servicenow



Jump-start your RMF process with ServiceNow and Okta



Digital Transformation The foundation for consumer-like services

Agenda

The Risk Management Framework Jump-start RMF with ServiceNow Okta automates RMF authorization ServiceNow and Okta in action





Digital Transformation The foundation for consumer-like services servicenow Meri Talk

...An effective enterprise risk management program promotes a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public. Such risks include, but are not limited to, strategic, market, cyber, legal, reputational, political, and a broad range of operational risks such as information security, human capital, business continuity, and related risks...

OMB Memorandum M-17-25

Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [OMB M-17-25]

Digital Transformation The foundation for consumer-like services

The RMF process



FIPS 199 / SP 800-60 Starting Point SP 800.37 / Sp 800.137 / 41P5 200 | SP 800-53 Categorize System Monitor Select Controls Controls **Organization-wide Risk Management** SP 800-39 lions Implement System Controls SP 800-51 Assess Controls SP 800-53A

Source: BAP

Digital Transformation The foundation for consumer-like services

Respond faster to security incidents, vulnerabilities, and enterprise risk



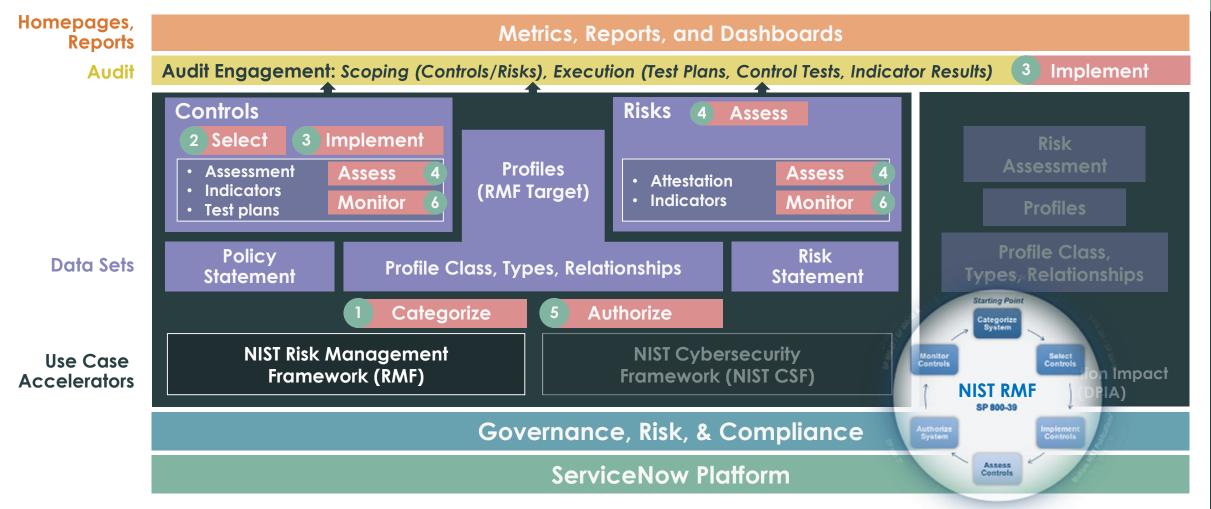
servicenow MeriTalk



Digital Transformation The foundation for consumer-like services servicenow Mei

Merilalk

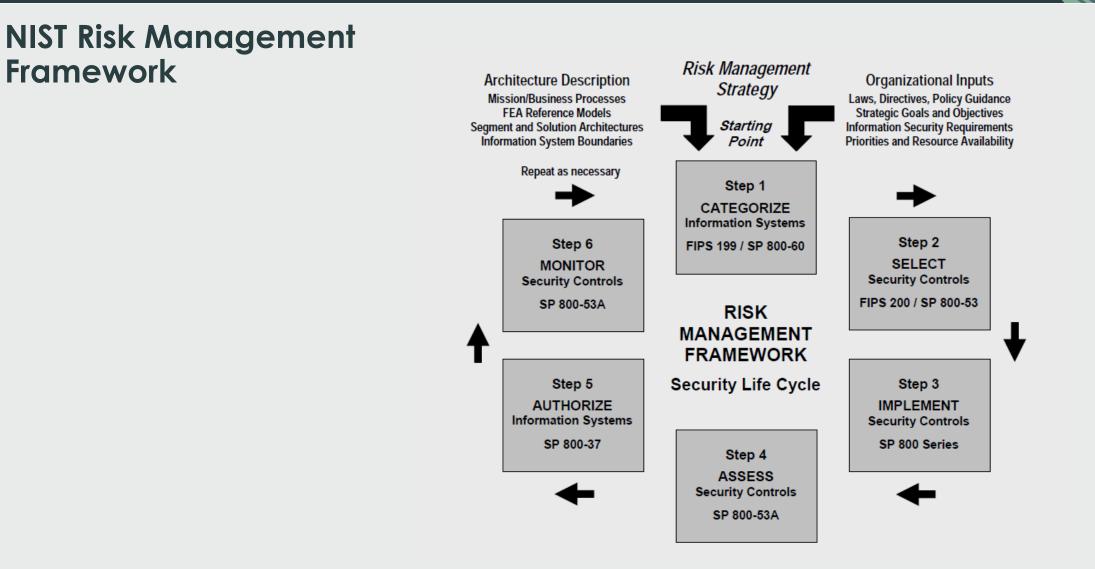
NIST RMF Use Case Accelerator on ServiceNow GRC



