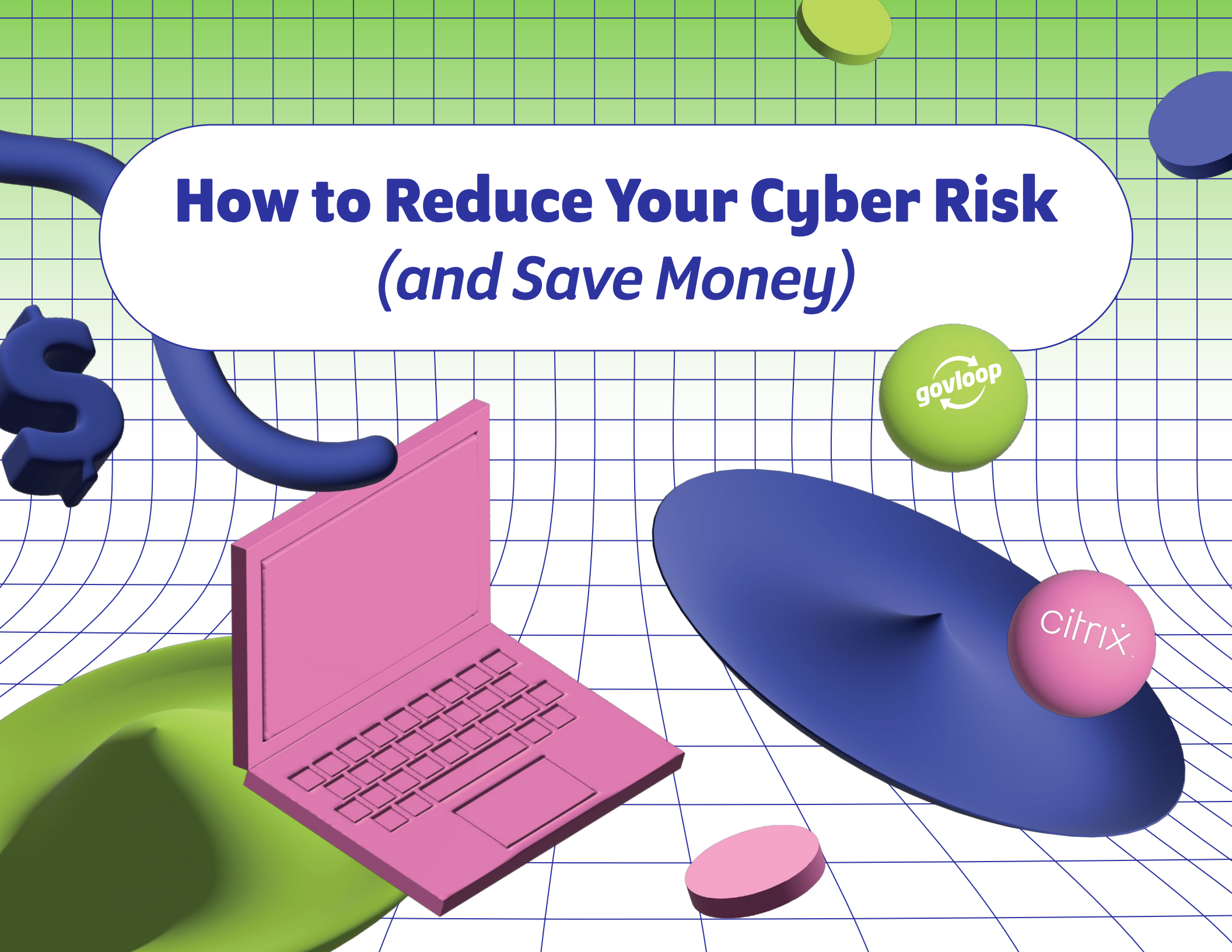
How to Reduce Your Cyber Risk *(and Save Money)*



