National Government Services

studio 2G

OPERATION AUTOMATION

LEVERAGING EMERGING TECHNOLOGY TO PROTECT CRITICAL HEALTH DATA

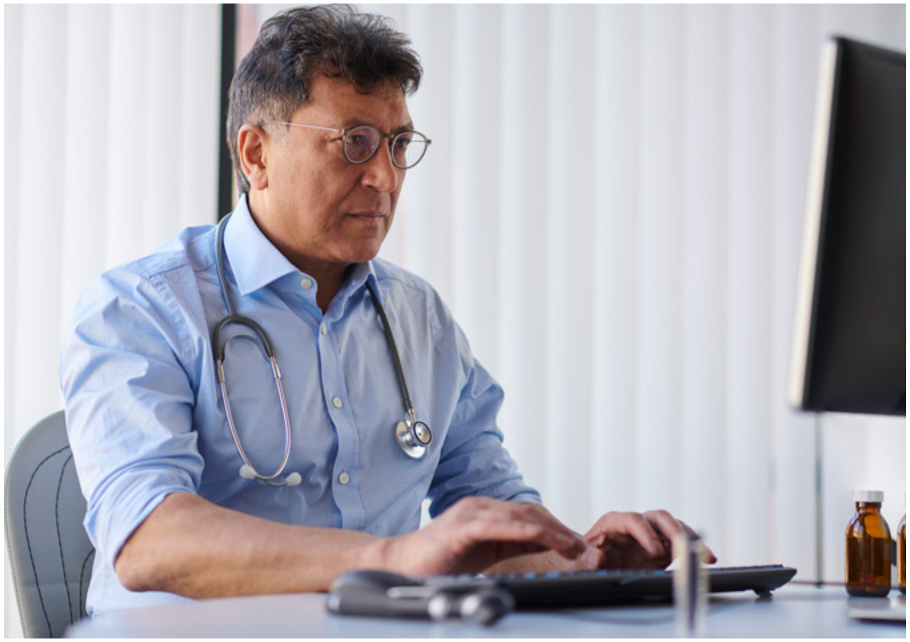
IT modernization efforts have taken center stage at today's health agencies. To drive successful health IT outcomes, federal health agencies must approach security early and often in the modernization process. Here's how.

INTRODUCTION

Today's government decision makers know that data is a strategic asset. Generally speaking, the more information workers have access to, the more impactful their decisions become.

However, data can also be a weapon of destruction. With more information comes more opportunities for cyber vulnerabilities. That's especially true in the health care sector, which has seen a spike in threat activity amid the global COVID-19 pandemic: According to an April 2021 report from **Check Point**, health care tied with utilities as the sector most targeted by ransomware threat actors. And these attacks show no signs of slowing down.

Indeed, to drive successful health IT outcomes, organizations must approach security early and often in the modernization process. Here are a few recommendations from experts across the health IT ecosystem.



PRIORITIZE INTEROPERABILITY TO IMPROVE HEALTH OPERATIONS AND RESULTS

The sheer volume of data presents a number of hurdles for the clinicians who need to access it. What's more, this data isn't always available because of legacy systems with poor user interfaces, lack of interoperability or system standardization, slowed modernization efforts and the evolving needs of health IT security. And much of this data comes from various and sometimes conflicting directions, making it difficult for health care providers to effectively treat patients.

However, these droves of information present an opportunity to revamp existing systems and processes, says Krista Yager, Chief Digital Officer at National Government Services.

"It's really about having a structured process to take any of these new data sources as they're coming in, make sure that the data is captured, it's stored, it's secured and it's … retained," Yager said.

Governance is also a key to ensuring the right people have access to data they need — and protecting this critical information from those who might abuse it.

> *"Organizations need to take steps to define processes, roles and standards around their data. That way, they can really ensure their information is kept in the hands of those who will use it appropriately."*
>
> **Jane Hite-Syed**
> *Chief Information Officer*
> National Government Services

DERIVE VALUE BY BRINGING AUTOMATION INTO THE VULNERABILITY DETECTION PROCESS

Automation can also help health IT organizations resolve incidents and vulnerabilities more quickly.

At the 2021 CMS Cybersecurity Forum, Benjamin Hostetler, senior information security advisor at National Government Services, noted that automating security control compliance can help health IT leaders save their organizations money.

“Each [automation] action calculates out to a monetary value, such as if an associate does those exact same actions,” he explained. “So . . . we can actually calculate out and give a projection on . . . the amount of time that we have saved using these automation capabilities, as well as ‘this is the dollar amount that we actually can potentially project out if we had to hire personnel to do these types of activities.’”

Implementing automation capabilities can also help staff refocus their time on more strategic tasks.

“Mean time to resolution . . . is also a great data point,” Hostetler added. “We typically look at that [in terms of] ransomware or a phishing attempt, and how long did it take the incident response group to actually resolve those?”

The data speaks for itself: Hostetler and his team tracked mean time to resolution during RA-5, a vulnerability management control from NIST-800-53. The result? Automating the vulnerability scanning process slashed mean time to resolution from an hour to a minute.

LEVERAGE AUTOMATION TO MEET TODAY'S SECURITY REQUIREMENTS

As today's threats and vulnerabilities become increasingly complex, health IT leaders are taking advantage of automated tools and expertise built to navigate modern challenges. Below are a few key capabilities that federal health agencies should look out for as they seek to protect their critical data.

