accenture

AFS Zero Trust

Strategy and Roadmap

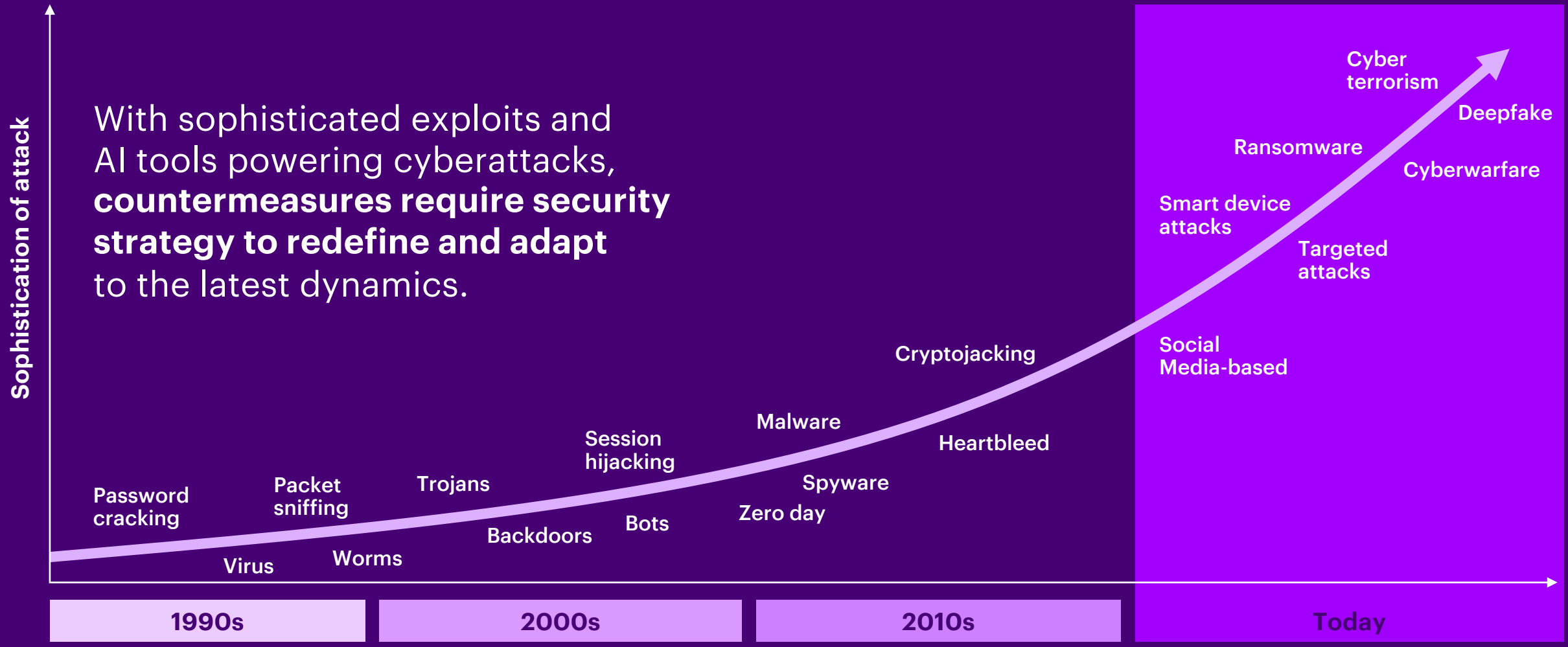
Partner Messaging Workshop

OUTCOMES OF OUR MEETING

1. Understand our strategy, understand our why
2. Empower you to take action within your market
3. Socialize capability roadmap and GTM activities for FY22Q4 and beyond

AGENDA

Threats are more sophisticated and effective



Security models cannot be static and must assume a threat actors are always present

New Assumptions

Intruders are omnipresent:
A bad actor is always present, so we must reduce the potential "attack surface"

Endpoints:
Devices can be friendly one moment and hostile the next, *even internal ones*

The network is insecure:
The network is not be considered a security control for protection

New Principles

Operate in real-time:
Use dynamic threat analyses of multiple threat vectors

Data is the priority:
What we're really protecting is our intellectual property and data

Streamline the security environment:
Ensure our complex security environment is more manageable and organized

This is known as the zero-trust security model

While the basics of zero trust have been a part of DoD for some time, we continue to build a cybersecurity strategy to protect DoD's most valuable asset—data

Protect data at any state

Must be protected at any state: rest, during processing, and while in transmission