Introduction

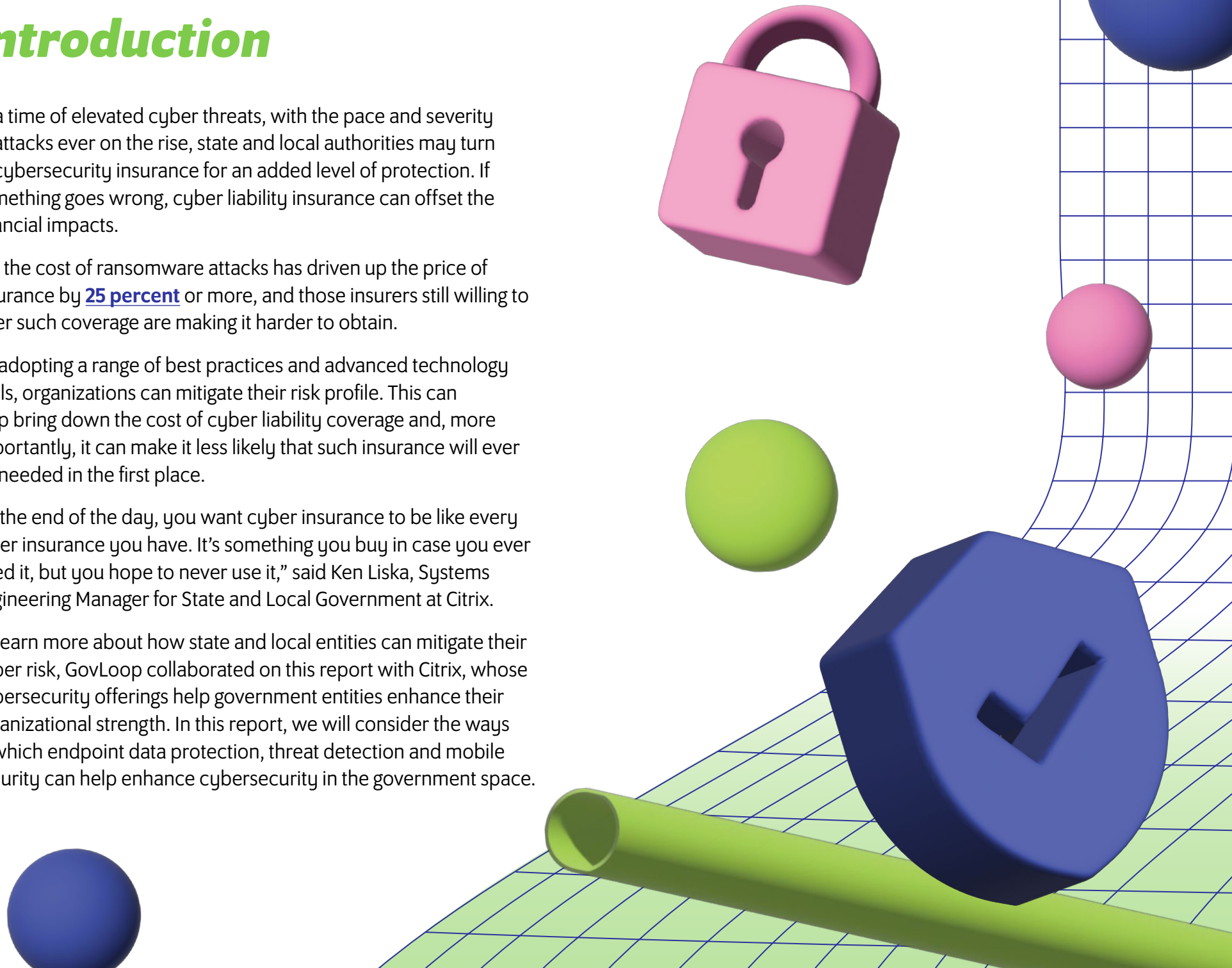
At a time of elevated cyber threats, with the pace and severity of attacks ever on the rise, state and local authorities may turn to cybersecurity insurance for an added level of protection. If something goes wrong, cyber liability insurance can offset the financial impacts.

But the cost of ransomware attacks has driven up the price of insurance by **25 percent** or more, and those insurers still willing to offer such coverage are making it harder to obtain.

By adopting a range of best practices and advanced technology tools, organizations can mitigate their risk profile. This can help bring down the cost of cyber liability coverage and, more importantly, it can make it less likely that such insurance will ever be needed in the first place.

"At the end of the day, you want cyber insurance to be like every other insurance you have. It's something you buy in case you ever need it, but you hope to never use it," said Ken Liska, Systems Engineering Manager for State and Local Government at Citrix.

To learn more about how state and local entities can mitigate their cyber risk, GovLoop collaborated on this report with Citrix, whose cybersecurity offerings help government entities enhance their organizational strength. In this report, we will consider the ways in which endpoint data protection, threat detection and mobile security can help enhance cybersecurity in the government space.



Need to Know

Cyber Liability Insurance at a Glance

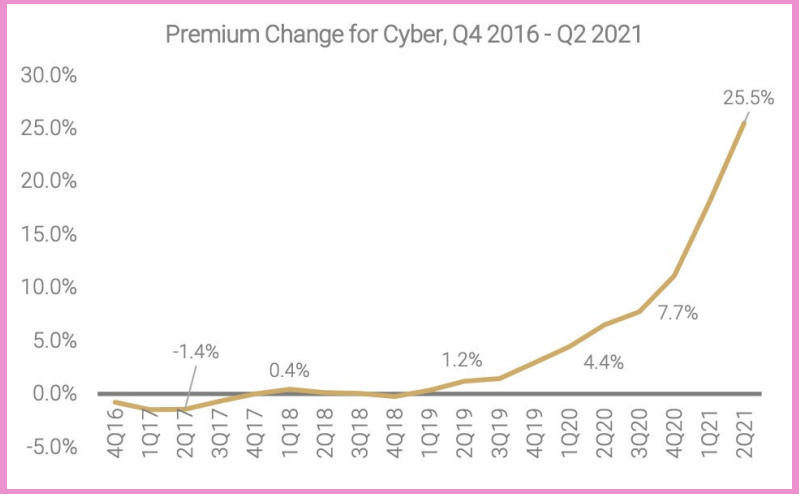
For state and local authorities, a cyberattack can be costly — not just in terms of operational capability or data loss, but also hard dollars. "Even mundane security breaches — a misplaced laptop storing confidential data — can trigger costly response procedures," according to the National Governors Association (NGA). "States can offset the cost of a breach by purchasing cyber liability insurance."

