Lookout

EBOOK

Embracing Zero Trust:

A Guide for Agencies to Address the Cybersecurity Executive Order

Table of Contents

Chapter One:
How We Got Here

The COVID-19 pandemic upended how Americans work, disrupting the typical in-office environment and creating uncertainty about how to move forward. By December 2020, 71% of Americans were working from home — as opposed to the 20% doing so pre-pandemic, according to a Pew Research report.

Organizations across sectors had to quickly adapt, evolve and transform IT processes to meet employees where they and their devices were: at home. Stronger security requirements, new collaboration tools and a shift in enterprise cybersecurity culture has rapidly changed how business is done — all while the cyber threatscape continues to evolve just as fast.

Stretching Security Through VPNs

The sudden move away from offices amid pandemic shutdowns pushed organizations to rapidly transition to remote work, sometimes overnight and unprepared. The adoption of virtual private networks, or VPNs, soared to an all-time high of 27%, and in the U.S. alone, the VPN market is an estimated $12.1 billion, according to the "Global Virtual Private Network Market Report 2020."

Definition: A VPN, or virtual private network, allows organizations to extend a private network across a public network so users can send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Organizations added VPN capacity to extend their perimeter-based security over the networks their employees are using. But with the lack of visibility into the risks tied to the networks and devices used by teleworkers, VPN adds considerable risk into the organization's infrastructure.

71%

of Americans were working from home by December 2020

"Most security infrastructure still assumes that everyone is connected to the corporate network and under the protection of perimeter-based security," says Lookout Senior Manager of Security Solutions Hank Schless. "This is why virtual private network (VPN) was one of the first investment increases when everyone shifted to remote work."

VPNs, however, don't account for the smartphones and tablets used by two-thirds of employees. These devices can connect directly to software-as-a-service, or SaaS, applications and data in the cloud. But mobile devices are especially prone to phishing attacks that steal credentials or deliver malware. This means VPN becomes an entry point by which a bad actor could compromise a device and enter an organization's infrastructure.

Definition: A phishing attack is a type of social engineering where an attacker sends a fraud message intended to trick a person into disclosing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure.

Ensuring their infrastructure and data is secure in a remote-first environment requires organizations to move past legacy VPN technology, and into security architectures that don't rely on perimeter-based solutions. The pandemic may have driven organizations to leverage VPN, but it also shed light on the need to rethink cybersecurity to safeguard enterprise networks in a telework-driven world.

Accelerating Cloud Capabilities — while Continuously Assessing Risk

There's no doubt cloud use is growing, especially for infrastructure-as-a-service, or IaaS, and SaaS platforms — and that trend will likely continue to grow.

IaaS services enable a flexible cloud model, providing virtualized computer resources over the internet. In an IaaS, resources are available as services and the infrastructure includes network, storage, servers and operating systems. Organizations accelerated cloud enablement of on-premise applications by implementing IaaS into their environments.

But the continued adoption of IaaS and SaaS don't come without risk.

With these services easily accessible via the internet, users no longer have to connect to perimeter-based security. This means agencies won't have the visibility they need into endpoints, users or networks and the ways they interact with apps and data. As chief information officers continue to grow their interest in cloud platforms and more emerging technologies, such as containerization, virtualization and edge computing, agencies will need to ensure they're not giving way to cloud sprawl and are adopting security solutions necessary to keep agency data and networks secure.

The Employee of Today

The pandemic impelled a work-from-home wave shifting to a hybrid-remote environment as restrictions loosen and offices reopen. The private sector may have been more familiar with and prepared for the fact that employees are working from anywhere and using any device, but the federal government had to reconfigure processes and technology to adapt — and they're here to stay.

The White House released return-to-work guidelines supporting flexible and remote work environments, including facilitating hybrid and telework where appropriate.

"Many employees — more than prior to the pandemic — will engage in a mix of telework and onsite work," according to the memo. "Employees who have been teleworking during the pandemic generally will remain eligible for telework, at least on a situational basis."