Control user access

Essential to implement security measures that enforce the right user access controls during data processing

Deploy tools at endpoints

Deploy tools to prevent data loss at endpoints, edge devices, and in-app to prevent unauthorized access

Mitigate data loss

Prevent data loss, encrypt data at rest, monitor security vulnerabilities, and implement governance safeguards

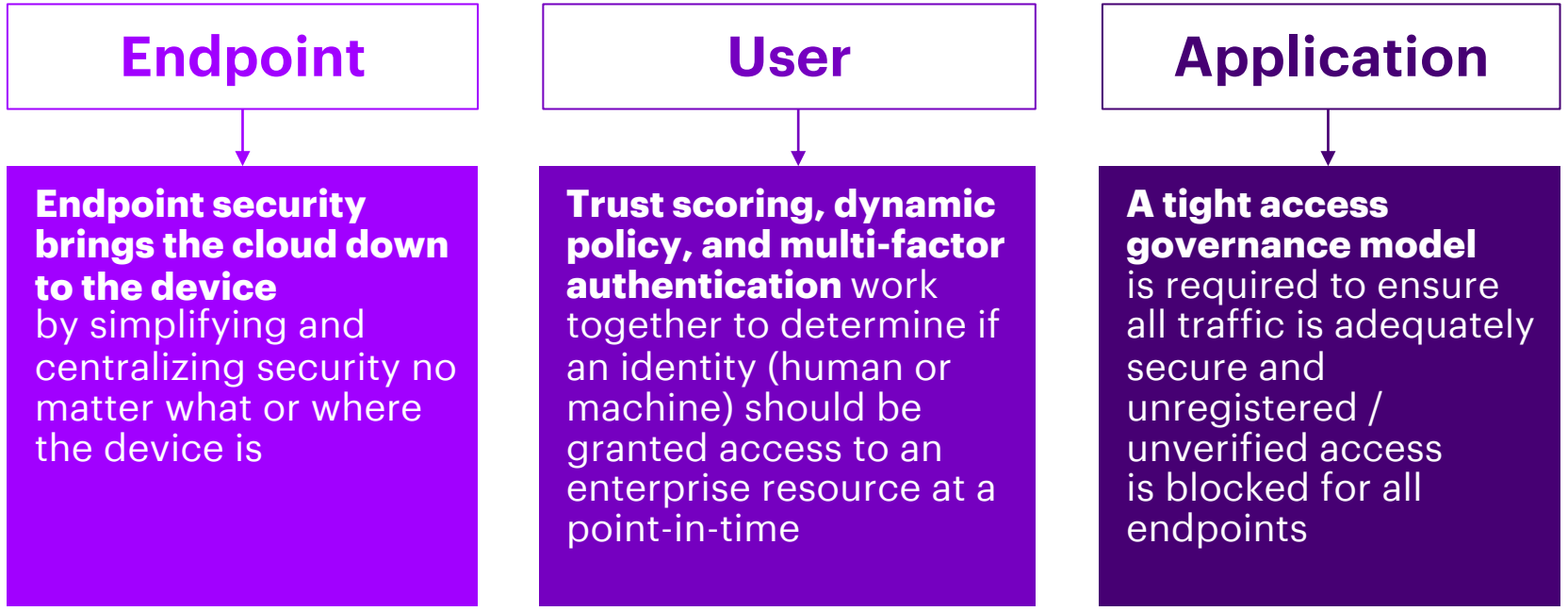
Adhere to classifications

Ensure adherence to data and system classifications as we integrate applications to foster frictionless business

Enforce controls

Enforce existing controls such as data labeling, systems authentication, data usage, disposal policies, etc.

Industry is converging around three, often highly and immediately technical, “entry point” conversations



While entirely accurate, do these talking points differentiate AFS?
What business outcomes are delivered?