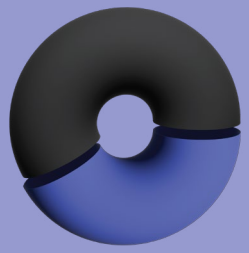
Cyber insurance can help pay for things like customer notification and credit- and identity-theft monitoring. It can offset the expense of litigation and regulatory fines. But it isn't a cure-all. There's typically a labor-intensive application process, and there are loopholes for insurers, which, for example, may not have to pay in the case of a nation-state attack.

The best way to purchase and utilize such coverage is in conjunction with a vigorous risk-reduction effort. "Cyber liability insurance is one component of a holistic risk management strategy; it is not a substitute for a robust information security program," according to NGA.

By the Numbers

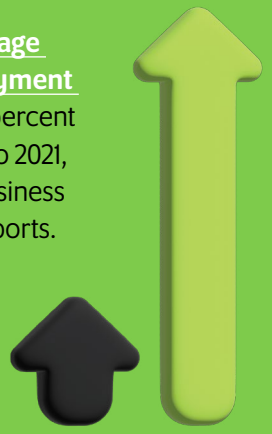
The average premium for cyber insurance coverage increased 25.5% during the second quarter of 2021, according to a survey from the Council of Insurance Agents & Brokers (CIAB).





In a recent survey, 40 percent of central government agencies said they had experienced a ransomware attack.

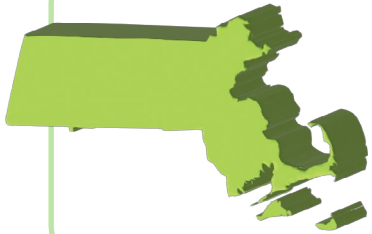
The average ransom payment shot up 82 percent from 2020 to 2021, Harvard Business Review reports.



In the News: The Growing Threat Landscape



A ransomware attack impacted the police department in **Bristol, Virginia**, in 2021, with cybercriminals taking control of departmental computers and accessing classified data, which was later sold on the dark web.



A Labor Day ransomware attack impacted the servers of the **Cape Cod Regional Transit Authority**. Though services were largely uninterrupted, the attack suggests no government agency is immune.



Evidence was destroyed at the **Atlanta Police Department** when five of the city's 13 departments were impacted by a ransomware attack in 2018.



In **Tenafly, New Jersey**, a ransomware event took out the school district's computer system and forced schools to cancel final exams.



An attack on the municipal government in **Ellsworth, Kansas**, caused the city to take down its systems and limit some internal operations.

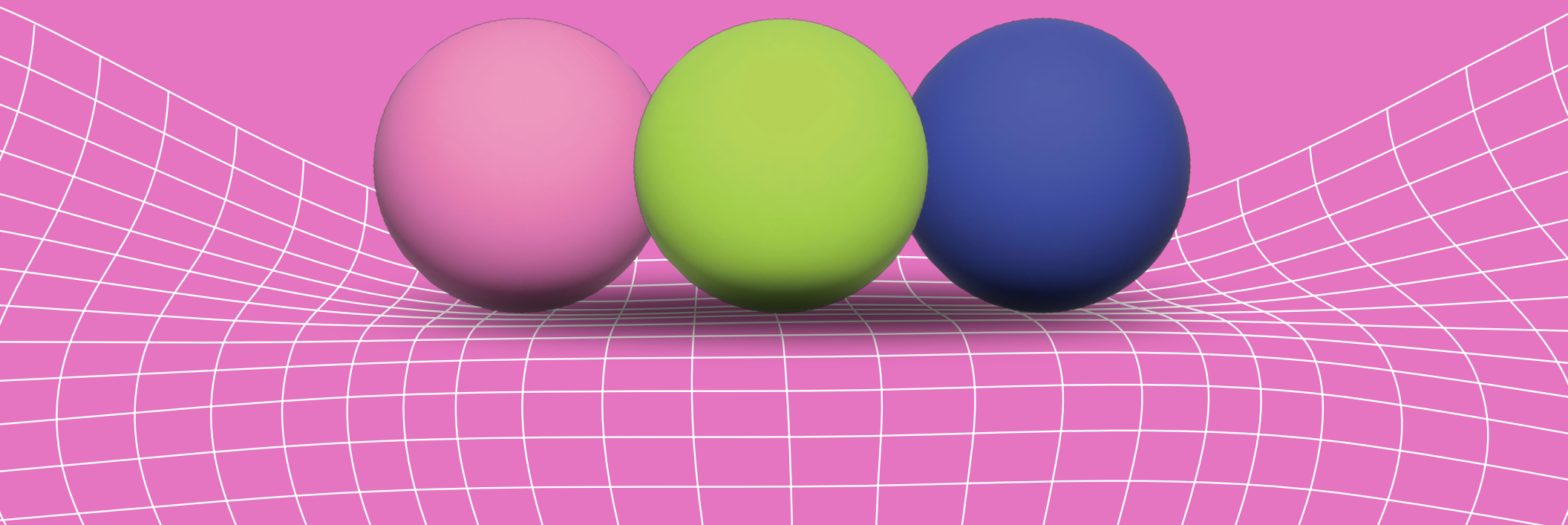


Digital documents became inaccessible and online city services were down for weeks after the **city of Baltimore** fell victim to a ransomware attack in 2019.

