State and Local Government Solutions

4 Security Considerations for Better Organizational Resiliency

The recent global pandemic taught us that anything can happen. Yet whatever the event—from weather emergency to civil unrest—state and local governments must continue to serve their communities and provide essential services.

Technology teams inside government agencies are gathering and analyzing data to help them stay agile and deliver the right response to any situation. Yet the more data-driven they become, the more enticing they are for cyberattackers.

AT LEAST 113
state and local governments in the U.S. were affected by ransomware in 2020[1]

$18.88 BILLION
is the total cost to American government organizations for recovery and downtime caused by ransomware attacks in 2020[2]

$665,000 TO $40.53 MILLION
is the average cost of a cybersecurity breach to state governments[3]

22 DAYS
is the average length of interruption after ransomware attacks on businesses and organizations in the U.S.[4]

How are state and local government leaders responding?

In 2022, the Center for Digital Government surveyed IT leaders in state and local agencies to gain more insight into their cybersecurity concerns.[5]

Here's what they found:

More than
4 IN 10
reported not being fully confident in their organization's ability to protect against cyberthreats

48.4%
say they use separate products for issues such as endpoint security, network security, data center security, and application security

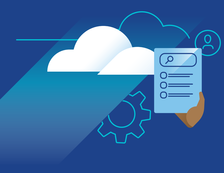
2 OF THE TOP 3
challenges are staffing-related, including a lack of staff and cybersecurity skillsets

4 security initiatives that build organizational resilience

1 Adopt a Zero Trust architecture (ZTA)

ZTA helps you better secure data and supports greater productivity, organizational agility, and improved user experiences.

Why it's important
With the growth of remote and hybrid work, security methods based on the network perimeter are no longer effective.



2 Expand the use of identity and access management (IAM)

With IAM, IT teams can spend less effort, time and money on manually managing network access while reducing the risk of internal and external data breaches.

Why it's important
Traditional methods based on different sign-ons for every app or system create management headaches and security risks.

3 Modernize applications

Modern apps provide the ability to offer new features and functionality to citizens and workers while mitigating cyber risks.

Why it's important
The security threats that exist today didn't exist when legacy applications were designed, so many are vulnerable to techniques and exploits that attackers can use to breach a government system.

4 Migrate to one or more clouds

Using the cloud—or multiple clouds—provides improved security, better failover options, and enhanced disaster recovery.

Why it's important
If all of your apps and data are located in a single, on-premises data center (or even a single cloud environment), your agency is vulnerable in the case of failure or another kind of disastrous event.

VMware solutions help you protect citizen data and grow resiliency

VMware is a trusted partner for state and local government agencies. No matter where you are in your security journey, VMware will help you determine where you are now, where you want to be, and how to get there.

Our security solutions can help you improve your security posture from endpoint to app to cloud to network.

Find out why state and local governments are securing their environments with VMware.

LEARN MORE

1. ICMA. *"A Look at Local Government Cybersecurity in 2020."* Donald F. Norris. July 14, 2021.
2. American City and County. *"Report: Ransomware attacks cost local and state governments over $18 billion in 2020."* Jason Axelrod. March 22, 2021.
3. KnowBe4. *"The Economic Impact of Cyber Attacks on Municipalities."* 2020.
4. Statista. *"Length of impact after a ransomware attack Q1 2020–Q3 2021."* Joseph Johnson. November 10, 2021.
5. Center for Digital Government. *"Cybersecurity Survey 2022: Custom Research Commissioned by VMware."*