Yet safety remains top of mind in all sectors as personnel engage with enterprise networks from home, using various devices and through unsanctioned applications. In fact, the Lookout 2020 "Mobile Phishing Spotlight Report" found a 37% increase globally in the enterprise mobile phishing encounter rate between the fourth quarter of 2019 and the first quarter of 2020. In response, government and industry are working together to welcome a new, safe future of hybrid work.

i

37%

global increase in the enterprise mobiile phishing encounter rate between the fourth quarter of 2019 and the first quarter of 2020

Chapter 2:
Executive Order Calls to Action

As the pandemic fueled a remote workforce, it also broadened the cyberattack surface — upping risk to critical infrastructure and citizens' day-to-day lives. Major cyberattacks like SolarWinds, Microsoft Exchange and Colonial Pipeline are driving the federal government to make impactful cyber changes.

A Pivotal Executive Order

To keep pace with the rate and sophistication of today's cyberattacks, the White House issued a memorandum on improving the nation's cybersecurity that lays out a path for agencies to move closer to Zero Trust implementation within the next year.

Zero Trust is identified as the single most effective strategy to safeguard against modern cyberattacks and comply with new regulations, says Tony D'Angelo, vice president of public sector at Lookout.

A 2020 National Institute of Standards and Technology report notes: "Zero Trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary."

"Trust in this case is all about whether a user, their device and the network they are using will introduce risks of a cyberattack," D'Angelo says. "Zero Trust is about 'not trusting' the user, device or network connection until you can verify the risk level and understand whether it meets your security requirements."

> "Zero Trust is about 'not trusting' the user, device or network connection until you can verify the risk level and understand whether it meets your security requirements."
>
> Tony D'Angelo
>
> *Vice President of Public Sector,* Lookout

Definition: Zero Trust security is the concept that devices shouldn't be trusted by default, even if previously verified or connected to an enterprise network. NIST defines Zero Trust as an "evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources."

Fortifying the government's overall cybersecurity posture is a core focus of the federal IT modernization plan. The Technology Modernization Fund, which was established under the Modernizing Government Technology Act of 2017, is a centralized pool agencies can use and apply for loans for technology upgrades.

In March 2021, Congress added $1 billion for the TMF as part of the American Rescue Plan Act, to be available until Sept. 30, 2025. Rep. Gerry Connolly, D-Va., a co-author of the MGT Act, said the additional investment into the TMF will enable agencies to better meet citizen needs.

"Despite urgent congressional action to provide unprecedented levels of economic assistance, those in need have had their misery exacerbated by a broken IT infrastructure that has prevented them from receiving timely support," Connolly said after the bill passed, as reported by Nextgov.

"This $1 billion investment will enable federal agencies to better respond to the coronavirus pandemic and future national emergencies as well as meet the urgent economic needs of American families," he added.

Moving the Needle on Cybersecurity

As part of IT modernization and to adhere to federal guidelines, agencies are quickening the adoption of Zero Trust architectures and establishing higher standards for data security in a post-perimeter world. This sentiment expands the federal space, as private and public industry alike are beefing up cybersecurity to prepare for the now.

> "Having employees working from home means they're relying more on mobile devices for day-to-day productivity and accessing data outside the protective perimeter of the corporate office."
>
> Jim Dolce
>
> *CEO*
> Lookout

“Having employees working from home means they’re relying more on mobile devices for day-to-day productivity and accessing data outside the protective perimeter of the corporate office,” Lookout CEO Jim Dolce says in a blog post.

The trend of employees choosing to work from home has been going on for years, thanks to the adoption of cloud technology and mobile devices, Dolce noted.

“But digital transformation timelines have been exponentially accelerated by this pandemic-driven shift to a remote workforce,” he said.

As a result, government agencies must move to an integrated endpoint-to-cloud security strategy, and comply with new regulations to shield against modern cyberattacks.

Chapter Three:
Zero Trust: Concept to Completion

“According to a survey, 72% of organizations are prioritizing the adoption of a Zero Trust model, and 59% have accelerated their efforts due to the prevailing focus on remote work,” Dolce said at a CyberScoop event.