3 Tools for Reducing Your Cyber Risk

To reduce the cost of cyber insurance and strengthen defenses overall, state and local authorities need to focus on risk mitigation. Robust cyber protections can help inoculate an agency against attack, empowering administrators to effectively safeguard both operational systems and sensitive data.

To that end, they need to be sure they are addressing three key elements of cyber defense. They need to have in place endpoint data protection; a mechanism for timely threat detection; and tools in support of mobile security.



1

Endpoint Data Protection

Endpoint data protection encompasses a widening range of risks. It addresses, for example, the vulnerabilities that come with increasing Internet of Things (IoT) deployments. It may also encompass end-user devices, whether owned by the business or the employee.

"If your users leave the building, or even if they're in the building, you need to protect them from everything that's out there on the internet," Liska said. In general, admins need to ensure that users are not downloading viruses or otherwise opening the door to ransomware or malware. "You want to make sure you're protecting that device from malicious websites," Liska said.

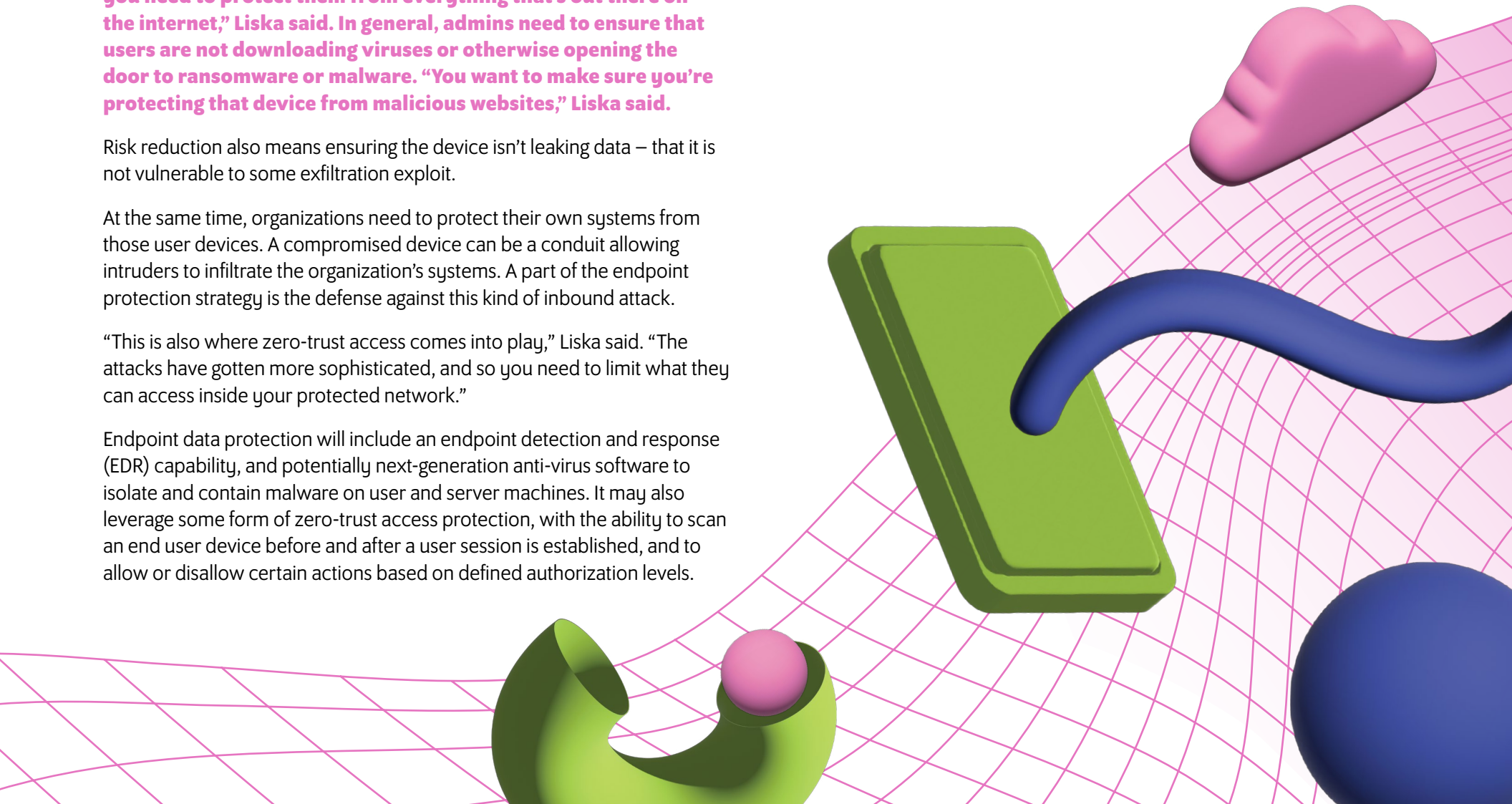
Risk reduction also means ensuring the device isn't leaking data – that it is not vulnerable to some exfiltration exploit.

At the same time, organizations need to protect their own systems from those user devices. A compromised device can be a conduit allowing intruders to infiltrate the organization's systems. A part of the endpoint protection strategy is the defense against this kind of inbound attack.

"This is also where zero-trust access comes into play," Liska said. "The attacks have gotten more sophisticated, and so you need to limit what they can access inside your protected network."