Digital Transformation The foundation for consumer-like services

servicenow

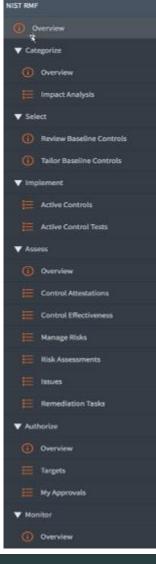




Digital Transformation The foundation for consumer-like services

RMF Use Case Accelerator

- Policies
- Controls
- Assessments/Attestations
- Risks
- Issues
- Remediation tasks
- Test plans
- Dashboard





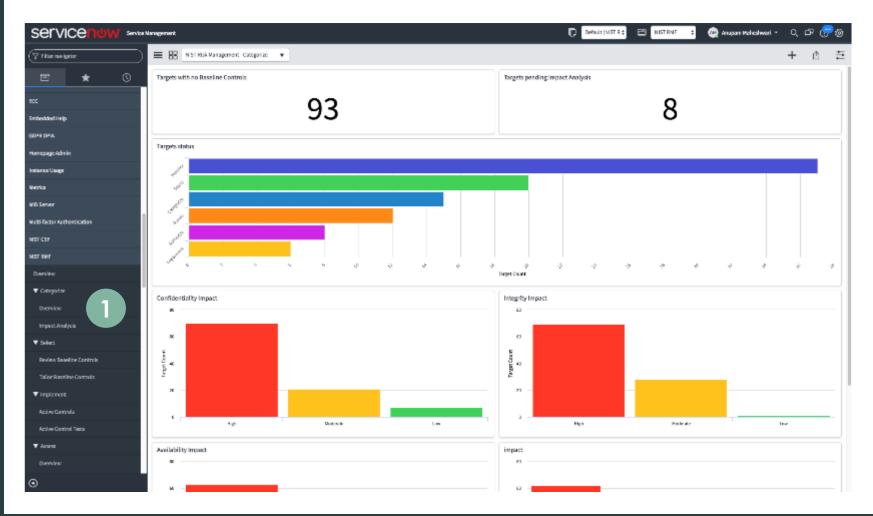
© 2019 ServiceNow, Inc. All Rights Reserved. Confidential.

Digital Transformation

The foundation for consumer-like services

servicenow | Meri Talk

Step 1: Categorize Information Systems



- For the information systems, assess the criticality of the assets and potential adverse impact to business from any state changes
- Use Confidentiality, Integrity and Availability factors in the assessment.
- Based on this criticality identify the <u>assets that</u> <u>are most critical and</u> <u>represents the high risk.</u>

