Simplifying Government Cybersecurity in a Complex Digital World

To serve citizens and conduct government business, state and local agencies need cybersecurity controls that ensure data, applications, workflow processes and other vital resources are protected and available regardless of where they exist in the enterprise environment. Doing so enhances trust in digital government, encourages adoption and helps ensure regulatory compliance. However, planning, implementing and maintaining cybersecurity is an exceedingly complex task that is exacerbated by digital transformation efforts and unexpected disruptors like the COVID-19 pandemic. To simplify cybersecurity and protect mission-critical systems and data, government organizations need a comprehensive, network-based approach that helps them securely connect, proactively monitor and effectively defend against constantly evolving threats. These capabilities are critical at any time, and an even higher priority now when organizations need to quickly deploy new digital applications to serve citizens, extend their networks to remote workers and outsmart cybercriminals who are taking advantage of vulnerable agencies.

Modern Cybersecurity: Built In, Informed, Automatic, Tailored

Used in concert, the following tactics create a holistic, multi-layered approach that allows organizations to simplify security, ignite digital transformation and remain agile in the face of disruption.

Build security into the network. With today's highly distributed network edge, it's impractical to deploy isolated solutions for each device, application, cloud environment or endpoint. Organizations need an integrated strategy that bakes security (firewalls, security gateways, encryption, etc.) into the network from the beginning. Doing so improves threat monitoring, detection and response by efficiently shifting the first line of defense closer to where data and users (and, therefore, potential threat sources) actually exist.

Use global threat intelligence and human expertise. Deep visibility into global threat intelligence, combined with human-informed analysis, empowers organizations to better understand security threats and take appropriate action. Expansive visibility

The Changing Cybersecurity Landscape

Without a network-based approach to security, the following challenges can increase an organization's risk:

Shortage of qualified cybersecurity personnel. In a Deloitte-NASCIO study, inadequate staffing was a top barrier to cybersecurity, with 30 state CISOs reporting a cybersecurity competency gap.[1] Competition for cybersecurity talent from the federal government and the private sector is an ongoing challenge.

Increasingly sophisticated threats. Even before the pandemic, threats had become more powerful and persistent. Black Lotus Labs, Lumen's threat research and operations arm, on average monitored 1.2 million unique threats daily during the first half of 2019.[2] Now, malicious actors are using social engineering, pandemic-related phishing emails and other ploys to target remote workers. The national Cybersecurity and Infrastructure Security Agency (CISA) reports an increase in COVID-19-related phishing, malware distribution, registration of new domain names and attacks against newly deployed teleworking infrastructure, and expects these threats to continue.[3]

An ever-expanding perimeter. The proliferation of distributed endpoints, IoT sensors and cloud-based applications blurs the network edge and generates a flood of data that must be protected wherever it is. Pandemic-related network changes such as the use of virtual private networks (VPNs) exacerbate vulnerabilities. At NASCIO's recent virtual conference, secure remote access of the network was panelists' top priority.[4]

Data privacy regulations. To comply with long-standing data privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA), organizations must implement appropriate controls and track compliance across endpoints, applications, users and data. Now they must also contend with the European Union's General Data Privacy Regulation (GDPR), the California Consumer Privacy Act (CCPA) and other states' emerging regulations, which give consumers more control over their information and increase pressure on organizations to protect private data wherever it is. To manage risk in this dynamic environment, organizations need to stay well-informed and adjust compliance controls and auditing to reflect changes.

requires an extensive network backbone and security operations centers (SOCs) around the world. However, machine-readable intelligence from these various sources is not enough. Skilled intelligence analysts further improve decision-making by using their experience and expertise to understand threats in the context of an organization's business requirements and unique vulnerabilities.

Orchestrate and automate security processes and controls. By proactively defending the network from threats, a security orchestration and automation response (SOAR) platform expedites threat response and mitigation. It also reduces repetitive and manual tasks so staff can focus on higher-priority or more complex threats. SOAR processes apply global threat intelligence, big data analytics and machine learning to threat data, and then automatically block threats in real time by pushing policy updates to the targeted asset. For example, if someone tries to penetrate an organization's firewall, the SOAR platform can remediate the threat within minutes instead of the hours it would traditionally take an analyst to review the threat, devise a remediation strategy and then implement it.

Partner with an expert who can tailor cybersecurity to fit evolving needs. A trusted advisor with expertise in network-based cybersecurity helps fill skill, technology and process gaps. The right partner helps an organization simplify security and minimize risk so it can better serve citizens and advance its mission. The key is working with a partner that can apply practical expertise and tailor solutions to the unique challenges of state and local government.

Simplifying from the Start

Consider the following suggestions to simplify and improve security in all phases of planning and implementation.

Fold cybersecurity enhancement into modernization projects. To maximize investments in digital transformation, incorporate cybersecurity into the overall vision and strategy. Determine what data will be delivered to constituents and employees, the value it will bring and how users will consume it. Then, use a data privacy framework to articulate how the organization will incorporate, manage and protect the data.

Consider the NIST framework. The National Institute of Standards and Technology (NIST) framework focuses on five key functions (identify, protect, detect, respond and recover) and provides guidance and best practices that help organizations understand and evaluate their risk management.

Prioritize. Using the NIST framework, compliance requirements and the organization's top risk management priorities as a starting point, identify areas where the organization is most vulnerable and which assets absolutely cannot be compromised. Address those areas first.

Leverage managed services where practical. A third party that specializes in integrating the full spectrum of network security technologies can offer access to technology, expertise and perspective that are difficult to maintain in house. Organizations using managed services report a reduction in remediation response times, false positives, compromised devices and security events that require investigation.[5]

Keeping Cybersecurity Front and Center

Cybersecurity must remain a priority even amid rapid change. A network-based, integrated approach simplifies security and data protection and helps minimize risk even when organizations must move quickly. This approach includes built-in security, global threat visibility and intelligence, orchestration and automation, and collaboration with the right technology partner. Using this approach, organizations can respond rapidly to ever-changing demands, reinforce transformation efforts and increase the public's trust in digital government.

This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Lumen.

ENDNOTES:
1. Deloitte-NASCIO Cybersecurity Study. 2018.
2. https://www.centurylink.com/business/security/black-lotus-labs.html
3. https://www.us-cert.gov/ncas/alerts/aa20-099a
4. https://govdatadownload.netapp.com/2020/05/mascio-mid-year-2020-state-cio-lessons-learned-during-pandemic/#.Xvqd4ecnblU
5. https://www.centurylink.com/asset/business/enterprise/white-paper/idg-managing-to-the-edge-the-necessity-of-network-integrated-security-white-paper.pdf

Photo provided by www.shutterstock.com

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: LUMEN®

Lumen is guided by our belief that humanity is at its best when technology advances the way we live and work. We deliver the fastest, most secure platform for applications and data to help government deliver amazing experiences. Learn more about Lumen's network, edge cloud, security and communication and collaboration solutions and our purpose to further human progress through technology at **www.lumen.com.**