Endpoint data protection will include an endpoint detection and response (EDR) capability, and potentially next-generation anti-virus software to isolate and contain malware on user and server machines. It may also leverage some form of zero-trust access protection, with the ability to scan an end user device before and after a user session is established, and to allow or disallow certain actions based on defined authorization levels.

Agencies may also leverage mobile device management, or MDM, as a way to further strengthen their defenses and reduce the risk associated with the ever-expanding range of network-connected endpoints. A cloud access security broker (CASB) can help as well. As a cloud-based security policy enforcement point, "that helps protects the user from the evil internet," Liska said.



2

Threat Detection

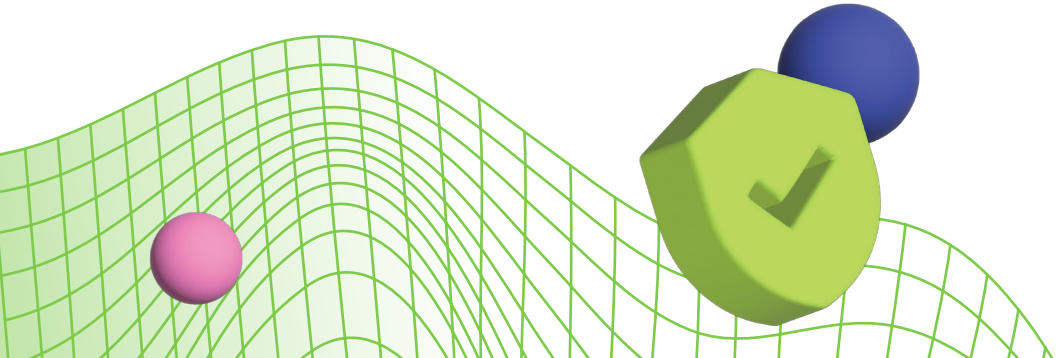
Threat detection refers broadly to the ability to notice and act upon unusual behaviors in the network. Doing this in a timely fashion is key to risk reduction: The longer bad actors can linger inside the network undetected, the more damage they are likely to do.

Security information and event management (SIEM) is a key capability here. In support of that detection capability, IT leaders can and should leverage advanced analytics tools. "You need some form of security analytics to monitor your connections and give you real-time insights that are actionable, opposed to just logging," Liska said.

While traditional IT environments typically will run some form of an analytics engine, many still require human intervention. "Somebody still has to know a problem existed, so that they can go back through logs and see what happened," Liska said.

A modernized solution, on the other hand, will make use of machine learning and analytics based on artificial intelligence (AI). With advanced analytics, "you will know what attacks have been attempted, what might be occurring, what might have snuck through the armor of your environment," he said.

Advanced analytics also makes it possible to automate security enforcement when aberrant user behavior or other anomalies are detected in the system. This approach will help reduce risk by alleviating much of the manual work for IT, while at the same time providing timely enforcement and lowering the likelihood of unauthorized breaches.



3

Mobile Security

Mobile security is increasingly an important piece of the overall risk-reduction effort. State and local governments make extensive use of mobility, whether by empowering field inspectors to connect via mobile devices, or supporting office employees with work-related apps to help them be productive from any location.

A number of technologies rise to the fore in support of robust mobile security, most notably MDM, as noted earlier, and mobile application management (MAM).

MAM is especially helpful to organizations utilizing a "bring your own device" approach, in which personnel make use of their own smartphones, for example, to access workplace applications. In this scenario, it's important to have insight into what's happening on those devices, as well as some level of control.

"MAM doesn't give your organization full rights over the device: You can't delete the device or search everything on it," Liska said. "Instead, it creates 'containers' on that device that allow your organization to deliver just what it needs to, in order to protect that device or those connected applications."

For agency-owned devices, MDM offers a higher level of control. "With this, the organization can actually control what can be installed on the device. They can find the device, they can wipe the device," Liska said.

Agencies also need to think about governance, ensuring that mobile-device users can access needed resources on the network without having to jump through too many security hoops. "You don't want to set up a scenario where a user thinks they can do all the work they need to do, but then they bring a mobile device on a trip and find they can't log in," Liska said.

