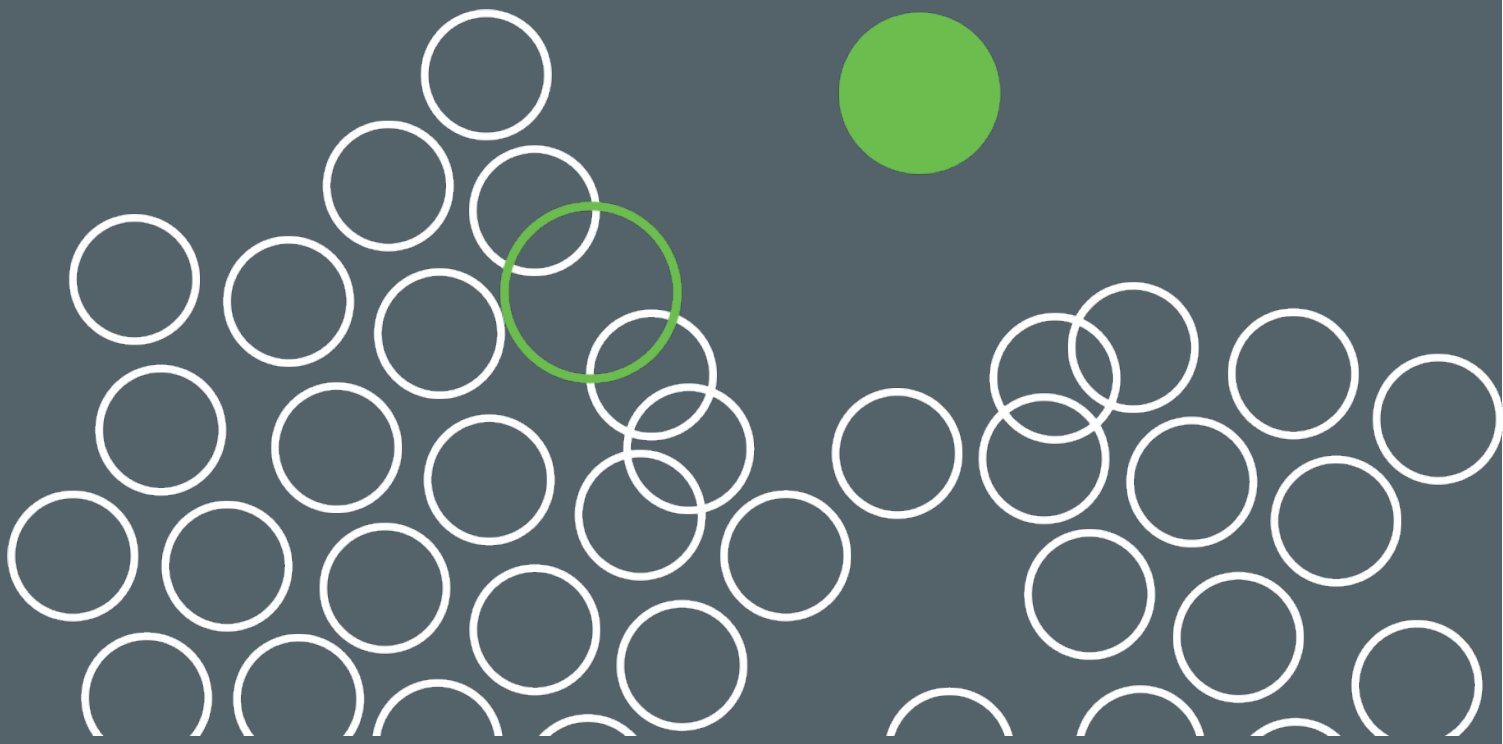
Duo Security is now part of Cisco.

How Ethical Partnerships Empower Agencies to Get Smart About Security

Federal leaders weigh in on what the Kaspersky Lab case has meant for government IT security — and what it will take for the U.S. to ensure their systems are safe and secure.



In 2017, the U.S. government made a decision that would alter how government agencies work with and vet suppliers.

After allegations that cybersecurity company Kaspersky Lab had engaged in activities with the Russian Federal Security Service — with the possibility that Kaspersky software could be used to gather sensitive and classified information from government entities — the U.S. banned all use of the company's software across the federal government.

While the case was eventually dismissed, it set the stage for important discussions about how and why the U.S. government should seek to better investigate their contractors.

Today, as the public sector continues to innovate, new tools and technologies offer agencies the opportunity to work faster and more efficiently. But if the Kaspersky Lab case has taught us anything, it's that with this innovation — and more data at our fingertips than ever before — comes risk. And for that reason partnering with ethical suppliers is critical to an organization's cybersecurity efforts, as well as our national security.

In a recent webcast from NextGov, underwritten by Duo Security, cybersecurity reporter Mariam Baksh spoke to federal leaders about what the Kaspersky Lab case has meant for government IT security and how partnering with trusted suppliers, like Duo Security, can empower agencies to keep their IT systems secure going forward. Below are a few key takeaways.

1. Set a Precedent

When it comes to securing systems against malicious actors, it's important to start off on the right foot.