The conversation framework

Customer INTO AFS

Executive Order 14024, OMB Federal Zero Trust Strategy, CISA Zero Trust Model, DoD Zero Trust Reference Architecture

Digital Transformation

Identity | Device | Network | Application / Workload | Data

AFS OUT to Customers

AFS Adaptive Security
built upon open hybrid cloud technologies

Progressive Safeguards | Risk-based Identity & Access | Dynamic Operations | Cyber-savvy Workforce

Unified strategy, technology, and operations capabilities

Accenture Federal's four focus areas align to CISA and DISA's defined zero trust strategy

Progressive safeguards

Protects high-risk, high-value targets through **intelligence, risk-based scenarios and vulnerability hunting**

Risk-based identity & access

Drives integrated and collaborative security risk management across functions

Cyber-savvy workforce

Adapts quickly and securely during disruption and change

Dynamic operations

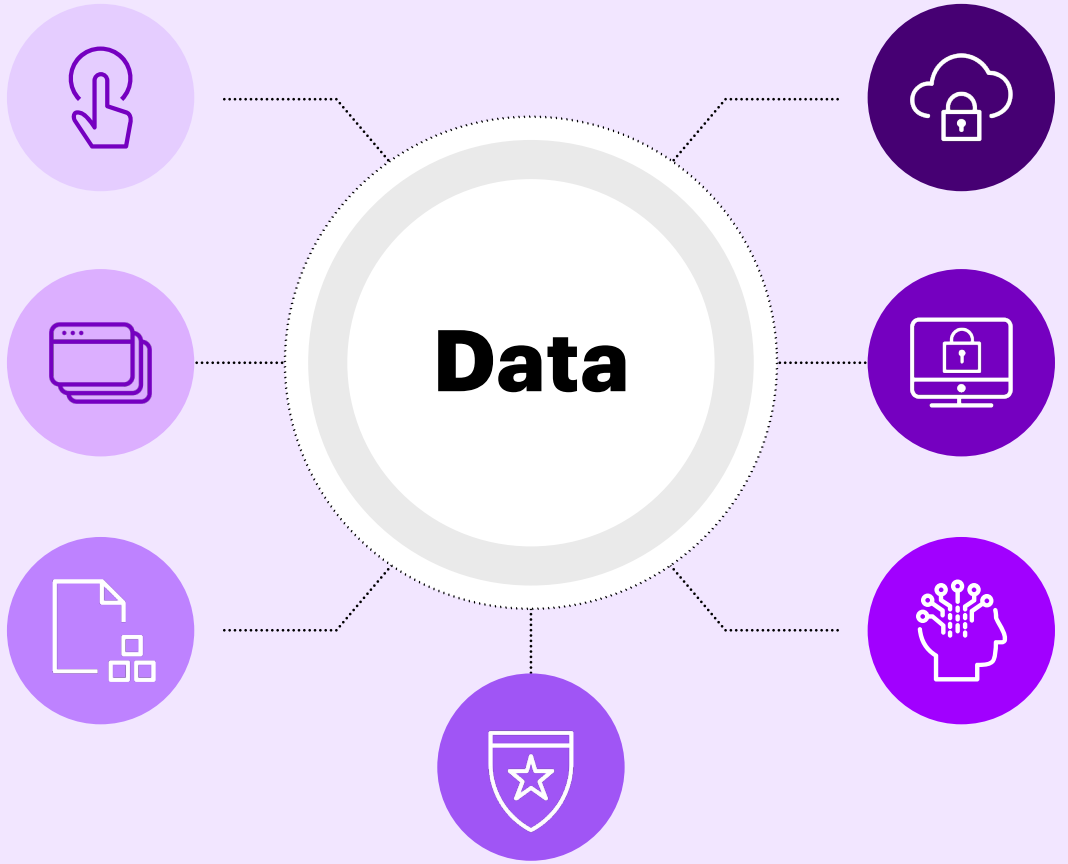
Enables independent/autonomous resiliency while reducing impacts from the unknown

Progressive safeguards are identity-driven and applied at each layer

Discoverability and governance
Automated discovery to identify managed and unmanaged endpoints, software, and network assets

Application-centric
Security designed holistically and from day one (secure from the start)

Secured templates
Secure policies tailored for re-use



Endpoint security
SASE shifts the security processing power from the device to the cloud

Passwordless and keyless
Ultimately moving to eliminate passwords and adopting fast ID online (FIDO)

Behavioral analysis
Intelligent, data-driven predictions based on patterns and anomalous behavioral detection

Quality of experience (QoE)
Delivers a good and secure user experience without hindering the QoE of the application