Organizations are turning to Zero Trust architectures to secure applications, data and resources regardless of where they reside. The General Services Administration published a buyer’s guide in June 2021 to implementing a Zero Trust architecture, referencing NIST SP 800-207 guidelines for updating network cybersecurity in a “world where remote work is prevalent, and traditional network defenses are inadequate.”

Following this blueprint, GSA suggests agencies can brush up their security posture by implementing Zero Trust principles — and the executive order is a strong reminder of the need for all industries to reimagine cybersecurity.

“To deploy Zero Trust and secure mission-critical data, agencies need an integrated security platform that covers the endpoint, the cloud and everywhere in between,” D’Angelo says.

Implementing Zero Trust from the endpoint to cloud is a necessity. Critical data has moved from servers and hardware to the cloud, meaning users can access that data from any network on any device.

Smart Zero Trust-based access decisions, requires telemetry assessment of endpoints, users, networks, data and the ability to provide granular access based on those insights. This is called continuous conditional access. Without a cybersecurity platform that provides telemetry from endpoint to cloud, organizations are left with a blind spot — especially as they increasingly adopt cloud productivity services like Microsoft Office 365. Users will connect with enterprise data beyond email and from various devices, so access to these cloud services must be continuously monitored.

Leveraging Cloud for Success

Security running inside data centers won’t cut it anymore. Organizations need security delivered from the cloud, especially in a remote-first environment. Employees can — and are — working from anywhere, using personal devices and networks organizations can’t always control. From detecting endpoint threats to stopping insider threats and protecting data, security now requires a lot of data and computing power. This is what Tom Davison, senior director of international sales engineering at Lookout, alludes to in his blog — only cloud-delivered solutions have the scalable storage and computing capabilities to leverage machine intelligence to efficiently deploy cybersecurity

Why Endpoint Threat Telemetry is Critical

D'Angelo notes four steps to modernizing government cybersecurity with Zero Trust based on the White House executive order. It starts with ensuring the agency can continuously assess risk on endpoints.

When gauging risk, security leaders must assume nothing is free of risk until proven otherwise, and employee user accounts, devices and networks must be evaluated. Assessments should also happen continuously.

"To deploy a modern Zero Trust architecture, you need to track the constant change in risk levels of all user devices, including iOS, Android and Chrome OS devices. These endpoints are the leading targets for advanced persistent threat (APT) reconnaissance and attacks that steal login credentials due to the effectiveness of mobile phishing," Lookout Chief Strategy Officer Aaron Cockerill wrote in a recent blog post. "Mobile devices are rarely connected to enterprise perimeter security as they are usually on cellular or public or home Wi-Fi. They also frequently have OS and app vulnerabilities that open doors for exploitation and data leakage."

Agency cybersecurity leaders should ensure any device, including smartphones or tablets, won't introduce malware or allow an attacker to gain access to the infrastructure.

Understand your users with robust CASB and ZTNA solutions

The second step is to provide dynamic and granular access to cloud-based or on-premises applications. D'Angelo says multifactor authentication is a good way to know if an account is compromised. But it's not enough.

"Agencies also need to be able to spot abnormal behavior that might indicate an internal or external threat," he writes.

Definition: Granular access controls define who can have access to each part of a system and what they can do with that access.

This can be done with a cloud access security broker, or CASB, a secure access technology to provide access and security to cloud applications.

CASB, a cloud-based software, acts as an intimidator between a remote user and a cloud application, like Dropbox, Google Workspace or Slack. Users begin to use these cloud applications from home with or without prior approval of IT, so CASB tools provide IT management visibility into all cloud services in the enterprise while enabling them to implement security controls.

Zero Trust network access, or ZTNA, solutions also play a role, as they perform the same function for on-premises applications running in an organization's data centers.

ZTNA understands what users need for work via contact-aware access to data, so it knows what to allow access to depending on the risk level and of the user and device. Currently, organizations rely on VPNs to provide access to software and data inside their data centers, which provides a connected user unlimited access.

Both CASB and ZTNA have robust user entities and behavior analytics, or UEBA, functionality. These tools enable security teams to understand how employees usually behave, so they can detect anomalies and stop insider threats and advanced cyberattacks.

