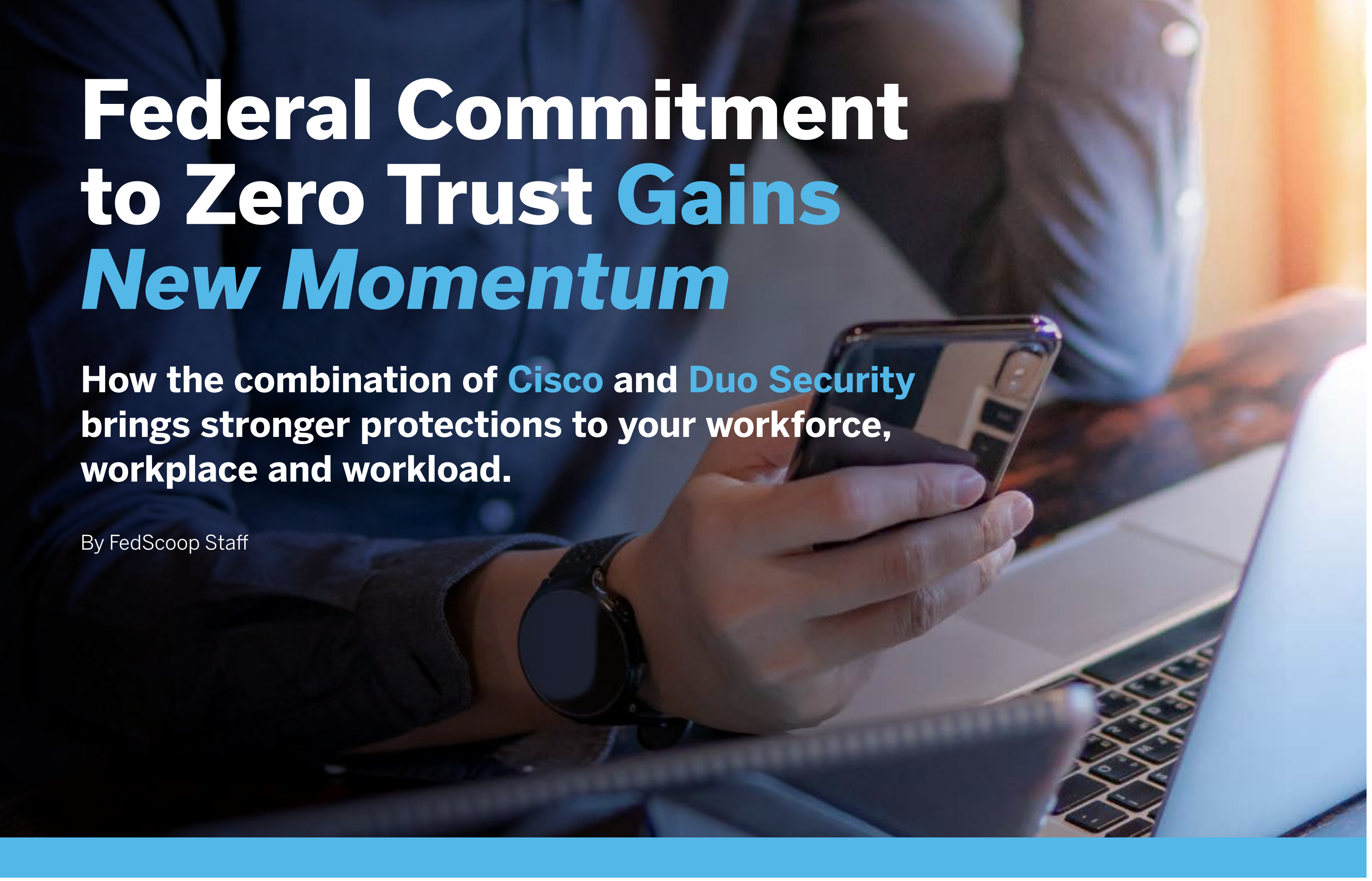


Federal Commitment to Zero Trust Gains *New Momentum*

How the combination of Cisco and Duo Security brings stronger protections to your workforce, workplace and workload.

By FedScoop Staff

FEDERAL AGENCIES have been moving to secure their networks using zero-trust principles for more than a decade. However, a number of factors are coming together in 2020 that are enabling agencies to better embrace the constructs of zero-trust security, and to begin leveraging them to better protect their resources.

Creating a zero-trust environment doesn't mean trust no longer exists. Rather, the focus is on establishing trust where and when it counts: not at a network perimeter checkpoint, but at the moment an authenticated user—using a successfully interrogated and approved device—seeks to access a specific application or resource.

That's getting easier for federal agencies, thanks to a combination of initiatives over the past year from federal policymakers—and a raft of advances in technology capabilities.