Digital Transformation

The foundation for consumer-like services

Step 2: Select baseline controls

					Default (Global #	Globel	🔹 🅘 System	Administrator	< ଟ	0 🕸
(♥ HHF (8) <	Target MIST - Develop and manage enterprise-wide knowledge management (KM) (apability (Mist RMP Targets view)						Ø	🛻 eeo Updata	Request Approval	Delete	$\uparrow ~ \downarrow$
0 * 3	* Name	NIST - Develop and manage enterprise-wide kno	owied			Active					
E Active Controls	* Owned by	Security Officer (IMF)	۹	۲		Profile	NIST - Sub Process	Develop and manage o	ter 9, 🛞		
E Active Control Tests	Description										
V Assess	Francovork	A NIST CSF, NIST RMF									
Overview	IST CSF Assessment										
E Control Attestations			_	1							
E Control Effectiveness	RMF State	Implement	-								
💭 Marage Riska	Confidentiality	Moderate	0		h	mpact	Moderate		0		
📰 Risk Assessments	Integrity	Moderate	0								
Extension and a second	Availability	Hoderate	0								
📻 Remediation Tasks	Scoping Considerations	8									
▼ Authorize	Risk Decutive	Risk Executive (RMP)	Q,	0	Approval 5	Status	Not Requested				
() Destriew	+ Authorizing Official	Authorizing Official (1942)	Q,	0							
🗮 Targeta	Justification										
🗮 Wy Approvals											
▼ Monitor Update S	lequest Approval Delete										
Overview				1							
indicators		ntrols Risks Approvals Activities Assess	sments								
▼ Administration	re Policy Statements Go to N	ane 🔻 Search					44 4	1 to 100 c	f 252 🕨	••	
O dwices	Sutements				-				-		
E Assessment Types	Access Control For Gutput D		≡ Category (empty)	= Comps	ance Score Percentage		 Impact Moderate, Hig 	h			
E Attestation Types	Reportion Of Partice			(enst)	🛎 7. Moderata Mich						

 Select the baseline security controls based on the criticality of the assets, apply tailoring guidance based on the context and identify supplemental controls if required.

servicenow

Meri Talk

Digital Transformation

The foundation for consumer-like services

Step 3: Implement controls

				al Hard Fair Marker	 Funds 						- A . d.d.		
7 filter navigeter -		Controls ()	NET RMF Controls vie	w] New Gate Number	♥ Search						-∿ - ••	< _ 1 to	Sofi 🕨 🕨
0 ★ 🖻				ment Source = MIST 600-53-04		_	_	_	_		_	_	_
пана ани р	-	۹	≡ Mumber	≡ Neme	≡ Profile	≡ Cwmer	≡ Status	≡ Family	≡ Common	≡ Compensating	≡ Supplemental	≡ Assurance	≡ Source
PROPIA		_	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	=N ST 800-53
nəpəgə Admin		0	CTRL0021621	Configuration Management Policy And Proc	NIST_ODDTAM	Security Officer (RMF)		(angty)	true	true	true .	true	NIST 800-53 r4
ance Usage		(i)	CTRL0021618	Configuration Management Policy And Proc	NIST_OreCSM	Security Officer (RMF)	Non Compliant	(ongty)	true	false	false	true	MIST 800-63 r4
ia		(i)	CTRL0020678	Cross Organizational Auditing	NIST - Acree Corporation	Risk Executive (RMF)		(engty)	true	false	true .	faise	NIST 800-53 r4
Server		0	CTRL0020871	Information Exchange	NIST - Sub Process - Maintain productive 35595	Security Officer (RMF)		(engty)	faise	false	false	faise	NIST 800-53 r4
1 63#		(i)	CTRL0020961	Information Exchange	NIST - Sub Process - Plan and manage outtomer service contacts	Security Officer (RMF)		longty)	faise	false	false	faise	NIST 800-53 r4
TRNP		٥	CTRL0020736	Histion/Business Process Definition	NIST - Hanage Customer Service	Security Officer (RMF)		lengty)	faise	true	false	faise	NIST 800-53 r4
vorview		(i)	CTRL0020705	Histion/Business Process Definition	NIST - Acquire, Construct, and Manage Assets	Security Officer (RMF)	Non Compliant	(engty)	true	true	false	faise	NIST 800-53-r4
Categoriae Overview		0	CTRL0021899	Process integration	NIST - Americas - Sub Org	Security Officer (RMF)		(empty)	faise	false	false	true	NIST 800-53-r4
impact Analysis	0	Actions o	r selected rows t								44	4 1 2	sora 🕨 🌬
Select	-		,										
													Ċ
Review Baseline Controls													
implement													
Active Controls													
Active Control Tests													
Amen													
Overview													