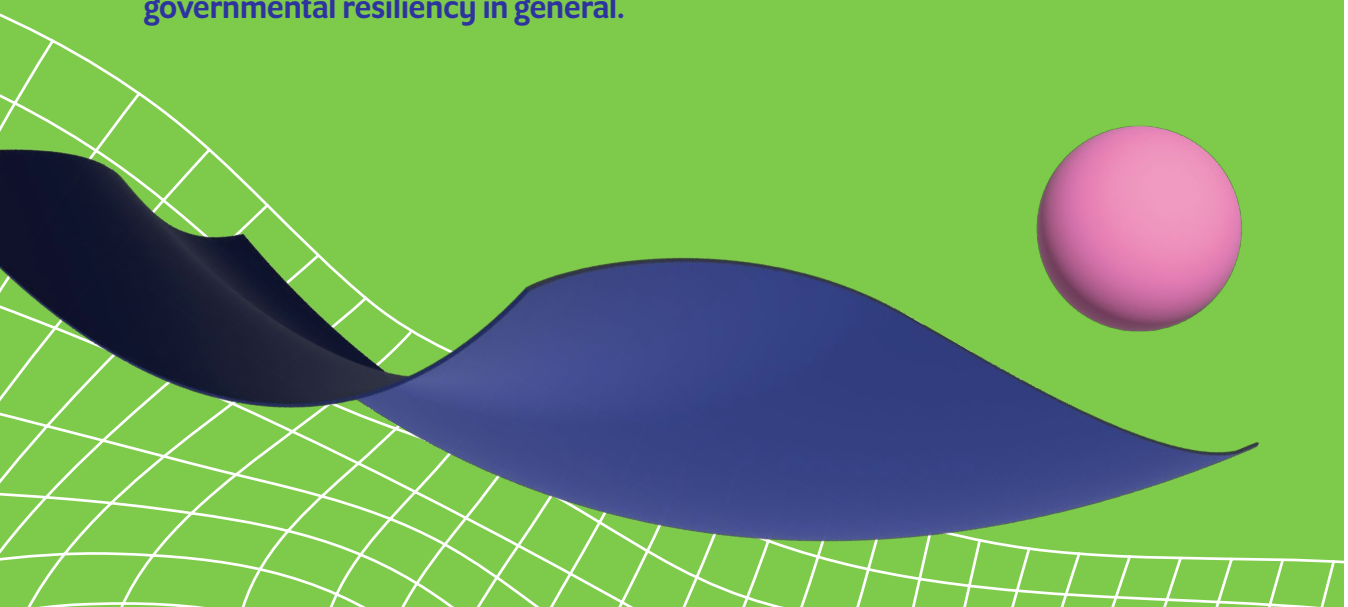
As a rule, this consideration applies across all defensive strategies. As agencies look to minimize cyber risk, they need to ensure their protections are not so rigorous or so onerous that they interfere with people's ability to get their work done.

How Maricopa County Is Elevating Cyber

An interview with Lester Godsey, Chief Information Security Officer, Maricopa County, Arizona

A few years back, IT leaders hoped that cyber insurance would help them sleep soundly at night. That is less often the case these days. In just the past few years, "our premium amounts have over doubled and our coverage amounts have been reduced by half, if not slightly more," said Lester Godsey of Maricopa County.

Maricopa is the fourth-largest county in the United States, and the fastest-growing county in the nation. Godsey gives a lot of thought to reducing cyber risk, both as a way to cope with the diminishing power of cyber insurance, and as a means to build greater governmental resiliency in general.



Emerging Challenges

A number of factors have come together lately to bring cyber to the fore in Maricopa County.

First, the 2020 presidential election placed the county at the center of an aggressive disinformation effort. As a result, "we've been implementing 'deception networking technology' and other tools to combat potential threats," Godsey said.

Then came COVID and the rapid push to cloud-based solutions. "We've had to make sure that our security controls and processes could ensure we had a minimally acceptable level of service, now that a majority of our services are going to the cloud, as opposed to being on premises," he said.

In the face of these emerging challenges, and tasked with defending county systems against an ever-evolving threat landscape, Godsey has taken a number of steps toward greater cyber resilience.

A Layered Defense

Maricopa County has deployed a range of proactive and reactive services. Godsey looks to align his efforts with the NIST Cybersecurity Framework, a set of standards and best practices designed to help organizations manage their cybersecurity risks.

The county has implemented endpoint protections and threat detection solutions, along with vulnerability scanning and security monitoring, both through its security operations

center and via a third-party managed detection and response service, or MDR, that provides 24/7 coverage.

"Our strategy is to take a layered defensive approach. We look at security controls on the edge. Email security still plays an important role. We look at data security, at endpoint protection: All of that combined constitutes our approach to cybersecurity," Godsey said. "An attack is inevitably going to come in that may bypass one or two or three of our security controls. A layered approach is our best strategy in trying to reduce the likelihood of an attack being successful."

An Enterprise Perspective

A big part of the cyber effort in Maricopa County comes down to Godsey's team working to get diverse governmental entities rowing in the same direction.

"We have a total of 56 different departments, and in eight of those the individuals who head up those departments are elected as opposed to appointed by the Board of Supervisors. That means they basically have the autonomy to do what they want, adopt what security controls, adopt whatever security framework they want," Godsey said.

From the CISO seat, Godsey works to ensure a common baseline in cyber.

"My objective is to try to leverage information security governance," he said. "Whether the departments adopt our services and controls and frameworks, or have their own in place, we should still have a universal approach – a minimally acceptable level of security controls in place, such that it reduces our overall risk to an acceptable level."

To that end, Godsey has developed a cyber strategy that gets updated twice a year to keep pace with the evolving threat landscape. He also works in close collaboration with others in county government, including the risk management department and the internal audit department, to ensure he's got a comprehensive organizational view.