Taken together, agency officials now have a more precise roadmap and better tools to address a protracted challenge: how to give authorized users broad access to agency resources while preventing any abuse of access privileges.

Agencies still face a never-ending game of catch-up: Data demands continue to escalate as quickly as the threats; and efforts to modernize aging systems often compound the complexities already inherent in large-scale government IT systems.

However, federal agencies are in many ways better positioned than many private sector enterprises to abandon the traditional reliance on network perimeter defenses in favor of highly granular and adaptive user and device authentication technologies, said Sean Frazier, a 25-year IT security expert at Duo Security, now a part of Cisco Systems.

"It doesn't always happen, but I think the public sector actually understands zero trust a little better than the private sector because of things like ICAM [identity, credential and access management] practices that were established as a core tenet of security a long time ago. Directives like the government's federal ICAM strategy and renewed guidance from NIST are helping agencies adopt a more agile approach to security," said Frazier, who serves as Duo's advisory CISO to federal customers.

Paving the way for zero trust

Frazier pointed to several examples over the past year, where the White House Office of Management and Budget laid out a clearer commitment for deploying identity and authentication practices to secure government data systems, including directives on:

FICAM – The Federal Identity, Credential and Access Management memo directs agencies to develop the means to identify, credential, monitor and manage user access to information and information systems across their enterprise as the primary method to ensure secure and efficient operations

TIC 3.0 – Revisions in OMB's Trusted Internet Connection policy aims to remove barriers across the federal government to cloud and modern technology adoption while enhancing network security.

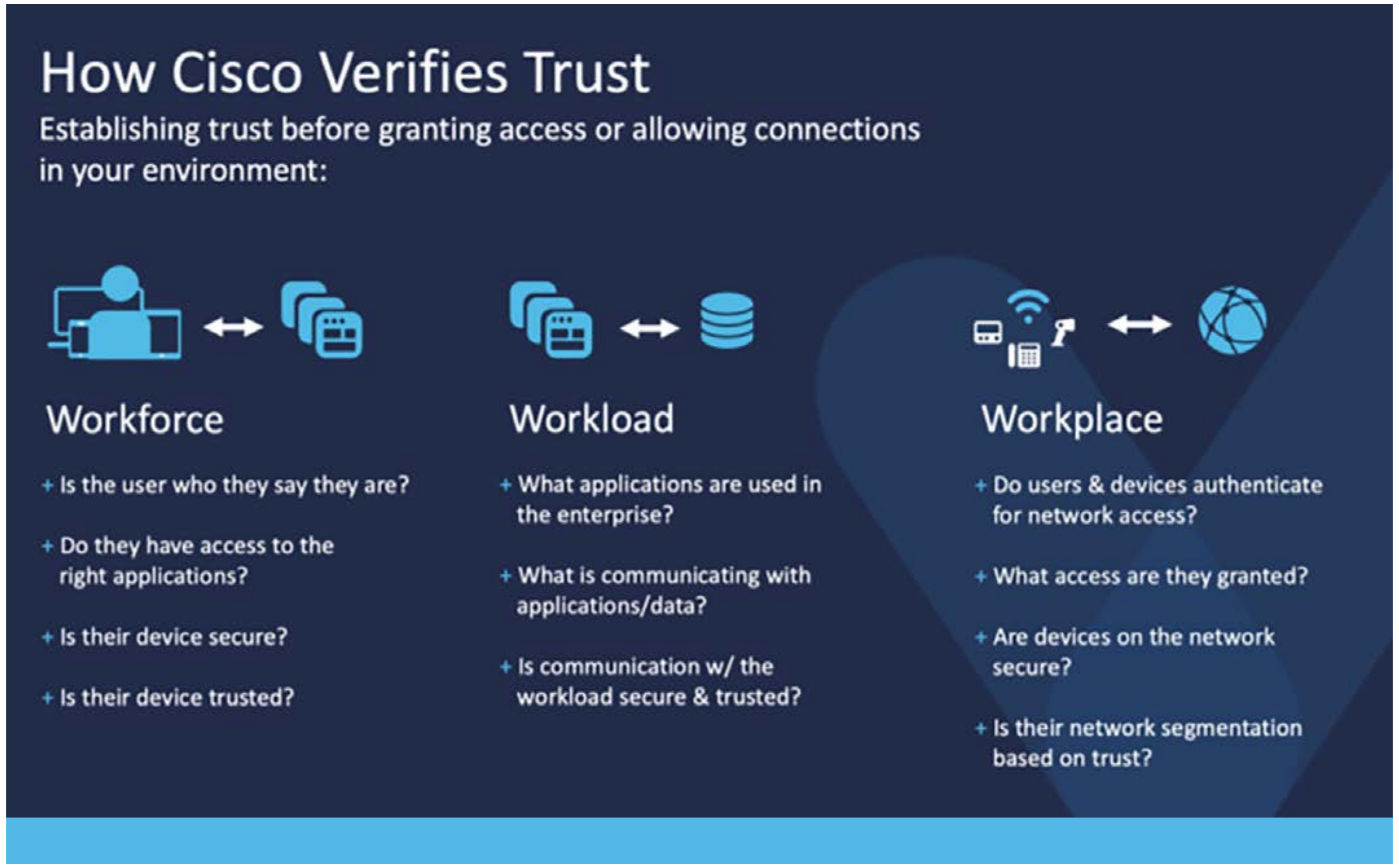
Federal Data Strategy and action plan provides a common set of data principles and practices to better leverage data as a strategic asset.

