

Learn more at **cyberres.com/industry/public-sector-government**

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes
A Micro Focus line of business