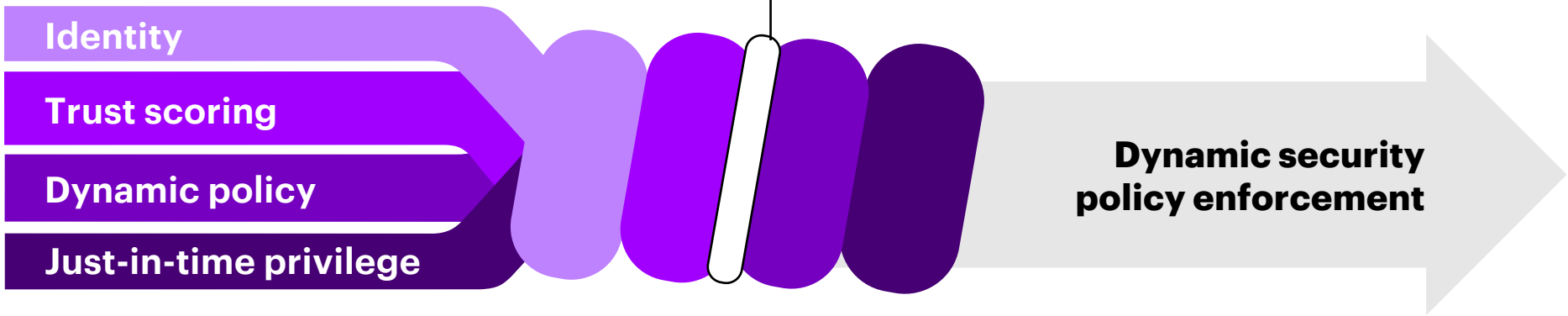
Risk-based identity & access strategy is underpinned by five functions

Identity

Is the identity allowed to authenticate?
Information that represents humans and non-humans to securely authenticate and authorize to other resources

Multi-factor authentication

Replaces passwords with strong, two-factor authentication and a user credential that is tied to the device through a PIN



Trust scoring

Should an identity be allowed access or to initiate a transaction?
Driven by the state of the identity, the profile, security posture, location, and behavior of the device, and other threat intelligence data, to establish a score

Dynamic policy

What is an identity allowed to do?
Hierarchical policies applied automatically as identities are assigned different attributes, allowing for base policies to be defined that cover a broad range of use cases

Just-in-time privilege

When should elevated rights be granted and for how long?
Elevated access rights are granted when they are needed, not simply because a given role allows it

Represents a **shift from perimeter-based data protection to identity-driven data protection**, using intelligence to classify and label data and to encrypt and restrict access based on organizational policies

Dynamic operations moves security operations to the forefront of the attack window

Fundamental philosophies

Move toward intelligent and autonomous

Detect and prevent threats, automate investigation and response

Reduce reaction time

Eliminate human intervention in the security loop as much as possible

Power our environment's security operations

Create and maintain the "Machine" or the security engine with seamless integration of capabilities in our DevSecOps journey

Make real-time decisions and adjustments

Base actions on business-defined policies, human/nonhuman identities, behavioral characteristics of devices and threats

Support with security playbooks

Supplement the security analyst with decision-making metrics to mitigate threats as they develop

Enabled by automation

Shift to "Managing the Machine" to scale, dynamically evaluate risks, and make real-time adjustments

A cyber-savvy workforce is critical, and requires a unique, domain-specific approach

Use of multiple training vehicles online courses, social engineering, and phishing attack tests are critical to success

Augment with domain-specific training to enhance security awareness for specific groups

Communicate roles to all players and empower employees to contribute to the overall security—security is everyone's responsibility

Training requires practice:

