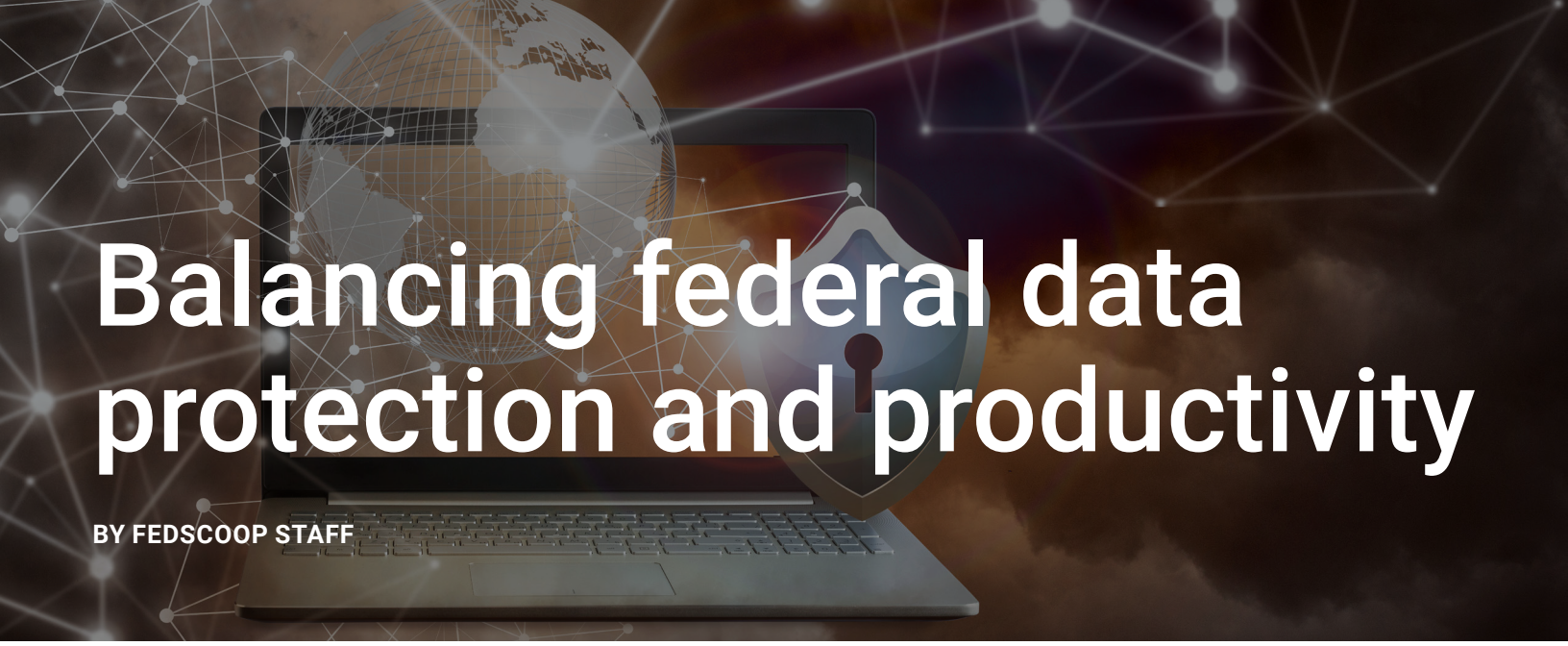

# Balancing federal data protection and productivity

BY FEDSCOOP STAFF

Federal agency CIOs and CISOs must shift how they invest in cybersecurity — focusing on protecting information, rather than systems — without sacrificing attention to the weakest part of their networks: end users operating on the endpoint.

The collision of two megatrends over the past five years is driving that need: Technology advances in mobile computing and the proliferation of cyberattacks. Mobility has the potential to make end users far more productive. However, 95 percent of all data breaches start at an endpoint because people are the weakest links in security.

The value of some data has increased astronomically over the past two decades, and more bad actors are trying to infiltrate and extract that data than ever before. For a long time, criminals focused primarily on stealing credit card information; so many credit card account numbers were stolen, the law of supply and demand kicked in and the price for each number plummeted.

## Hackers go where the value is

So hackers have moved on to stealing personally identifiable information (PII) for resale — everything from personnel to health records — and more recently to seizing enterprise data and holding it for ransom, as in the WannaCry attack earlier this year.

"The first step in any attack is getting in the front door, and we in the security industry are not doing a great job of keeping the door shut," said Brett Hansen, Vice President of Data Security Solutions at Dell.

The evolution of cybercrime is happening right before our eyes, yet we still have very porous front-end protection for endpoints, he added.

The assault on enterprise data systems is being compounded by the revolution in mobile computing as more employees are using more devices — and often their own, rather than provided by their agency or organization. This is why security at the endpoint has become even more important today. And the challenge will grow as the number of potential endpoints continues to grow exponentially.