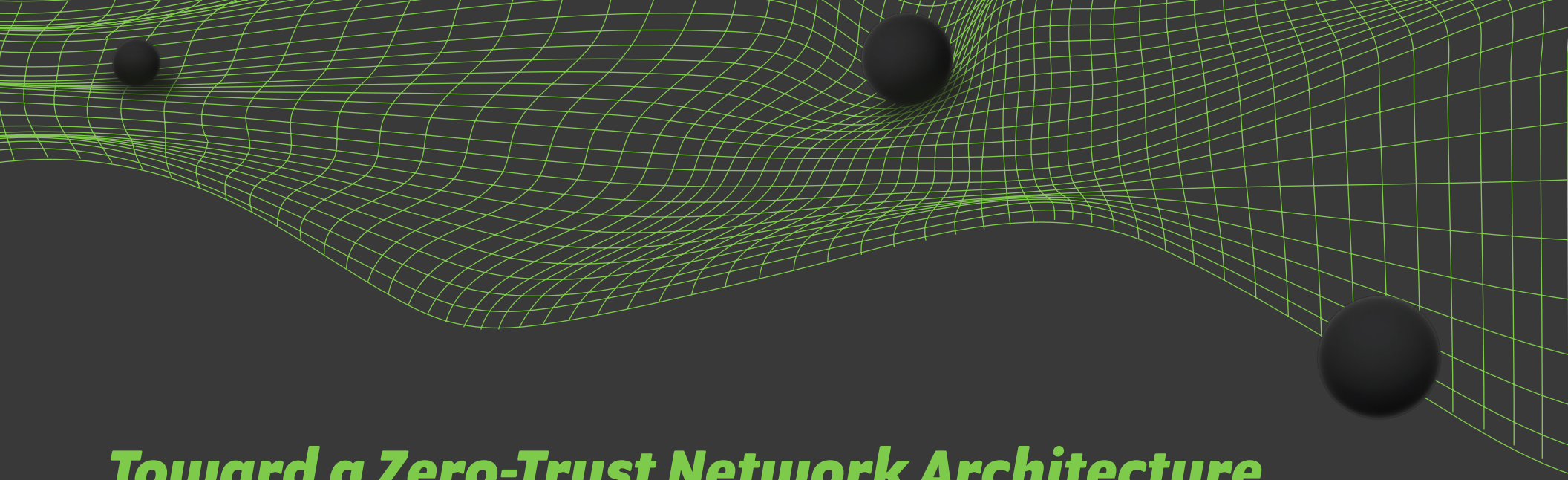
With cyber, risk management and audit professionals all at the table together, "we are able to provide a more holistic picture of risk," he said.

He also pulls together a scorecard on cyber protections from across county government to help elevate best practices and keep efforts coordinated. "It lists out all the departments, what controls they're using, whether my team is providing security services for that particular control set or if they've opted to go with their own," Godsey said.

That level of visibility helps ensure a comprehensive set of protections. "If there are gaps that need to be addressed, we come up with a game plan on how we are going to raise that bar together," he said.

"An attack is inevitably going to come in that may bypass one or two or three of our security controls. A layered approach is our best strategy in trying to reduce the likelihood of an attack being successful."





Toward a Zero-Trust Network Architecture

An interview with Ken Liska, Systems Engineering Manager for State and Local Government, Citrix

State and local agencies increasingly are turning to a zero trust-based approach to security, in which the identity and permission levels of users are verified every time they attempt to access applications, data or other resources on the network. But what does that mean in practice?

Here Ken Liska of Citrix talks about the ways in which a zero-trust network architecture can help reduce risk by preventing or limiting damage from ransomware attacks and other exploits.

How should agencies build zero trust into their cyber defenses?

It starts with having a secure enterprise browser. A lot of vendors will use a service to intercept a webpage and reroute your browser. At Citrix, we instead include an enterprise browser in our suite: That's just part of the package.

That gives the organization a known browser. They know what plugins are installed in it. They know what policies are put onto it. They know what's going to happen to the cache files when they're deleted. It's a more effective way of using your browser to get zero trust.

What are some other technologies that help create this architecture?

You want to think about having a web-app firewall, and also bot protection. A lot of attacks try to infiltrate a website through the allowed methods: Someone sends a query to the database and that then gives them access to the network. A web-app firewall protects against that. Bot protection prevents bots from interacting on and in your network. These are tools that look at the network activity, and if that activity matches what looks like a bot, this will try and stop it.

And how do analytics factor in?

An analytics solution based on AI or machine learning can learn the behaviors of different users and groups, assign them risk scores, create a risk timeline and act for you or alert when something's out of the ordinary. Just having data is not enough: You want the system to alert you not just to obvious malicious activity, but also to anomalous events.

A compromise will often start as what looks like normal activity — a logon or a file transfer, for example. Being able to notice a logon out of the normal business hours, and a file transfer significantly larger than usual, are two data points that a robust analytics solution can combine to note an elevated risk. This allows action to be taken while something is happening, before it becomes a major problem.

What are best practices for utilizing these tools?

Include security planning from the start, and focus on providing a quality, consistent user experience. Every time a user needs to learn a new system or remember how to make a connection, it introduces a loss in productivity and may lead to them working around the security systems in place.

The user experience when connecting through a virtual desktop infrastructure (VDI) or desktop as a service (DaaS), for example, should use the same tools and processes for a user utilizing zero-trust access. That's the approach Citrix takes, by leveraging the same Citrix Workspace user experience for all connections, across all devices. You can mix and match the best delivery method for the use case, without having to give the user a different entry point.

What's the best strategy for finding a technology partner in this effort?

