Thank you for joining us for the first ever Identity Management Day!

Created by the Identity Defined Security Alliance.
WEBINAR
SECURE YOUR BUSINESS WITH PROPER IDENTITY MANAGEMENT

April 13 @ 2PM EST

Featuring speakers from

Federal Trade Commission
&
Identity Defined Security Alliance

HOSTED BY
NATIONAL CYBERSECURITY ALLIANCE

Register Today
https://staysafeonline.org/event/secure-your-business/
• **Convening** partners who recognize strength in the security collective

• **Educating** individuals and organizations on cybersecurity best practices

• **Amplifying** collective efforts to increase cybersecurity awareness

Follow us on Twitter @staysafeonline

Visit us online at staysafeonline.org
Thank you to our national sponsors.

**Our sponsors help us reach**

- Over 10K webinar attendees
- Over 5K workshop attendees
- Over 15K subscribers

---

2021 Sponsorships Available
info@staysafeonline.org

**Signature Sponsor**
2 slots available

**Contributing Sponsor**
3 slots available

**Affiliate Sponsor**
3 slots available

**Webinar Sponsor**
Unlimited availability
Why we are talking about Identity Management today
Our Speakers

Julie Smith
Our Speakers

Lerone Banks
What is Identity and Access Management (IAM)?

The discipline, framework, technologies, and functions to ensure only the right people can access the right resources at the right time via the right device for their approved tasks.

- Enabling users to prove they are whom they claim to be – via multiple factors, so that the compromise of one factor does not enable access
- Ensuring that users, once authenticated, can easily access the right applications and resources (SSO)
- Prevent unauthorized users from gaining access
- Implementing additional controls for privileged users (PAM)
- Ensuring that users are tightly governed in what they can access and do
- How are permissions or delegations granted or revoked?
- Detecting whether identities are being used improperly or suspiciously – and triggering additional, appropriate controls
- Looking back to review events and confirm the identity system was being used properly
- Determining what happened if it was not
- How is the identity system governed?
- How are the policies and processes of the identity system managed?
- How are new identities added or removed from the system?
What is Driving the Importance of Identity Security?

- 79% of organizations have experienced an identity-related security breach in the last two years, and 99% believe their identity-related breaches were preventable. [Identity Defined Security Alliance]

- 81% of hacking-related breaches leverage weak, stolen, or otherwise compromised credentials. [Verizon Data Breach Investigations Report]

- 74% of data breaches involve access to a privileged account. [Centrify]

- 73% of users use the same password for multiple sites, and 33% of people use the same password every time. [DigiCert]

- 81% of IT security professionals said the number of identities in their organizations has at least doubled over the past decade. [Identity Defined Security Alliance]
Mission

The Identity Defined Security Alliance is a non-profit organization that facilitates community collaboration to help organizations reduce risk by providing education, best practices and resources to implement identity centric security.

Customer Advisory Board
Identity Defined Security Framework

**Security Outcomes**
An Identity Defined Security Outcome is a desired result that improves an organization’s security posture through identity-centric security and reduces the risk of a breach or failed audit.

**Approaches**
Identity Defined Security Outcomes can be achieved through many different identity defined security implementation approaches. These approaches are well-defined patterns combining identity and security capabilities that help organizations leverage an identity context to improve security posture.

**Best Practices**
Recommendations for establishing a solid foundation and improving the effectiveness of the Identity Defined Security Approaches as organizations begin the journey to identity-centric security.
### 19 Identity-Centric Security Outcomes

(www.securityoutcomes.idsalliance.org)

**Outcomes:**

- User accounts and entitlements are granted through governance-driven provisioning
- Privileged accounts and entitlements are granted through governance-driven provisioning
- User accounts and entitlements are removed through governance-driven de-provisioning
- Privileged accounts and entitlements are removed through governance-driven de-provisioning
- Application access is transparently audited and enforced
- Device characteristics are used for authentication
- Expected user behavior is used for authentication
- All privileged access requires MFA
- Access is revoked upon detection of high-risk event associated with that identity

**Approaches:**

- 2
- 2
- 3
- 3
- 4
- 3
- 2
- 4
- 3
Best Practices
(www.idsalliance.org/best-practices/)

Recommendations for establishing a solid foundation and improving the effectiveness of the IDSA Security Outcomes as organizations begin the journey to identity-centric security.
Identity Security Advice for...

**Individuals AND Employees...**
- Think Before You Click
- Share with Care
- Practice Good Password Hygiene
- Lockdown Your Login with technology
  - Password Vaults, Multi-factor Authentication
- Get Savvy about WiFi
- Keep a Clean Machine
- Own Your Online Presence

**Organizations...**
- Ownership and Governance of Identity Management
- Unique and Single Source
- Inventory Critical Assets
- Principle of Least Privilege
- Low-hanging technology
  - SSO/Password Vaults, Multi-factor Authentication, Privileged User Vaults
- Advanced technology
  - Automated provisioning/de-provisioning, identity-centric outcomes

Security is Everyone’s Responsibility
IDENTITY MANAGEMENT FOR CONSUMER PROTECTION

Lerone Banks, PhD
April 13, 2021
Federal Trade Commission

The views expressed are those of the speaker and not necessarily those of the FTC or any one of its Commissioners
Overview

• Intro to The Federal Trade Commission (FTC)

• Experiences in (risky) identity management

• Call to Action
Identity Management

• Mindset

• Actions

• Support
Mindset

• Your organization is a tech company

• Expect vulnerabilities

• Identity management is a continuous effort
(Basic) Call to Action

• Take inventory of resources
  • People
  • Expertise
  • Technology

• Take inventory of environment
  • Data
  • Processes
  • Security Program

• Maintain identity management program
  • Documentation
  • Evaluation
  • Evolution
(Advanced) Call to Action

• Manage internal change
  • Emerging threats
  • Flexible security program

• Plan for shifting paradigms
  • Cloud
  • Remote work

• Engage Professionals
  • Intelligence
  • Services
FTC Publications

business.ftc.gov/privacy-and-security/data-security

ftc.gov/datasecurity
Federal ID Management Publications

**NIST**

**GSA**
https://playbooks.idmanagement.gov/playbooks/