Those initiatives build on a number of foundational requirements for zero trust, prescribed as part of the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program, including requirements for agencies to fully inventory and analyze the users and devices operating on their networks.

Zero trust assist at NIST

However, perhaps the biggest bellwether of zero trust's arrival as a security model in federal government, said Frazier, is National Institute of Standards and Technology's release of a new draft publication that details the core components and design considerations of a zero-trust architecture (ZTA) network strategy [see sidebar]. The draft represents an important step forward to help agencies build on NIST's guidance on digital identity assurance and develop a zero-trust way of life, he said.

ZTA isn't a single network architecture; nor is it about only securing data. Rather, it captures a set of guiding design principles for agencies to use trust verification components to securely control access to a full range of digital assets, including compute resources, applications, Internet of Things (IoT) 360 actuators, printers, and other resources.



How Cisco Verifies Trust

Establishing trust before granting access or allowing connections in your environment:

Workforce

- Is the user who they say they are?
- Do they have access to the right applications?
- Is their device secure?
- Is their device trusted?

Workload

- What applications are used in the enterprise?
- What is communicating with applications/data?
- Is communication w/ the workload secure & trusted?

Workplace

- Do users & devices authenticate for network access?
- What access are they granted?
- Are devices on the network secure?
- Is their network segmentation based on trust?

Zero trust is a philosophy, not a product, Frazier emphasized. Achieving zero-trust security in federal agencies, he explained, involves the coordination of four underlying practices:

Continuous authentication – Verifying the identity and trustworthiness of users and devices continuously, using a combination of behavioral data points.

Device assessments – Ensuring devices meet a predetermined set of rules before they're granted access.

User controls – Determining access privileges on a per-application basis with role-based controls.

Application access – Providing granular, role-based access to specific applications based on your customized access policies.

Until recently, putting these concepts into practice required tremendous technical coordination. And even when there was a will, there wasn't always an easy way, given the age and complexity of most federal IT systems.

That's changing in significant ways however,—most notably with Cisco's acquisition of Duo Security in the fall of 2018.

Leveraging industry-leading trust solutions

Over the past year, the two companies completed the integration of Duo's unified, cloud-delivered zero-trust and multi-factor authentication (MFA) solutions with Cisco's software-defined (SD) infrastructure access and segmentation technologies.

The combination provides federal agencies a comprehensive zero-trust security approach to:

Protect your workforce – Duo Security's MFA and contextual user access policies ensure that only the right users and secure devices can access applications.

Protect your workplace – SD-Access helps secure and easily manage all user and device connections into and across your network, including IoT, so users and devices can access only what they need to do their job and function.

Protect your workload – Tetration automates and enforces network traffic and segmentation policies for applications in a multi-cloud environment.

"We already had much of this in place, but we did not have the workforce covered until we acquired Duo," said Cisco's Peter Romness, cybersecurity programs lead, U.S. public sector. "Buying the leader in the industry and effectively integrating them into our platform has really put us on track to fulfill these goals as the key tenants of **Cisco's zero-trust** security strategy."

The combination of zero-trust solutions also caught the attention of IT market analysts at Forrester. The Forrester WaveTM "Zero Trust eXtended Ecosystem Platform Providers, Q4 2019" recognized Cisco as a leader.

Duo has also benefitted from joining forces with Cisco. Cisco's resources helped accelerate the timetable for Duo to secure FedRAMP authorization for two of Duo's cloud-based, government-tailored access management solutions.

Duo Federal MFA and Duo Federal Access provide secure application access for federal agencies and other public sector customers to ensure only trusted users and trusted devices can access protected applications. Duo Federal Access adds stronger role-based and location-based access policies and biometric authentication enforcement that meet NIST Authentication Assurance Level 2 standards, providing proven assurance that users or devices can be trusted, according to Frazier.