The third step is to verify cloud configurations. D'Angelo says it's important to verify the security posture of cloud applications used by government employees. Misconfigurations in SaaS and IaaS applications can create opportunities cyberattackers exploit. Adopting SaaS security posture management and cloud security posture management tools can be used to verify cloud configurations.

Data Security that Goes Wherever Your Data Goes

The fourth and final step is to secure data wherever it goes. Managing the security of cloud applications and all the data that moves through them can be challenging, but agencies need to have full control over their data to ensure it's safe and protected.

"Continuous assessment of your users and endpoints is essential," said Cockerill in another recent blog post. "But the flip side of that is knowing the sensitivity of the data they access. To ensure your workers have what they need to stay productive while also safeguarding sensitive data, policy enforcement should be able to map risk with data sensitivity."

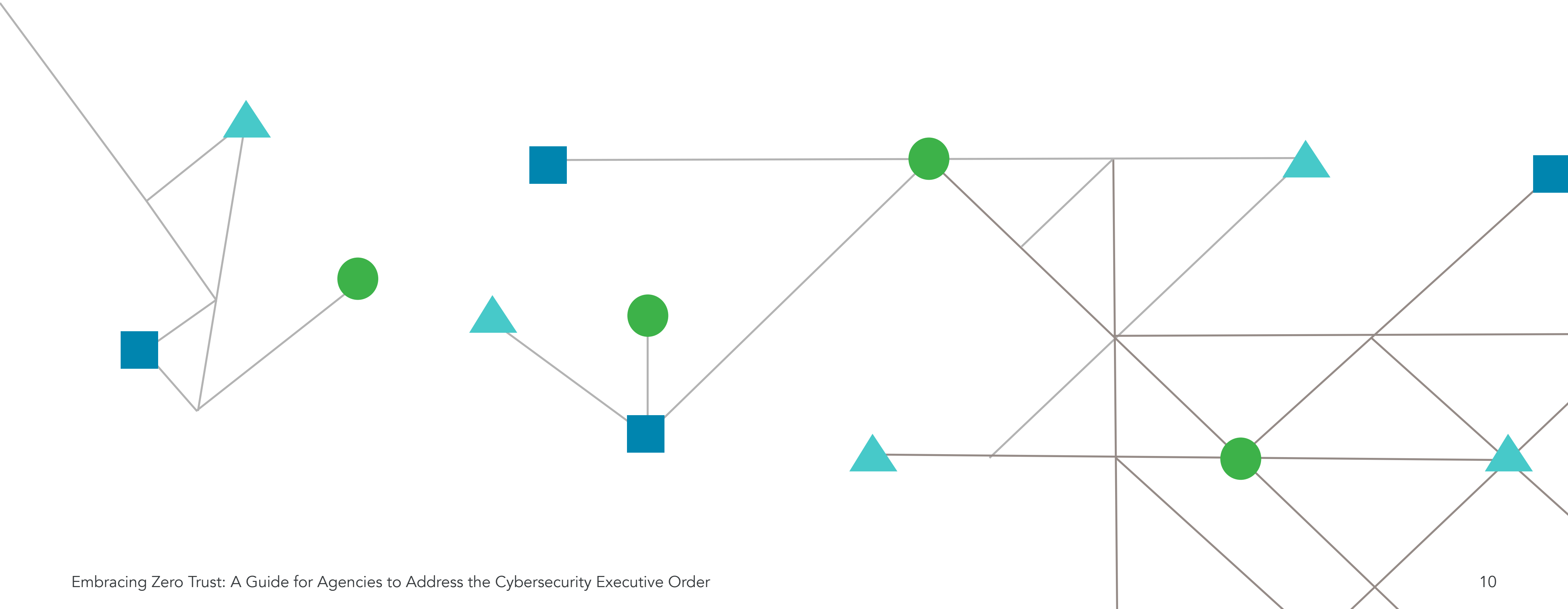
Visibility from Endpoint to Cloud

To deploy a Zero Trust framework and truly secure enterprise data, agencies need an integrated security platform that includes the endpoint, cloud and everything in between. Rather than patchworking different products from different vendors connected to a single VPN, Cockerill suggests first understanding where data is going. It's no longer sufficient enough to extend VPNs and top it off with two-factor authentication and network access control. This method verifies risk at the time of connection, omitting the fact that risk levels change all the time.

