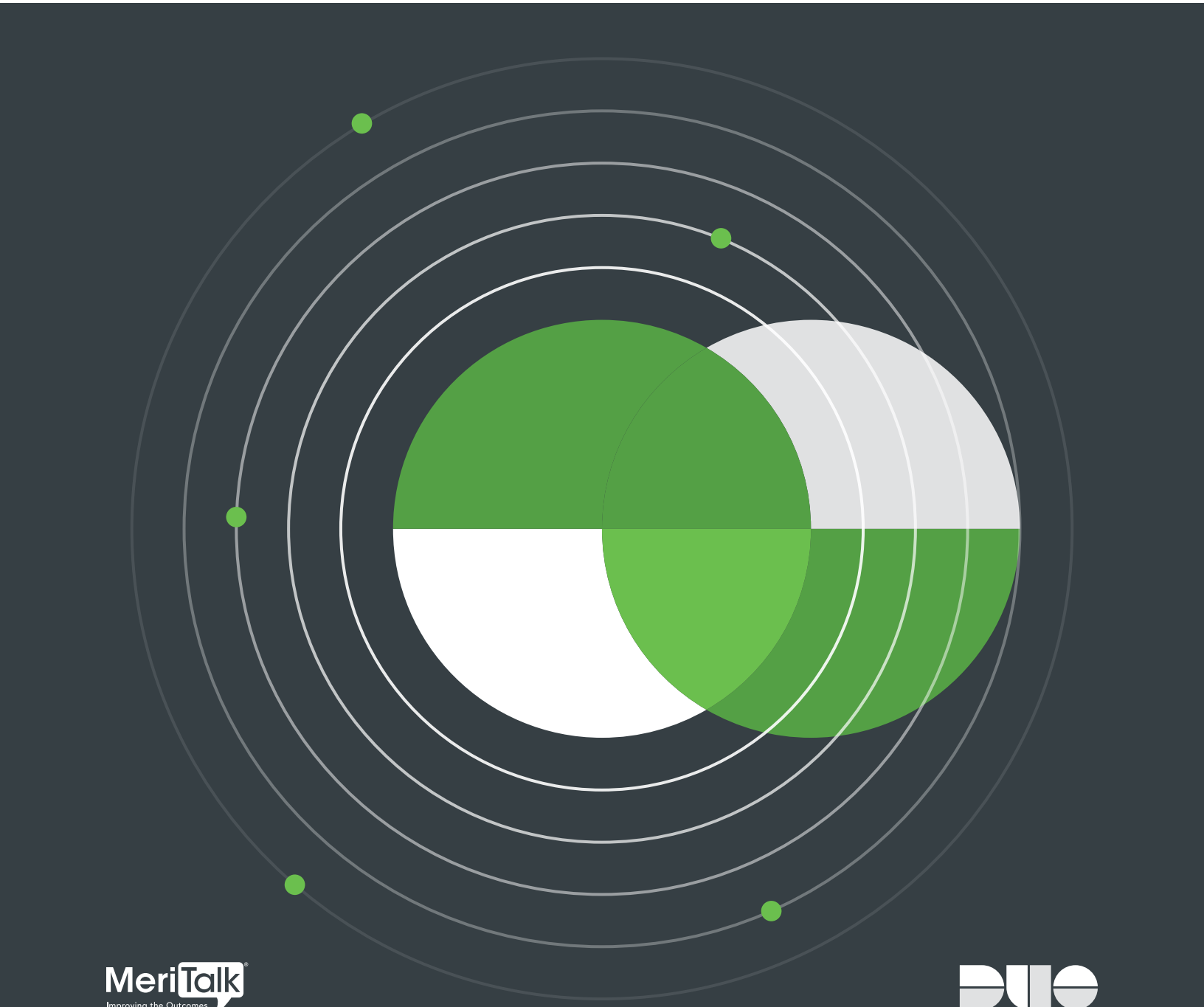
DUO SECURITY AND MERITALK PRESENT

The Path to Zero Trust Begins With Dynamic Authentication



MeriTalk
Improving the Outcomes of Government IT

DUO

The February 2021 hack of a water treatment plant in Oldsmar, Fla. – likely via a shared application – could have resulted in the poisoning of thousands of people, absent the observational skills of a supervisor who witnessed unusual network activity.

The breach of SolarWinds' Orion network management software, which caused billions of dollars in damages to nine Federal agencies and hundreds of private-sector firms, was caught in December 2020 in part because the private-sector firm that discovered it employed two-factor authentication (2FA). The firm dug deep into its systems when that authentication flagged a new device trying to get onto its network.

The SolarWinds hack was vastly more sophisticated than the water plant breach. However, they share a common lesson: If routine cybersecurity measures are employed, cyberattacks can be prevented or at least mitigated.