servicenow MeriTalk

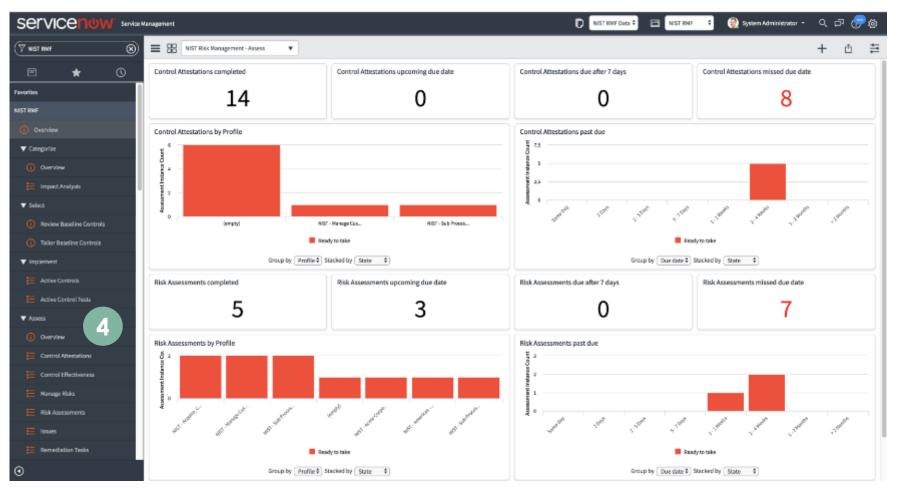
 Implement the controls for the identified assets within the enterprise architecture; use management discretion to apply security configurations settings on controls.

Digital Transformation

The foundation for consumer-like services

servicenow Merilak

Step 4(a): Controls owners perform attestation of controls

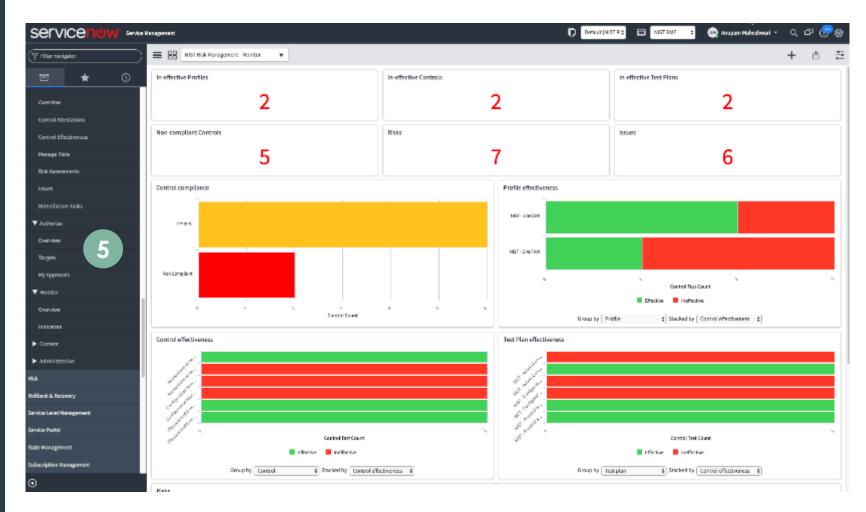


- Trigger attestation to control owners to ensure controls are implemente for the respective information assets and ask for evidence.
- In case of noncompliance, trigger an issue to ensure remediation is done and controls are implemented on priority.

Digital Transformation

The foundation for consumer-like services

Step 5: Authorize



- Ensure all activities such as risk assessment, control testing and issues are reviewed by management.
- If acceptable, authorize operations.

Digital Transformation

The foundation for consumer-like services

Step 6: Monitor

Servicendw service	lanagement				Default (Global #	Global	🔹 👰 System/	dministrator A.	ଏଟ (D 🕸
(7 m= 🛞	< Target NST - Develop and manage enterpris	e-wide knowledge managament (KM) capability (Ni		Ø	ere Updata	Request Approval	Deiete	$\uparrow \downarrow$		
= ★ ©	* Name	NIST - Develop and manage enterprise-wide know	wied,		Adžve					
Active Controls	* Owned by	Security Officer (IMF)	۹		Profile	NIST - Sub Process -	Develop and manage ent	er 9, 10		
Active Control Tests	Description									
▼ Anten	Surrent .	A NIST CSF, NIST RXF								
Overview	Framework	MIST CSF, NIST HAP								
Control Attestations	NIST RNF NIST CSF Assessment									_
Control Effectiveness	RMF State	Implement	0							
🗮 Marage Risks	Confidentiality	Noderate	0		Impact	Moderate		0		
🗮 Risk Assessments	Integrity	Noderate	0							
🗮 issues	Availability	Noderate	٥							
E Remediation Tasks	Scoping Considerations	8								
▼ Authorize	Risk Executive	Risk Executive (RMP)	۹ (6	Þ	Approval Status	Not Requested				
() Overview	* Authorizing Official	Authorizing Official (094P)	۹ ()	D .						
🗮 Targets	Justification									
🗮 My Approvals										
▼ Wonitisr	Update Request Approval Delete									
Overview										
🗮 indicators		trois Risks Approvais Activities Assessm	nents							
▼ Administration	Baseline Policy Statements Go to Na	ne Y Search					44 4	1 to 100	of 262 🕨 🖡	
() Choices	Policy Statements									
Assessment Types	Q ≡ Norre				ance Score Percentage		≡ impact			
Attestation Types	Access Control For Output De	5005			(empty)			 G Moderate, Hij 		
	C Secondary Of Defer				(amendu)			· 7 Moderato His		