Duo's FedRAMP authorization adds to Cisco's FedRAMP portfolio, which includes Cisco's Cloudlock, to help agencies secure cloud identities, data and applications; Cisco Webex Meetings; Cisco Hosted Collaboration Solution for Government; and Cisco Hosted Collaboration Solution for Defense.

"With Cisco and Duo, you get an exciting and capable product from a startup company like Duo with the force and backing of a major player, like Cisco," concluded Romness. "And you get the power of the network brought to bear upon the idea of "multi-factor authentication and the other advantages that Duo brings."

Another advantage of the Cisco-Duo combination, said Frazier, "is the ability it brings to manage authentication and access to resources in multiple cloud environments, as well as on-premises resources. With Duo, administrators can easily add MFA to any cloud application including Office 365, Azure, AWS, Google, Workday, Box and more. Not everything belongs in the cloud. But if you can get economy of scale, you need to make sure you get security in the bargain."

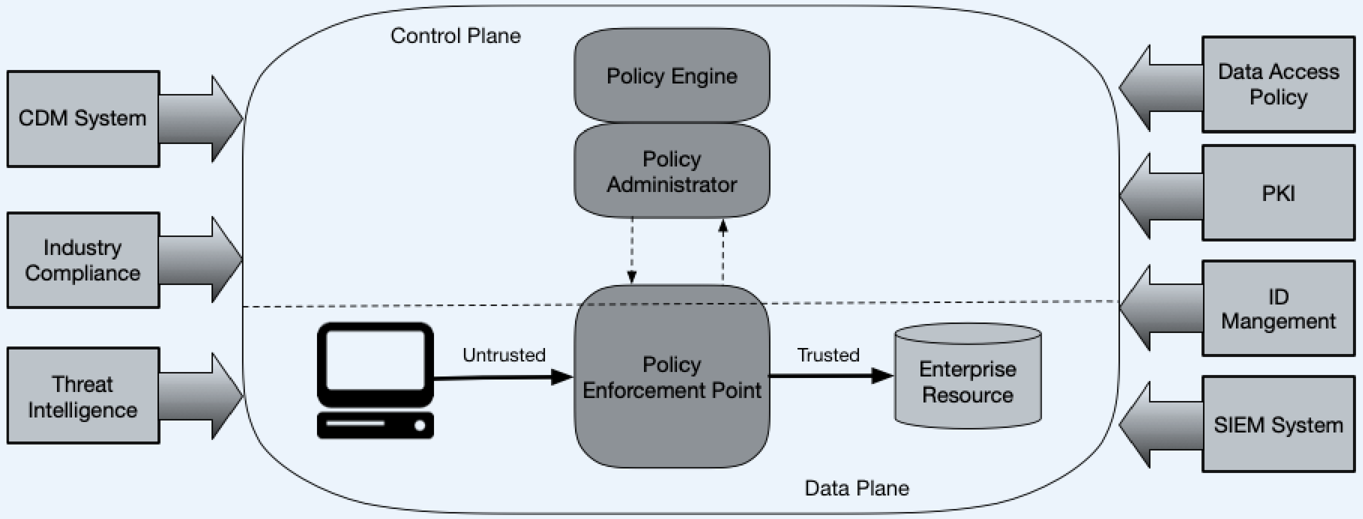
Learn more about how Cisco's and Duo Security's zero-trust strategies can better protect your agencies workforce, workplace and workload.

NIST lays out design tenets for Zero Trust Architecture

The initial draft of Zero Trust Architecture guidelines by the National Institute of Standards and Technology provides federal agencies with essential tenets and components for designing a zero-trust security strategy. It recommends:

1. **All data and computing services are considered resources.** Personally-owned devices, if allowed to access enterprise applications and data, must be included.
2. **All communication is secure regardless of network location.** Access requests from within the network must meet the same security requirements as those from outside of it—and communication must be encrypted and authenticated.
3. **Access to individual enterprise resources is granted on a per-connection basis.** Every device requesting access must be evaluated before access is granted; and authentication to one resource doesn't automatically grant access to another resource.
4. **Access to resources is determined by policy.** That includes verifying the state of user identity, the requesting system and behavioral attributes when warranted.
5. **The enterprise ensures all owned and associated systems are in the most secure state possible.** And they need to monitor systems and apply patches or fixes as needed to ensure they remain se**cure.**
6. **User authentication is dynamic and strictly enforced before access is allowed.** NIST refers to this as a "constant cycle of access" of threat assessment and continuous authentication, requiring user provisioning, authorization and reauthentication throughout user interaction.

Zero Trust Architecture Logical Components



Core Zero Trust Logical Components

Source: NIST SP 800-207; Cisco overview of ZTA