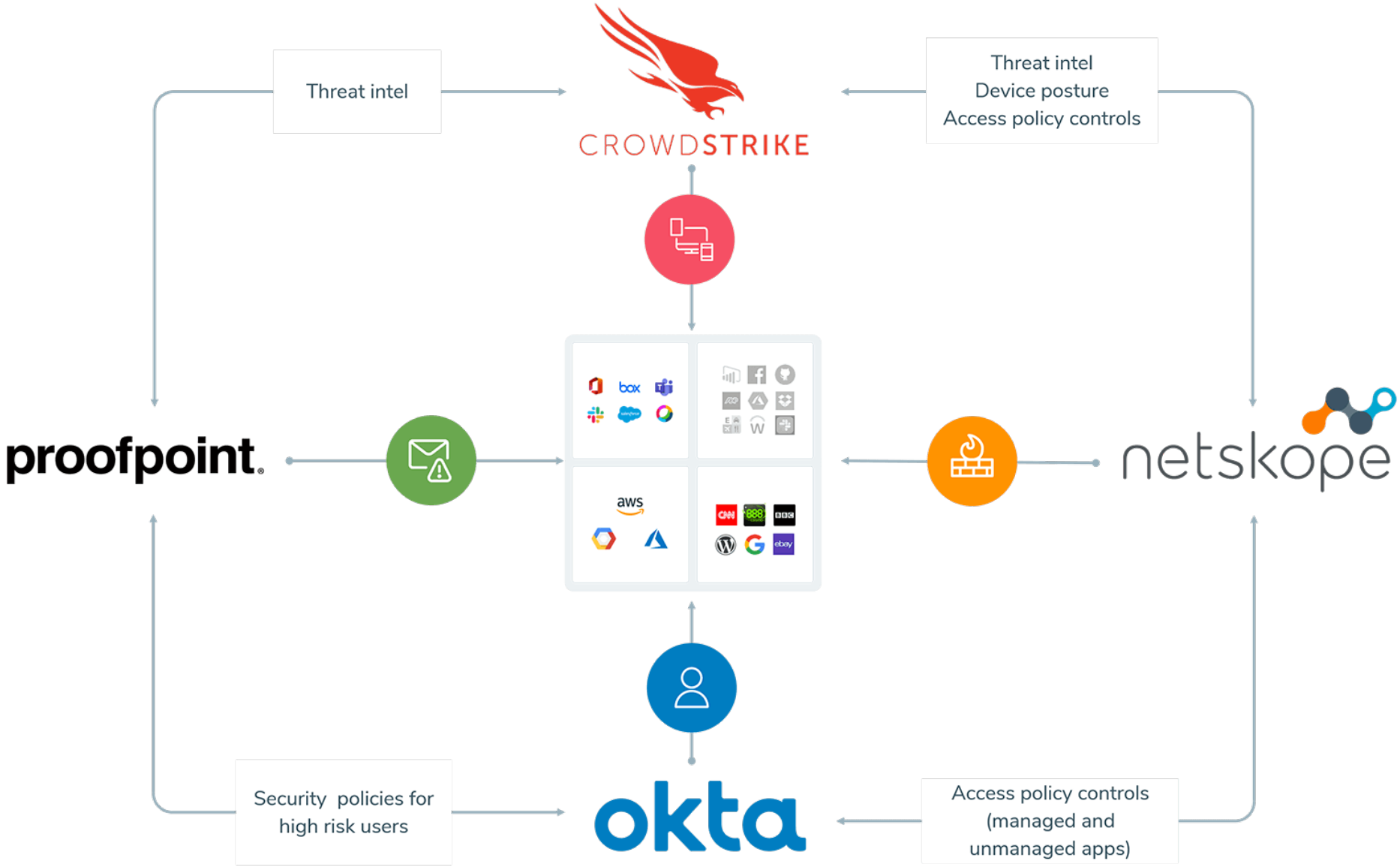
- interactive training
- simulated phishing attacks

Implement practical ways to train and hone the security skills within specific roles through real-world scenarios for both insider and outsider threats

Clear rules of the road must be created, communicated and understood by the entire organization

Accountability must be stressed at all levels and functions

Example Tech Stack



How our services align to the conversation framework

Progressive Safeguards

Protects high-risk, high-value targets through intelligence, risk-based scenarios and vulnerability hunting

Risk-based Identity & Access

Drives integrated and collaborative security risk management across functions

Dynamic Operations

Enables independent / autonomous resiliency while reducing impacts from the unknown

Cyber-savvy Workforce

Adapts quickly and securely during disruption and change

Prepare and respond to risks & threats

Security Strategy, Risk & Regulatory

- Security Strategy
- Security Program Design
- Security Training & Awareness
- Integrated Risk Management
- Industry & Regulatory Controls

Cyber Defense

- Red & Purple Teaming
- Threat Intelligence
- Threat Hunting & Incident Response
- Crisis Management
- Threat Operations Design & Build

Transform enterprise security capabilities

Identity & Access Management

- I&AM Modernization
- Identity Governance & Administration
- Access Management
- Privileged Access Management
- Cloud Infrastructure Entitlement Management

Secure Cloud & Networks

- Cloud Security Strategy & Architecture
- Secure Cloud Migration
- Secure Cloud Modernization
- Secure Network Modernization
- Edge Security

Secure Applications, Platforms & Data

- Security Testing & Vulnerability Management
- Secure Development & DevSecOps
- Data Security & Privacy
- Platform Security
- Product Security

Operational Technology Security

- OT Assessment & Strategy
- OT Security Operations Center Transformation
- OT Network & Technology Transformation
- OT Automated Asset Discovery
- OT Incident Response