Today, a Zero Trust framework needs to account for a remote workforce where data has completely moved to the cloud. Users are connecting with their own devices networks, which may introduce new risks. Organizations need visibility into everything — the user's activity, the endpoints and networks they use, and the apps and data they interact with.

This means tracking constant change in risk levels of all user devices, analyzing user behavior to detect unusual activity and fully understanding the sensitivity of the data that access is being granted to. ZTNA, for instance, can be applied here to ensure access is granted to specific on-premises applications users need for work, and continuously monitor that activity.

To make this even more seamless, Lookout has expanded its capabilities to meet these needs. Its Continuous Conditional Access solution integrates its security and access platforms so organizations can make risk assessments of endpoints and users, and apply that information to granular Zero Trust-based access controls.



Chapter Four:
Today's Evolving Threatscape

"Cyberattackers are becoming more sophisticated with well-orchestrated techniques like ransomware-for-hire and socially engineered attacks that can be performed repeatedly, with greater frequency and at lower cost," D'Angelo says.

In addition to implementing Zero Trust access, organizations in all sectors must focus on the complex threatscape created by nation-states and adversaries.

HP-backed research by the University of Surrey found a 100% rise in "significant" nation-state incidents between 2017-2020. The SolarWinds hack, for instance, is suspected to have been committed by a group backed by the Russian government.

Security teams no longer operate under an if-we-are-attacked mentality. Rather, they expect they will be attacked, and need the telemetry data to proactively hunt for threats and respond to incidents when they happen.

Proactive Threat Hunting

Threat intelligence is one of the primary goals listed in the executive order. Specifically, the White House intends to improve the ability to detect vulnerabilities and cybersecurity incidents on government networks.

"Implementing a governmentwide endpoint detection and response system will improve information sharing within the federal government and enable proactive threat hunting to stop threats early on the networks and enable continuous improvement of cyber defenses," D'Angelo says.

> "Implementing a governmentwide endpoint detection and response system will improve information sharing within the federal government and enable proactive threat hunting to stop threats early on the networks and enable continuous improvement of cyber defenses."
>
> Tony D'Angelo
>
> *Vice President of Public Sector,* Lookout

With the influx of people working remotely, IT teams need complete visibility into network activity as if they still had a perimeter. Coupled with the spike in frequency and cost of cybersecurity breaches, IT teams have shifted their focus from protecting the endpoint to protecting the data.

Organizations have activity monitoring for servers, desktops and laptop computers, especially in the office. What they don't often have is the same telemetry data for smartphones, tablets and mobile devices. Considering people use their mobile devices for work now more than ever, attacks on these endpoints have surged.
"What Lookout security analysts have observed first-hand is that cybercriminals are building campaigns that are targeting tablets, smartphones and Chromebook in addition to desktops and laptops," Lookout Principal Product Manager Alex Gladd writes in a blog post.

Security teams need the same comprehensive data for mobile endpoints they have for servers, desktops and laptops. This is where extended detection and response comes in — the next critical requirement that empowers teams to rapidly detect and respond to mobile threats.

"Telemetry data is compiled with fundamental elements — uniqueness of data set and length of time," D'Angelo says. "This can enable agencies to stop nation states from deploying repeatable attack mechanisms."

The Lookout endpoint detection and response solution uses behavior-based threat protection by analyzing thousands of telemetry data points from smart devices running its application. Lookout uses the data collected to identify threat indicators and displays the data and analysis via a console so organizations can easily monitor their mobile fleet. Security teams can even search through the mobile endpoint security graph to track active attacks and prevent further data damage.