"It's so important to get these things right early," said Dan Sutherland, chief counsel at the Cybersecurity and Infrastructure Security Agency, during the webinar. "Lawyers think by precedent — how have things been resolved in the past and how should we resolve them now? It really lays the groundwork for where we are."

Sutherland has been practicing law for over 30 years but says working on the Kaspersky Lab case was one of the highlights of his career. This is because professionals across all levels of government came together to ensure that potentially dangerous software was removed from public sector machines.

"[There was] amazing collaboration," he said. "We all — lawyers and others — worked together to assess the type of risk we had to take some action on. With a critical eye, we then developed an inter-agency working group that tried to develop a process for an effective decision to be made by decision-makers."

The Department of Homeland Security, he continued, issued a binding operational directive requiring agencies to identify exactly where and how they used Kaspersky's products and services while offering Kaspersky the opportunity to present its case. Elaine Duke, DHS's acting secretary at the time, ultimately decided that the U.S. government should proceed with the removal of all Kaspersky products and services. With CISA's help, the justice department defended the decision in federal district court and the court of appeals — and won both cases.

Sutherland said that moving forward, the Kaspersky case will serve as an important model for how the U.S. government should confront similar challenges. The hope is that the case will empower public sector IT leaders to look for trusted suppliers to work with, who can offer high-level threat protection.

2. Proactively Mitigate Threats

Indeed, the case has already had several knock-on effects. In 2018, the U.S. government decided to take additional measures and President Trump signed into law the SECURE Technology Act, which aims to mitigate supply chain threats to the U.S. government.

"We wanted a more systemic solution to this problem," Federal Chief Information Security Officer at the Office of Management and Budget Grant Schneider said during the webcast. "We wanted to be able to look at what the impacts are from an enterprise perspective."

Schneider, who worked with Congress to pass the bill, said that the act offers a risk-based solution to supply chain threats. "We believe that through the SECURE Technology Act, we'll be able to leverage and protect classified information," he added.

But threats are constantly evolving, and thus guidelines need to evolve with them. To account for this, the law also established the Federal Acquisition Security Council (FASC), a working group composed of members from DHS, the Department of Defense, General Services Administration, Office of the Director of National Intelligence, Federal

Bureau of Investigation, OMB and the National Institute of Standards and Technology. The group aims to increase information sharing within the federal government and establish criteria for the types of products that may pose security risks.

Today, the council is working on an interim final rule, which will lay out the processes and procedures it will use to conduct evaluations and assessments. Ultimately, through collaboration, federal entities can continue to stay one step ahead of threats and adjust accordingly when new vulnerabilities arise.

But many agencies haven't yet done the work to make that happen. In fact, a 2019 report from DoD's Inspector General found that many organizations are relying on contractor-owned systems that haven't put even basic cybersecurity measures in place, like implementing multi-factor authentication and requiring the use of strong passwords. Duo Security is one vendor that can help agencies and their contractors follow basic cybersecurity best practices.

"Authentication is basic hygiene," Duo Security Chief Information Security Officer Sean Frazier said in a recent Duo Security report. "If you have an account, if it's Level 1, and you have access to a login account and it's not [multi-factor authentication], that's malpractice. That should be a Level 1 process."

3. Develop a Comprehensive Framework for Supply Chain Security

Knowing how to identify a contractor that poses a threat is one thing — preventing it is another. That's why earlier this year, the Department of Defense released the Cybersecurity Maturity Model Certification, which serves as the gold standard for security implementation across the defense industrial base.

"The whole rationale is protecting the network which our data would be riding on," said Stacy Bostjanick, director of Cybersecurity Maturity Model Certification, Office of the Under Secretary of Defense for Acquisition & Sustainment. "The model gives requirements for processes and procedures that must be followed to secure networks in order to handle covered, unclassified information. This puts companies on notice that they have to meet these standards."

The CMMC also requires a third-party to assess contractor compliance with these practices and procedures. Going forward, every government contractor will need to complete this certification so that DoD can maintain quality assurance on all of its tools and technologies.

"The concept of having walls around our data has really gone away," said Frazier. "Adopting a zero-trust security model while leveraging CMMC can guide agencies and their partners into a better security lifecycle. They reduce the threat surface down to the data."

Frazier and his team have worked with government organizations and contractors to implement tools to help meet CMMC's requirements. Duo Security's controls map to several CMMC domains, for example, including access control, audit and accountability, configuration management, identity and authentication, and maintenance.

After the Kaspersky trials, CISA also came up with a holistic approach to determining issues and threats. The framework looks to assess the functions the product or service performs, the software it has access to and the laws the vendor operates under, among other questions.

"The concept of having walls around our data has really gone away. Adopting a zero-trust security model while leveraging CMMC can guide agencies and their partners into a better security lifecycle. They reduce the threat surface down to the data."

– Sean Frazier, CISO at Duo Security

These guidelines, along with the CMMC, will help establish liability in future public-private partnerships. As more government organizations move toward a shared services model and agencies continue to rely on ethical partners and vendors to drive solutions, it has become increasingly important for all parties involved to understand their roles — and any risks they bring with them.

To learn more about Duo Security's offerings, including CMMC resources, check out: duo.com/gov.