SECURITY SOLUTIONS
FOR GOVERNMENT

State and local government organizations are highly attractive to cybercriminals, who see them as both vulnerable and highly profitable.

These offices collect and manage massive amounts of personal and financial information. It needs to be secured, but also readily available online—making it vulnerable to loss or theft. Not only can criminals steal this data outright to be sold or used for fraud, they can encrypt it via ransomware to extort payments of millions of dollars.

Many government entities also control critical operations, such as power grids or water systems, that must be fully functional at all times. Ransomware or DDoS attacks that deny access to vital services in demand for payment can be particularly dangerous, as hackers know organizations will often pay up rather than interrupt service.

Finally, government systems are often targeted by hacktivists seeking to leak information, damage reputations or disrupt operations.

ESET's solutions for state and local government

ESET security solutions address the challenges common to organizations nationwide, including:

- Securing confidential information, such as tax records and credit card numbers, while also providing online access
- Preventing interruptions or shutdowns of vital services, such as electricity or water, caused by ransomware or DDoS attacks
- Budget restraints exacerbated by the Covid-19 pandemic, including loss of tax revenues
- Equipment ranging from legacy hardware and multiple OSes to the latest mobile devices
- Compliance, auditing and reporting requirements driven by PCI DSS, ADA, FISMA, HIPAA and more
- The need for cybersecurity education for all employees

$18.9B: Cost of ransomware attacks on US government organizations in 2020. [1]

In 2020, U.S. government organizations suffered 79 ransomware attacks, which potentially impacted 71 million people. [2]

CISA reported ransomware incidents against 14 of the 16 U.S. critical infrastructure sectors, including IT. emergency services and food/agriculture, in 2021. [3]

Only 38% of respondents working for state and local governments said they had received cybersecurity training. [4]

Recommended products:

ENDPOINT SECURITY
Combines multilayered technology, machine learning and human expertise to provide cross-platform protection for desktops, laptops and mobile devices.

ENCRYPTION
Ensures that patient data stored on removable drives, laptops, and emails is unreadable to unauthorized parties, giving you safe harbor from HIPAA penalties.

TWO-FACTOR AUTHENTICATION
Limits access to data and equipment to authorized users by requiring a one-time-only password, meeting requirements for data security.

CLOUD-BASED SANDBOX ANALYSIS
Provides advanced, proactive protection against threats like ransomware and zero-day exploits by analyzing suspicious samples in an isolated cloud sandbox environment.

BACKUP AND RECOVERY
Safeguards data, applications, and systems in both physical and virtual environments to help you recover from a lockdown due to ransomware or shutdowns caused by natural disaster.

CYBERSECURITY TRAINING
Adds a vital layer of protection by educating employees on how to recognize phishing, avoid online scams, create strong passwords and understand internet safety best practices.

ESET business solutions for state and local government

ESET PROTECT solutions include the following components:

Endpoint protection
Advanced multilayered protection for computers, smartphones and virtual machines.

Server security
Real-time protection for data passing through all general servers.

Remote management console
Single-pane-of-glass remote management; available via cloud or on-premises.

Additional solutions include:

Endpoint detection and response for increased visibility into emerging threats, risky employee behaviors and unwanted applications.

Two-factor authentication to restrict access to networks, devices and data and meet compliance requirements.

Online cybersecurity awareness training for faculty and staff to reduce risks posed by phishing, social engineering and other scams.

	ESET PROTECT Entry	ESET PROTECT Advanced	ESET PROTECT Complete	ESET PROTECT Enterprise	ESET PROTECT Mail Plus
Remote management via cloud or on-premises console	✔	✔	✔	✔	✔
Endpoint protection	✔	✔	✔	✔	
Server security	✔	✔	✔	✔	
Full disk encryption		✔	✔	✔	
Cloud sandbox		✔	✔	✔	✔
Mail security			✔		✔
Cloud app protection			✔		
EDR				✔*	

* Currently available on-premises only

Testimonials

ESET CYBERSECURITY AWARENESS TRAINING PREMIUM:

"I knew this training was beneficial…when many employees told me they picked up on the recent phishing attacks through email and avoided clicking on attachments that contained viruses."

—Director of IT & Communications, City of Jamestown, New York. **SEE CASE STUDY**

"The interactive nature and interesting content make it easy for users to pay attention and test what they are learning."

—Spokeswoman, large city government organization **SEE CASE STUDY**

ESET ENDPOINT PROTECTION ADVANCED:

"The fact that it just works and is low on maintenance needs, combined with the ease of install and reasonable pricing, really helps an understaffed IT department."

—System Administrator, Johnson County, Texas **SEE CASE STUDY**

Sources:

[1,2] Comparitech.com. March 2021.
[3] Cybersecurity and Infrastructure Security Agency, Feb. 2022.
[4] IBM-Harris Poll Survey. 2020. Public Sector Security Research.