> "Telemetry data is compiled with fundamental elements — uniqueness of data set and length of time. This can enable agencies to stop nation states from deploying repeatable attack mechanisms."
>
> Tony D'Angelo
>
> *Vice President of Public Sector,* Lookout

READ: To enable its corporate-owned, personally enabled mobility policy, this Global 2000 bank deployed Lookout Mobile Endpoint Security to 9,000 Android phones managed by VMware AirWatch and found hundreds of diverse threats upon deployment.

“There are times, for example, where you will find desktop and mobile phishing sites that are both linked to malware targeting desktop and mobile users, revealing a larger coordinated campaign,” Gladd writes. “Using the EDR console enables you to identify these pivot points and make preemptive discoveries without first waiting for a user to be phished or a device to be compromised.”

Definition: A pivot is identified as where malicious code comes from and the associated web domains.

However, tools to support proactive threat hunting must be a part of a comprehensive strategy to fully gain advantage.

> “Using the EDR console enables you to identify these pivot points and make preemptive discoveries without first waiting for a user to be phished or a device to be compromised.”
>
> Alex Gladd
>
> *Principal Product Manager*
> Lookout

Chapter Five: Embracing a New Age of Cybersecurity

There's no denying the pandemic expedited digital transformation for government entities and propelled cybersecurity requirements to meet today's standards. As the government welcomes new technologies for business continuity and citizen services, protecting the nation's networks and data remains critical. The cybersecurity executive order and recent memorandum are a major step in developing a formal plan to address the evolving cyber threatscape.

"We read about ransomware attacks in the news now almost on a weekly basis," D'Angelo says. "It's a positive sign to see the federal government take proactive versus reactive steps to building a plan, develop a multi-agency ransomware task force, and work with the private sector for Zero Trust security solutions that will address a specific set of cybersecurity requirements."

Cross-sector Collaboration

As the nation continues to grapple with an increased attack surface and inundation of cyberattacks, collaboration between public and private entities on the adoption of modern cybersecurity practices is more critical than ever.

As an incentive, the State Department announced a reward of up to $10 million for information leading to the identification or location of any person tied to foreign-state-sanctioned cyberattacks on U.S. critical infrastructure.

The executive order also highlights efforts to axe barriers of collaboration between public and private organizations, promoting threat intelligence sharing that will result in faster response and reporting of cyber incidents.

Conclusion: Zero Trust Secures Data in a New Cyber Threat Era

The federal government is embracing its digital shift. By requiring a Zero Trust framework in the executive order, the White House aims to cover the attack surface gaps exposed in today's modern post-perimeter world.

"The administration recognizes the need to address emerging threats such as phishing attacks, which are the primary method used by bad actors to steal credentials and launch ransomware attacks," D'Angelo says.

Lookout remains committed to keeping federal, state and local agencies secure through its comprehensive platform that addresses the requirements of a modern endpoint-to-cloud Zero Trust architecture.

To achieve this level of security, Gartner has categorized the technologies needed to adopt Zero Trust as Secure Access Service Edge, or SASE. SASE solutions include CASBs, ZTNAs, secure web gateways and data loss protection. Lookout takes this one step further by integrating it's leading mobile endpoint security solution, ensuring that organizations has visibility and policy enforcement capabilities from endpoint to cloud.

Definition: SASE, as defined by Gartner, is a security framework prescribing the conversions of security and network connectivity technologies into a single cloud-delivered platform to enable secure and fast cloud transformation.

"It is best to deploy these multiple core services in a single cloud-delivered platform," Dolce says. "This allows IT managers to require the same consistent policies to all content transfers to and from any of these SASE applications."

A platform approach integrated from endpoint to cloud is critical. With this method, as Dolce notes, organizations can have consistent security policies across all applications and data, and a single platform eliminates the swivel-chair administration of multiple discrete products that can introduce human error. Plus, with proper visibility, a single platform can provide the telemetry data from all security functions for Zero Trust-based access, threat detection and incident response.

While guided by government policy, the majority of U.S. critical infrastructure is owned and operated by the private sector — so agencies can't do this alone. Information sharing is essential to cyber resilience, and Lookout is committed to collaborating with government partners to strengthen the U.S. cyber defense and protect critical infrastructure.

Lookout