- Setup indicators for continuous monitoring of the risks and controls.
- Monitor the overall risk profile for the information assets through reports on dashboard.

Digital Transformation The foundation for consumer-like services servicenow MeriTalk



servicenow

Digital Transformation The foundation for consumer-like services servicenow Merilalk



okta + servicenow

Digital Transformation The foundation for consumer-like services

Here's the problem...

Managing user onboarding and off boarding, and application permissions is a time consuming activity that if not automated and orchestrated delays RMF authorization, thus delaying value activation by agency enterprise.

We have the answer...

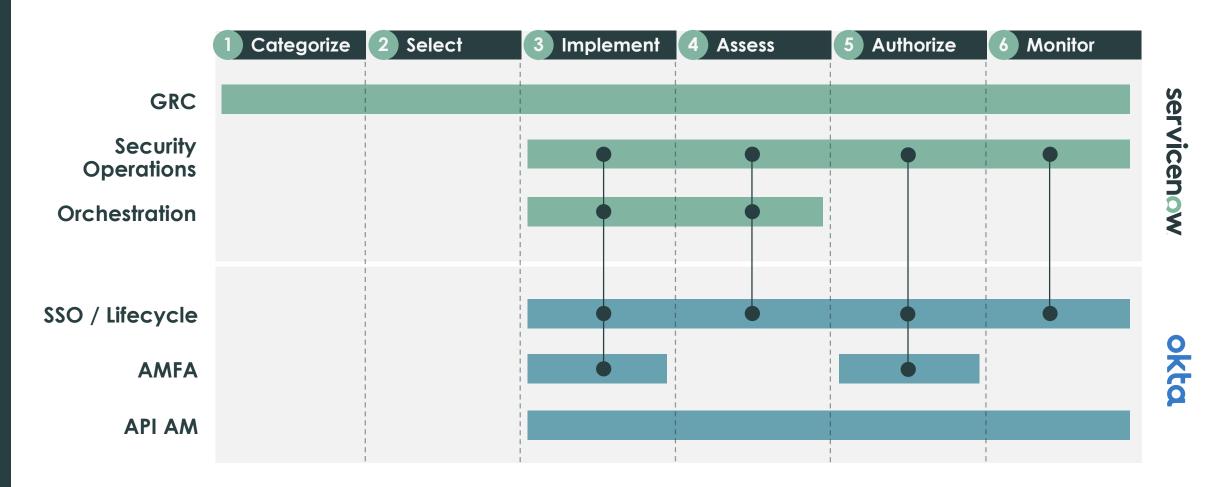
servicenow

Meri Talk

Digital Transformation The foundation for consumer-like services servicenow Me

MeriTalk

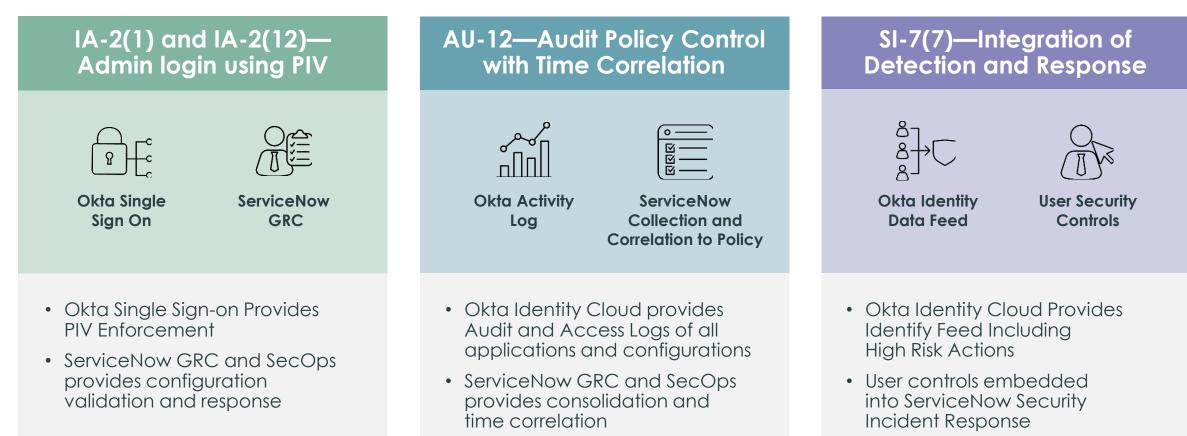
RMF and speed of value delivery



Digital Transformation The foundation for consumer-like services servicenow MeriTalk

S.

NIST 800-53v4 RMF Control sample use cases



Servicenow federal summit servicenow Merilian Digital Transformation The foundation for consumer-like services

Okta + ServiceNow Integration Portfolio



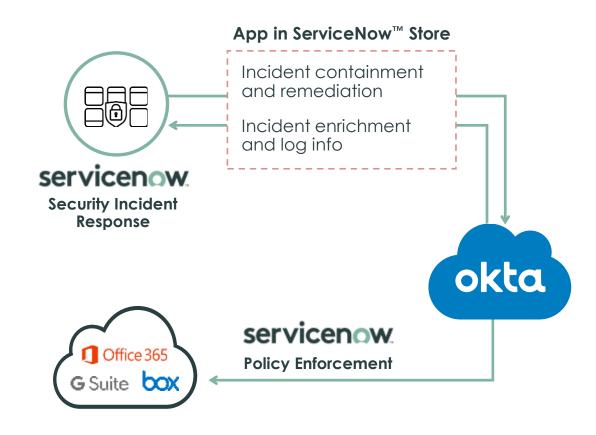