## Rethinking endpoint security

The problem for agencies and organizations, however, is how to erect strong security controls without also hindering employee productivity. Whether it's because security slows down the network or employees have to follow more procedures, enhanced protection decreases the productivity gains mobility offers.

Educating employees about cyber hygiene can help. The challenge becomes how to align the organization's cybersecurity strategy with the business strategy and finding ways to help workers to maximize their productivity. It requires a holistic view of both your business strategies and your security posture, and

**95 percent**
of all data breaches start at an endpoint

**STRATEGY TIP:** **Scanning traffic for known malware is no longer viable, with the more than 500,000 different pieces of malware created every day. Focus on technologies that can automate endpoint security against external threats — while preserving productivity.**

designing data security procedures that align with the types of employees you are managing, the work they are doing, the types of data they need to access and the objectives of your organization.

More specifically, CIOs and their IT security teams need to know:

- Where do the different networks in the organization touch?
- How many of those networks can be reached from a given endpoint?
- Are there critical networks for sensitive information that can be reached by hacking into non-sensitive systems (e.g., automated HVAC or environmental control systems)?

When those connections are found, have a conversation with the various owners of those business units or programs. Understand why those connections are there. Do the facility or environmental systems have to be accessible from the personnel system network?

There is no one-size-fits-all security solution to this challenge, but the enterprise has to identify, understand and rationalize as many of these connections as possible.

The next step is to start exploring new endpoint security options. Companies and government agencies have spent billions of dollars on cybersecurity — the White House budgeted more than $19 billion for it in fiscal 2017. But clearly all that spending is not producing the desired results, or there wouldn't be headlines every few weeks about another major data breach.

## Bad actors — the external threat

Another factor forcing CIOs to rethink their approach to security spending is the sheer volume of malicious attacks. Scanning traffic for known malware is no longer viable, with the more than 500,000 different pieces of malware created *every day*. No matter how frequently malware references are updated, systems can't keep up.

**"The first step in any attack is getting in the front door, and we in the security industry are not doing a great job of keeping the door shut."**

**— BRETT HANSEN**
**Vice President, Data Security Solutions**
**Dell**

**STRATEGY TIP:** **Align your organization's cybersecurity strategy with management strategies — and to maximize worker productivity. Take a holistic view of the work employees are doing, the types of data they need to access and the mission of the organization.**

There are, however, promising new approaches to automating endpoint security against external threats — while preserving productivity, including:

- Sandboxing, which sequesters potentially compromised traffic to allow for closer inspection;
- Machine learning, which uses algorithms to identify characteristics — not hashes — of malware and quarantines suspicious traffic; and
- Behavioral analytics, which uses software tools to spot data transmission patterns that are out of the ordinary.

No one of these is a silver bullet. Defense-in-depth at the endpoint is still a necessity. But rethinking the entire approach to cybersecurity and improving endpoint protection with these tools can help.

## Insider threats

No amount of endpoint protection can guard against insider threats. An insider threat could be intentional; but more often than not, it could simply be negligence.

"End users want to get their job done; that's their primary motivation," Hansen said. "People focus on what they're compensated on. Very, very few people are measured on their data hygiene."

The ability to easily share information has its downside. A majority of employees would say they have some sense of responsibility for data security, but a 2017 Dell global study of business professionals found 72 percent expressed a willingness to share confidential data outside their organization. More than 50 percent use a public cloud, and nearly half access social media using organization-issued devices.

Part of the new approach to cybersecurity should include software tools and other measures to prevent employees from sending out confidential information. Enterprises, for instance, should put mechanisms in place that:

- Encrypt data, no matter which device is used to view or transport the data (e.g., via email, attachment, thumb drive)
- Define the data, so it can be controlled even outside the organization
- Guard data, for example, from being cut, copied and pasted
- Place time limits on data and document availability
- Prescribe who can use or see the data

## Put thought, not just money, into security

The proliferation of security tools, and the rising pressure to protect data, have led to a huge run-up in security spending. But it's time to spend smarter, rather than spend more, on protecting information.

Every enterprise wants the management of security to be easier. Right now, most organizations have a multitude of security tools, all of which must be kept up to date, configured properly and monitored for incidents and breaches. New options on the market, however, can consolidate and automate these tasks, and provide greater total visibility in a single console. That not only enables IT managers to coordinate control of new and existing tools, but also make faster decisions when malicious activities inevitably occur.

More importantly, as cyberthreats evolve, so will techniques to combat them. CIOs and CISOs need to have sufficient flexibility to accommodate new tools and innovations in the cybersecurity space. That's because no one company will be able to cover all the threat variations.

At the same time, agencies and organizations must also take steps to avoid being locked into a single vendor's ecosystem. That becomes an easier task when agency leaders focus on protecting information, rather than systems — and remember that the endpoint, whatever form it takes, is always the weakest link in the system.

*Visit FedScoop's special* Digital Transformation Heroes *series for more on digital transformation in the federal government.*

*This article was written and produced by* fedscoop *for, and sponsored by,* DELL EMC