These cyber events and others reinforce the notion that organizations don't always learn from past experiences. Over-privileged accounts, shared accounts without strong multi-factor authentication (MFA), and weak identity proofing still compromise the government's security architecture, even though agencies often could leverage existing security technologies and build upon them.

Move From Static To Dynamic Authentication

Authentication is a great example of these existing technologies. Traditional methods of authentication, such as public key infrastructure (PKI) smartcards and biometrics, are incredibly strong. They demonstrate that the person accessing a system has either the password and private key or the fingerprint required to access that system. But today, agencies need greater assurances – assurances that the person is interacting with the system in acceptable ways.

Secure Shared Administrative Accounts

Agency policies often dictate one personal identity verification (PIV) for one person, but that doesn't work with shared administrative accounts. Agencies need MFA on these accounts – delivered in a way that isn't endlessly complex.

One solution – a best practice – is to separate the primary and secondary authentications. For example, username and password are handled by Active Directory, and a second factor is handled by another system. The second factor is unique to each end user, so administrators can see who is accessing the administrative account and what device they are using. This separation of controls helps prevent lateral spread of cyber threats across compromised administrative accounts, which has been a hallmark of breaches over the past decade.

To achieve this, agencies can build upon their existing authenticators by incorporating additional security checks into the authentication workflow. Those checks account for other aspects of a person's digital identity, such as the device and browser used to access the system; the type of MFA used; and where the authenticator resides.

The process of determining whether an authentication request is trustworthy is the heart of dynamic authentication. It enables the agency to quickly react to changes and emerging threats. With a smartcard, for example, the dynamic authentication process begins by checking the personal identity verification (PIV) credential to confirm it is using a valid security certificate, and to determine if the credential is a physical PIV or a derived credential. A derived credential is most likely on a mobile device.

If a mobile device is in use, additional checks are done, such as determining the operating system and whether Flash or Java is enabled. These checks permit agencies greater flexibility in bring your own device (BYOD) adoption for employee telework and contractor access to agency systems. Dynamic authentication can restrict access to some applications only to agency-managed devices, and it can allow access to less sensitive applications from personal, unmanaged devices.

Hit "Pause" For Better Security

Agencies can accomplish these additional security checks by pausing the authentication process with a dynamic authentication policy engine. The engine queries data about the device and compares it against organizational policies before granting access to agency systems. The process builds policy enforcement into the authentication process, and it uses the agency's existing authentication technology – no rip and replace required.

Here's a real-world example: In December 2020, Apple identified an iOS vulnerability that would allow arbitrary code execution in versions 14.3 and earlier, and it advised users to update to the latest version immediately. At Cisco, which has about 400,000 endpoints across about 120,000 users, including unmanaged devices, administrators enacted a global policy in a few hours that prevented anyone from logging on to its systems with a device running an outdated iOS version.

Involve End Users In The Security Mission

Besides improving speed to security, dynamic authentication enables organizations to enlist end users in agency security in ways that previously weren't possible. For example, when a user is prevented from logging on because of a security issue, the dynamic authentication policy engine tells the user about the specific issue. The user can then provide this information to the help desk, eliminating a potentially lengthy discovery process – and again, speeding security.

Dynamic authentication helps agencies to:

- Ensure only approved browsers are used to access resources
- Quickly enforce browser updates if critical vulnerabilities are discovered
- Prevent use of outdated operating systems
- Control mobile device access to resources
- Enforce or prevent specific versions of Java and Flash
- Limit privileged account access to domain controllers or critical servers only
- Set special permissions around local administrative accounts

Dynamic authentication enables agencies to quickly react to security incidents and adapt their authentication workflows to minimize risk on a global, application, or individual account basis.

In some cases, agencies can permit end users to manage certain aspects of their technology, such as their browser. Agencies don't necessarily need to take on browser management across the enterprise – pushing updates to all endpoints – because the policy engine checks and enforces browser policy during authentication. If a device isn't compliant, the policy engine delivers a link to the user – they just click to update, and authentication can proceed. Actively involving end users in maintaining the agency's security posture tends to lower resistance to new security practices because employees feel like they are part of the solution and it frees IT help desk resources.

Advance Toward Zero Trust

Each of these practices is a step along the agency journey toward a zero trust security framework, in which user trust is not granted until the user is authenticated and authorized. Zero trust was born from the need to push security perimeters past firewalls, ensure protection from stolen or lost credentials, and protect access to all applications, for every user and device. The COVID-19 pandemic moved zero trust from a theoretical discussion in many government agencies to a priority, and over the past year, 44 Federal agencies have dedicated teams to research or to start implementing zero trust.

Since unique user credentials became standard practice, every agency has been on the path to zero trust, and every agency will have a slightly different route. To learn more about the agency journey to zero trust with stronger, more dynamic authentication, visit Duo Security.