servicenow federal summit servicenow **Meri** Talk **Digital Transformation** The foundation for consumer-like services Security ecosystem Detection SIEM paloalto splunk> Orchestration TANIUM" Radar amazon webservices" CMDB Workflows **Automation** ArcSight X **Symantec** McAfee Virustotal 🗇 **vm**ware[.] servicenow 🔄 Check Poinť Azure ssh **Vulnerability Threat Intelligence Post Incident Review IT Connection** okta QUALYS" STIX CROWDSTRIKE Identity CARBON RAPID BLACK elastic • User lifecycle tenable Recorded Future Strong authentication okta Multi-factor authentication Network/device/app policies

Logos are trademarks or registered trademarks of their respective owners and not ServiceNow

Digital Transformation The foundation for consumer-like services servicenow Meri Talk

Okta Identity Cloud for Security Operations

Automatic User enrichment and Identity controls for Security Incident Response



Improve risk scoring; Reduce incident triage time

Add user context to active incidents

- Applications Provisioned
- Group Memberships
- Recent user activity (logins, etc)

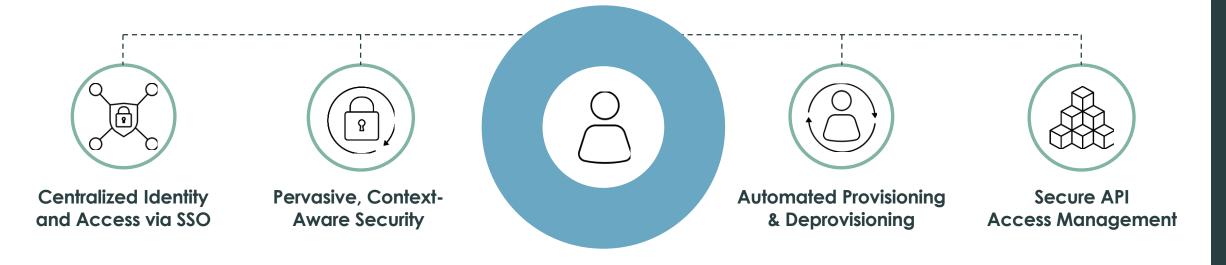
Accelerate incident containment

Provide contextual user controls directly within incidents in ServiceNow

- Clear active sessions
- Suspend / Unsuspend user
- Change / Add / Remove application access
- Change / Add / Remove group membership
- Force expire password, MFA token

Digital Transformation The foundation for consumer-like services servicenow Meri Talk

Okta is the foundation for Zero Trust security





Demo

Identifying the business risk of unauthorized access with ServiceNow and Okta



servicenow Meri







Thank you

Contact info?