You want a partner who can do everything you need to do. Most organizations aren't going to be able to go 100 percent zero trust, nor will they go 100% VDI or desktop as a service. You want to find a vendor who can give you a complete range of options, who can give you zero trust and a DaaS environment in the same solution. That's something that differentiates Citrix.



citrix®

ZTNA solutions to secure access to all corporate applications

Secure access to every app, on any device, with a zero trust framework

Network and application security has gotten complicated. Citrix solutions make it simple. By delivering zero trust network access (ZTNA) to all your corporate apps, you can help your remote workforce stay productive from anywhere — without exposing your network to threats or your apps to the internet.

Deliver zero trust network access to all corporate apps including web, SaaS, and DaaS.
Explore Citrix Secure Private Access

Protect access to virtualized apps with built-in desktop as a service (DaaS) cybersecurity policies.
Explore Citrix Daas

Take an interactive tour



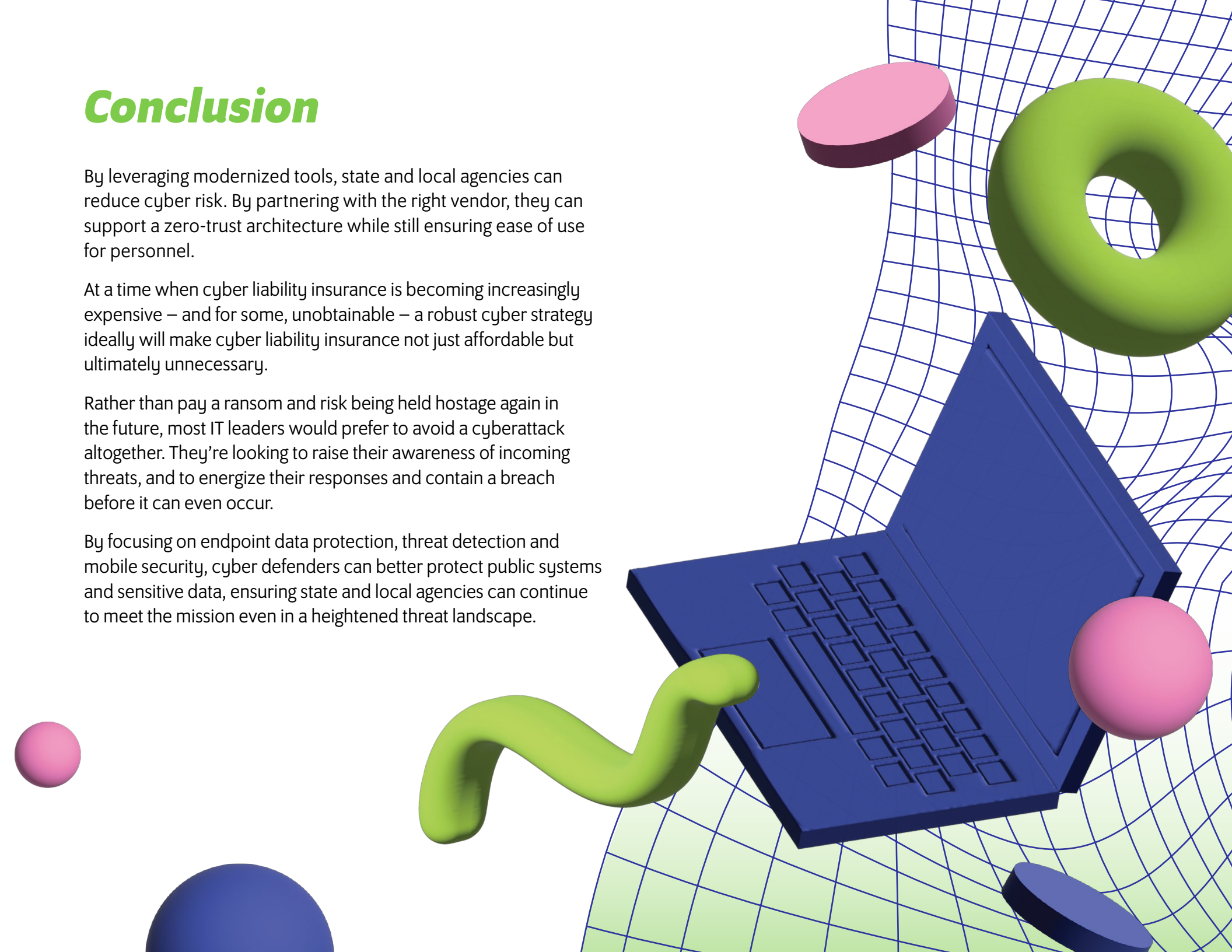
Conclusion

By leveraging modernized tools, state and local agencies can reduce cyber risk. By partnering with the right vendor, they can support a zero-trust architecture while still ensuring ease of use for personnel.

At a time when cyber liability insurance is becoming increasingly expensive – and for some, unobtainable – a robust cyber strategy ideally will make cyber liability insurance not just affordable but ultimately unnecessary.

Rather than pay a ransom and risk being held hostage again in the future, most IT leaders would prefer to avoid a cyberattack altogether. They're looking to raise their awareness of incoming threats, and to energize their responses and contain a breach before it can even occur.

By focusing on endpoint data protection, threat detection and mobile security, cyber defenders can better protect public systems and sensitive data, ensuring state and local agencies can continue to meet the mission even in a heightened threat landscape.



Thank you to Citrix for their support of this valuable resource for public sector professionals.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to **info@govloop.com**.
www.govloop.com | **@GovLoop**

