EXECUTIVE BRIEF

Strengthen government cybersecurity with unified threat management

Spectrum ENTERPRISE

Keeping infrastructure like roads and bridges in good condition is vital to public safety. That's just as true for digital infrastructure and cybersecurity. It's not just data that is at risk: Actual lives can be threatened as some attacks have disrupted systems that support emergency services.[1]

Even so, state and local governments have long wrestled with budgetary limits, competing priorities and lack of IT security expertise. According to one report, fewer than 40 percent of states have a dedicated budget line item for cybersecurity.[2] Meanwhile, even large private-sector employers say they face a worsening skills shortage as demand for security expertise continues to grow rapidly.[3] Compounding this problem is the piecemeal approach to security that emerges as organizations adopt different tools from a variety of vendors over time. Security measures that aren't engineered to work in sync — and the added complexity of keeping them up to date — increase the potential for gaps that bad actors can exploit.

Security measures that aren't engineered to work in sync — and the added complexity of keeping them up to date — increase the potential for gaps that bad actors can exploit.

The result has been a growing volume of attacks on agencies that sometimes lack the resources to protect sensitive citizen data and systems that underlie essential public services. According to an August 2020 report, cyberattacks on state and local government were up 50 percent since 2017 — and they show no signs of slowing down.[4]

One answer to the growing security challenge is unified threat management (UTM). A UTM solution brings together a range of security measures to create coordinated layers of defense. UTM typically includes a firewall, antivirus, VPN connections and other security systems designed to work in concert to counter threats. As a managed service, UTM also offers a way to simplify network operations for lean IT teams while keeping protection up to date automatically. UTM can be tailored to an agency's specific needs, fortifying a network against emerging risks and protecting constituents' data.

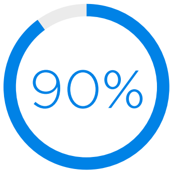
Ways UTM can protect against evolving threats

Threat	Solution
Social engineering: an attack that uses psychological tactics to manipulate people to grant access to the network, typically by opening an email attachment or link.	UTM can help avoid these psychological attacks from reaching employees by blocking them before they hit their inboxes. Web content filtering can also prevent employees from clicking through to dangerous websites.
Malware: software designed to cause damage to computers, servers or networks. It can be encrypted and deployed in a variety of ways.	With SSL/TLS deep packet inspection, UTM decrypts traffic as it attempts to enter your network. This capability can identify and prevent threats from breaching your firewall, keeping your information, employees and operations safe.
Fileless frameworks: malware that sneaks in using vulnerabilities in software and operating systems, rather than an executable file that requires action from the user. This can make them undetectable to many antivirus programs.	Vulnerabilities that require patches can be updated as part of a managed UTM service to keep devices up to date. UTM can also automatically update virus signatures and related data to keep protections current.

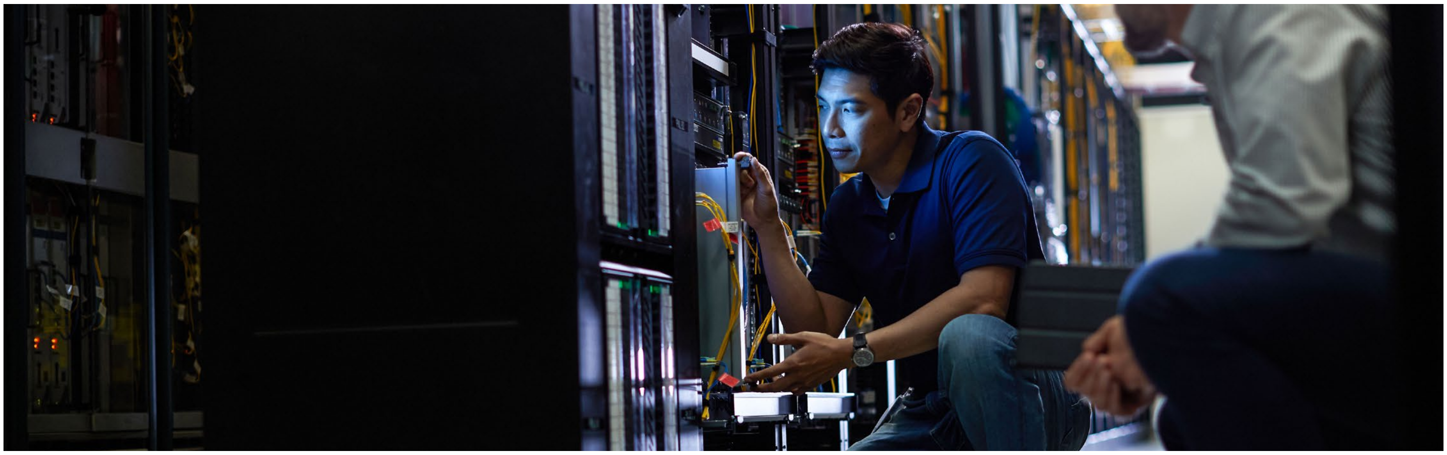
Attacks like these have the potential to expose citizens to identity theft and disrupt government operations for weeks at a time, underlining the importance of a comprehensive strategy to prevent network vulnerabilities.

1/3

of data breaches in 2020 were due to social engineering.[5]



of social engineering attacks use phishing scams.[6]



Gain the tools, support and expertise you need — all in one place

A fully managed, multilayered security solution can address multiple challenges faced by state and local government IT teams. A trusted service provider can configure and update security measures for optimal protection, providing expertise to agencies while allowing their IT teams to focus on other priorities. Adopting security measures from a single partner also reduces complexity and makes network operations easier to visualize compared to systems reliant on solutions from multiple vendors that might not be designed to work together.

What to look for in a UTM solution:

- Stateful firewall.
- IPsec VPNs to connect locations and remote users.
- Network address translation (NAT).
- Intrusion prevention system.
- Web/URL filtering categories and block listing.
- DNS protection against filtering, sinkholing and spoofing.
- SSL/TLS deep packet inspection.
- Comprehensive admin portal with logs and event tracking.
- Ongoing maintenance and always-on support.

Increasingly sophisticated cyberthreats have made the piecemeal security approach of many governments obsolete. IT leaders should consider the strength of a fully managed service that offers multi-layered protection from a single solution that is always up to date. UTM from a trusted provider offers the benefits of expert guidance, continuous monitoring and in-depth protection of government operations and data for the citizens who rely on them.

Learn more

1. Jenni Bergal, "Hackers Threaten to Release Police Records, Knock 911 Offline," Pew Research Center, May 14, 2021.
2. "2020 Deloitte-NASCIO Cybersecurity Study Highlights Imperatives for State Governments," Deloitte, Oct. 14, 2020.
3. "Studies Show Cybersecurity Skills Gap is Widening as the Cost of Breaches Rises," VentureBeat, July 28, 2021.
4. "State and Local Government Security Report," Blue Voyant, August 2020.
5. Juta Gurinaviciute, "5 Biggest Cybersecurity Threats," Security Magazine, Feb. 3, 2021.
6. Ibid.

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary. Restrictions may apply.
Subject to change without notice.