Four Actionable Steps for Agencies to Get Started with Zero Trust

A Zero Trust framework moves away from one-time security gating decisions, toward continuous assessment of the risk level of the user and device, and dynamically adapting access privileges based on changes in the risk level.

Tony D'Angelo
Vice President, Public Sector
Lookout

In May 2021, President Joe Biden signed an executive order to strengthen U.S. cybersecurity defenses. The guiding principle is that organizations need to adopt a Zero Trust framework for cybersecurity. You may ask: what exactly am I trusting and what does "zero" have to do with it? Trust in this case is all about whether a user, their device and the network they are using will introduce risks of a cyberattack. These risks could come in many forms – malware or ransomware, vulnerabilities that can be exploited, or compromised credentials or devices. 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.

Without Zero Trust, users are granted privileges to your infrastructure and data once and security teams have limited visibility into what the user or device is doing. Without reverifying the risk level, it is free to access any resources. If a cyberattacker subverts the device or user account, then the attacker can easily move laterally and likely to go undetected, resulting in a breach.

A Zero Trust framework moves away from one-time security gating decisions, toward continuous assessment of the risk level of the user and device, and dynamically adapting access privileges based on changes in the risk level.

As a result, a Zero Trust framework enables agencies to more effectively protect apps and data in the age of telework and cloud collaboration.

The federal government wants to apply modern Zero Trust technology to ensure that employees, data and its infrastructure are protected. Below are four steps you can take right away.

Step 1: Ensure your agency can continuously assess risk on endpoints

With many remote workers using personal devices these days, it's important to ensure that only trusted devices can access your network.

Agency cybersecurity leaders can take steps to ensure that any device – whether it's a smartphone, tablet, Chromebook or PC – will not introduce malware or create a pathway for an attacker to gain access to your infrastructure.

Step 2: Provide dynamic and granular access

Multi-factor authentication is a good first step towards knowing whether an account is compromised, but it's not enough. Agencies also need to be able to

Government data also should be encrypted wherever it goes — in transit and at rest — whether it is being emailed, uploaded to a cloud or downloaded to a local drive. Only the highest level of encryption is sufficient so that only authorized users with the encryption key can gain access.

spot abnormal behavior that might indicate an internal or external threat. This can be achieved with a cloud access security broker (CASB) solution that has robust user entity and behavior analytics (EUBA). By understanding how employees usually behave, agencies can spot malicious activity and prevent insider threats and advanced attacks.

Step 3: Verify cloud configurations

It's important to verify the security posture of the cloud applications used by government employees. Misconfigurations in software as a service (SaaS) applications, such as Box, or Microsoft 365, and infrastructure as a service (IaaS) like AWS, Azure or GCP environments can create opportunities that cyber attackers exploit.

Agency cybersecurity teams can utilize SaaS Security Posture Management (SSPM) and Cloud Security Posture Management (CSPM) tools to verify cloud security configurations and prevent them from creating opportunities for cyberattackers.

Step 4: Secure data regardless of where it goes

It can be overwhelming to manage the security of cloud applications and the data that flows through them, especially when multiple clouds exist and a myriad of work streams are in play. Agencies need to have full control over their data regardless of how it's handled or where it goes.

To ensure sensitive information does not leak out accidentally or is stolen by a threat actor, organizations have a single viewpoint to see what's happening and manage granular access policies based. This can only happen if there's an understanding of the user or device's risk posture, what they need access to and the types of data and apps required for productivity.

Government data also should be encrypted wherever it goes – in transit and at rest – whether it is being emailed, uploaded to a cloud or downloaded to a local drive. Only the highest level of encryption is sufficient so that only authorized users with the encryption key can gain access.

The Executive Order is a good reminder of the critical need for both the public and private sector to rethink 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.

For more information on how Lookout delivers Zero Trust to government, please visit www.lookout.com/gov. ■

About The Author

Mr. D'Angelo leads the Americas Public Sector team at Lookout, bringing more than 30 years of experience in the IT industry. He received his Bachelor of Science in mechanical engineering from the University at Buffalo and has spent his entire professional career in Washington, D.C. Having joined Lookout in 2019 to lead the Americas commercial enterprise team, he now heads the combined federal-SLED business unit.
Contact sales-pubsec@lookout.com for more information or visit www.lookout.com/gov.