Questions or comments

SHAWN WELLS

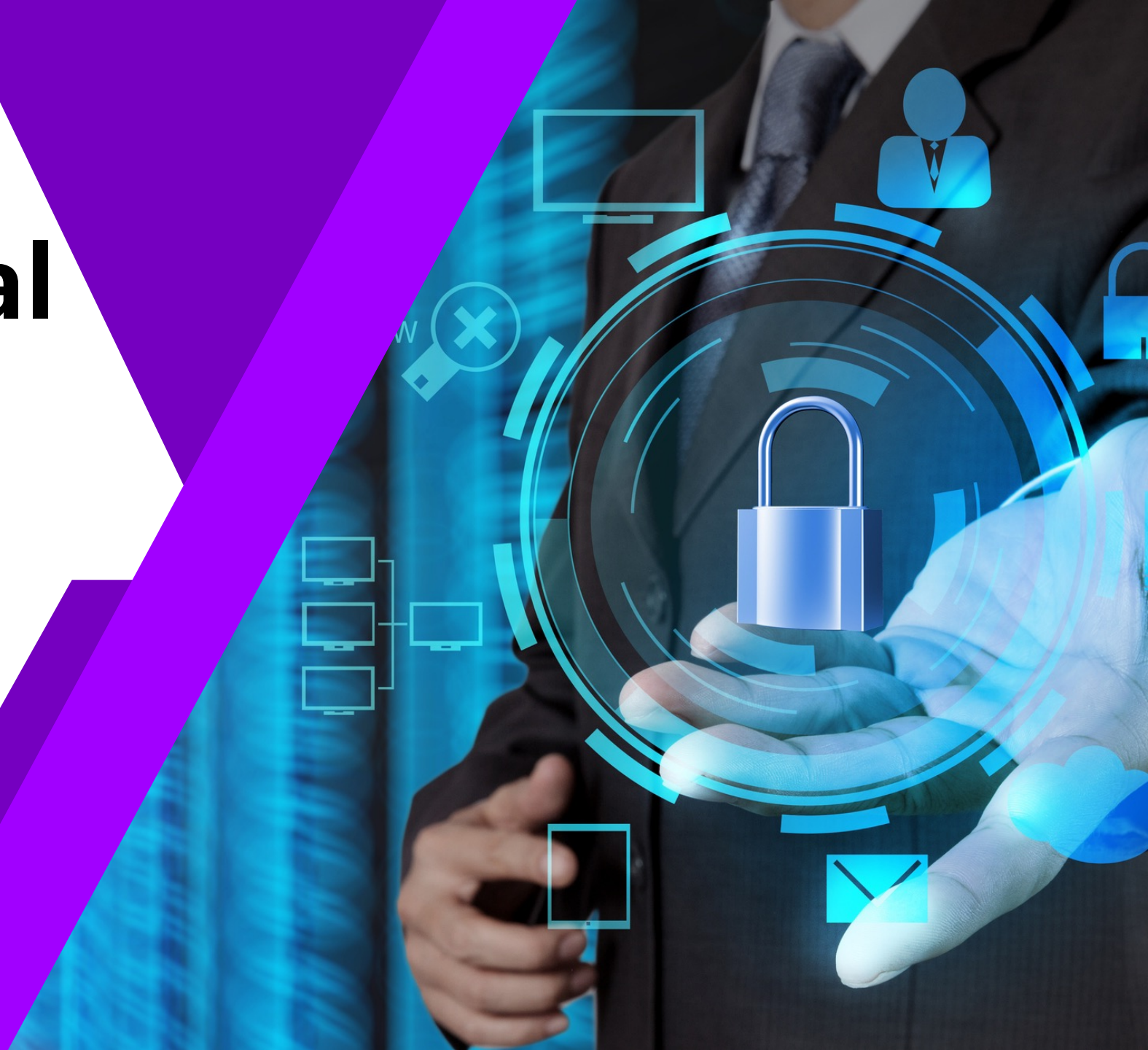
Managing Director
Cybersecurity Strategy & Technology

shawn.wells@accenturefederal.com

443-534-0130 **(Washington, D.C.)**

accenture

Supplemental



Accenture's DoD Zero Trust strategy is to fortify your cyber resilience, accelerate security innovation, and build elevated trust.

To achieve this, we will help DoD continue to **optimize against today's threats, while being adaptive** to an expanding and worsening threat landscape.

As the threat landscape continues to change and evolve, so must we.

We not only need to respond to the new threats as they emerge, but we must anticipate them.