Key Protective Capabilities:

1 **Identity and access management**
Protecting personal health data is a top priority for federal health agencies. Secure ID management and system access solutions can enable agencies to adhere to compliance standards and business needs, all while continuing to prioritize the user experience.

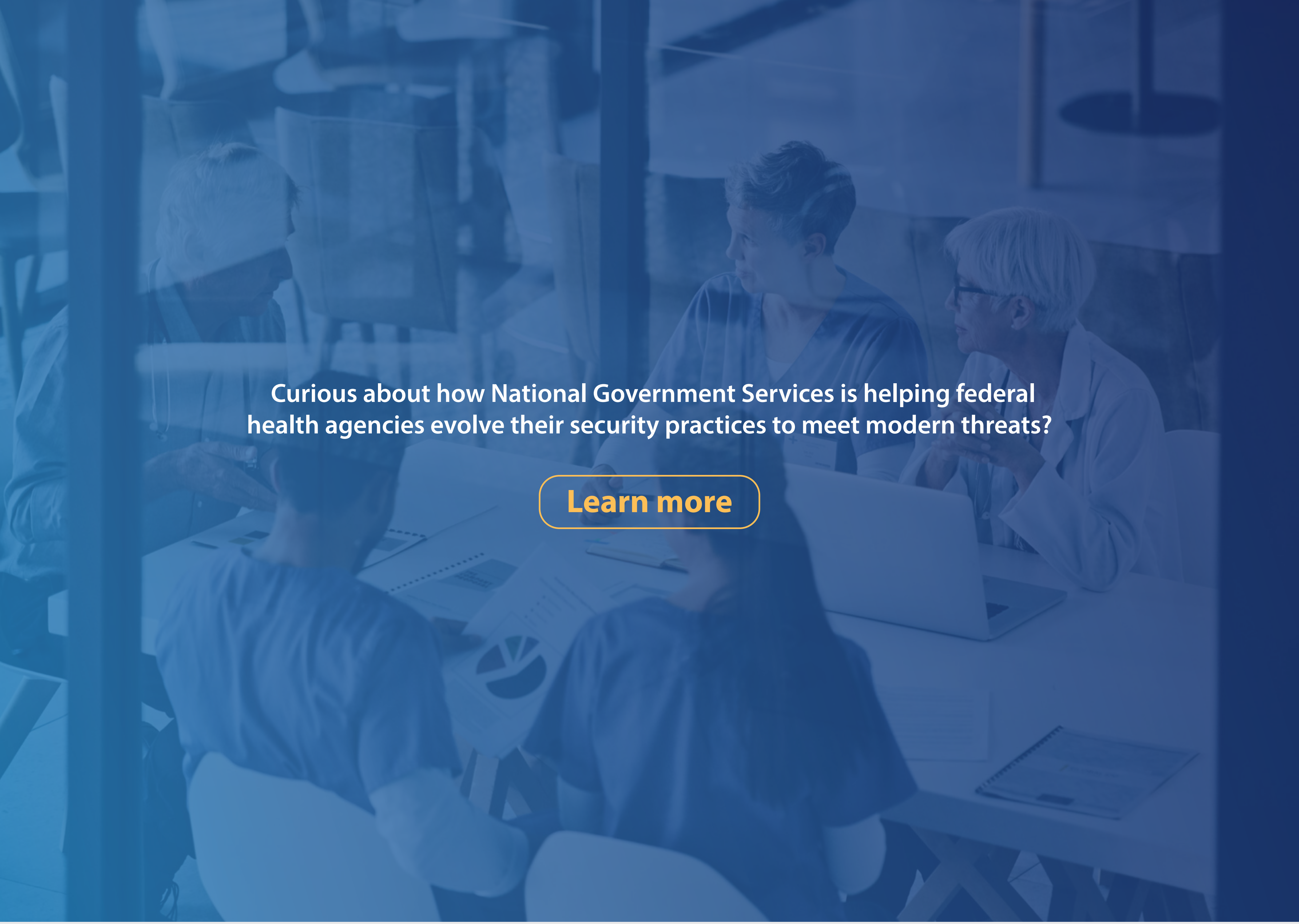
2 **Threat detection**
With increasingly sophisticated threats and vulnerabilities, health organizations require a more advanced approach to systems and data protection. Through advanced analysis, continuous monitoring and threat prevention, a proactive, outcomes-driven approach to quickly detect threats can set federal health agencies up for security success.

3 **Continuous diagnostics and mitigation**
With the scale and complexity of today's federal IT systems, finding the right mix of tools and controls presents agencies with a unique challenge. Application integrations can escalate incidents to the right people, while knowledge management repositories can help identify and monitor new cases.

4 **Strategy, risk and compliance**
Government and healthcare regulations are constantly evolving. Agencies must prepare for the future by implementing security controls that meet FISMA, NIST, CMS HIPAA, CMS ARS and IRS Pub-1075 requirements.

5 **Network penetration testing**
With proactive planning and application testing, organizations can prepare for potential threats and develop a pre-emptive strategy to detect and counter malicious activity.

6 **Infrastructure and endpoint security**
Intrusions can happen from various internal systems and endpoints. Federal health agencies are placing more emphasis on limiting the vulnerability from the technology used most by end-users, which are widely targeted for cybersecurity attacks. Antivirus protection, behavioral monitoring and code scanning can help organizations gain real-time visibility into potential incidents.



Curious about how National Government Services is helping federal health agencies evolve their security practices to meet modern threats?

Learn more