Building a Strong Cybersecurity Program during IT Transformation in the Banking Sector

Milano 24 marzo 2022

Banks need to

their customer interaction

Banks need to

evolve

their customer interaction

Banks need to

evolve

their customer interaction

Banks need to

evolve

their customer interaction

Banks need to

evolve

their customer interaction

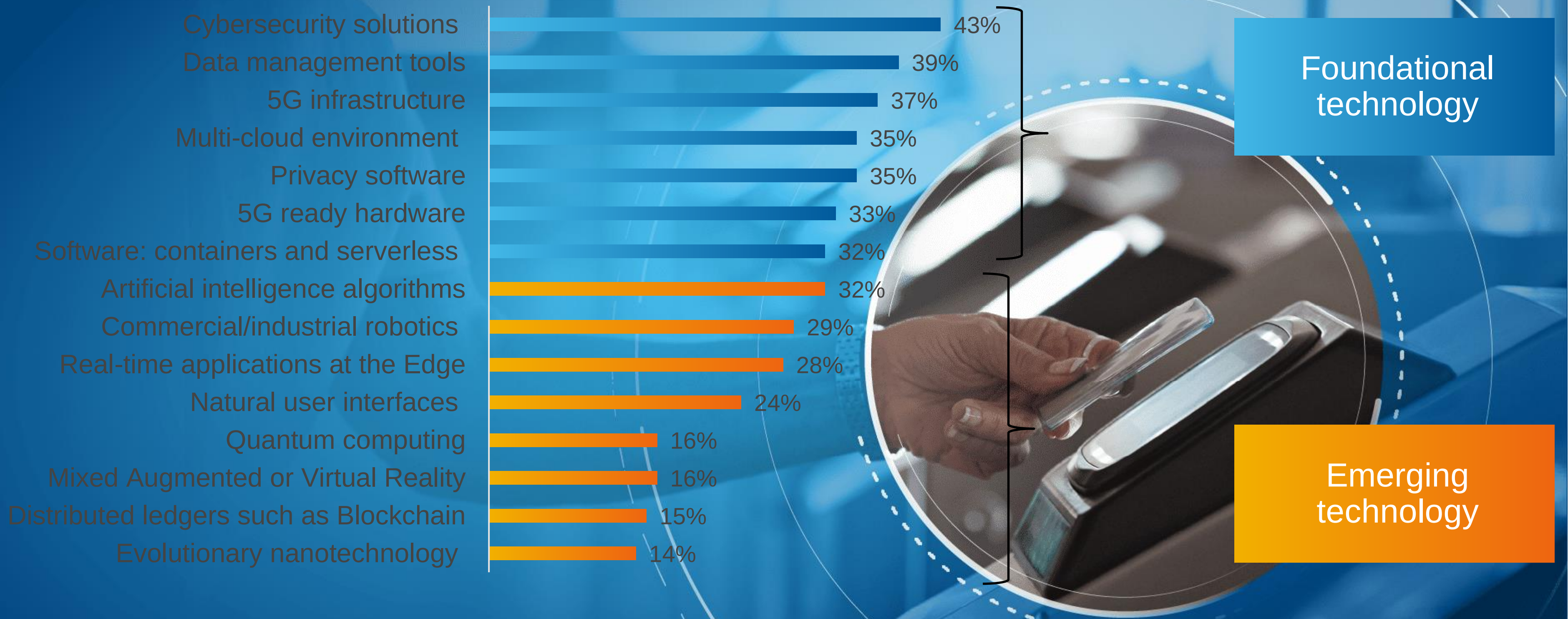
The need for financial services will never go away. In fact, banking will be needed more than ever before.

Going forward, we would need more banking embedded in our lives to give us what we want, when and where we need it.

We need to adopt the API-First mindset and embedded in all the potential applications and customer experiences that need banking.

Banks won’t be able to attract all users on their digital channels – the only way to reach them is to be embedded in others’ applications.

Overall planned IT investments over the next 1-3 years



Design Principles for Security

Implement a strong identity foundation

Enable traceability

Apply security at all layers

Automate security best practices

Protect data in transit and at rest

Keep people away from data

Prepare for security events

Remediation:

-Encryption at rest and in transit

-Keep up to date with security threats and remediations, automate security checks

Design Principles for Reliability

Test recover procedures

Automatically recover form failure

Scale horizontally to increase aggregate system availability

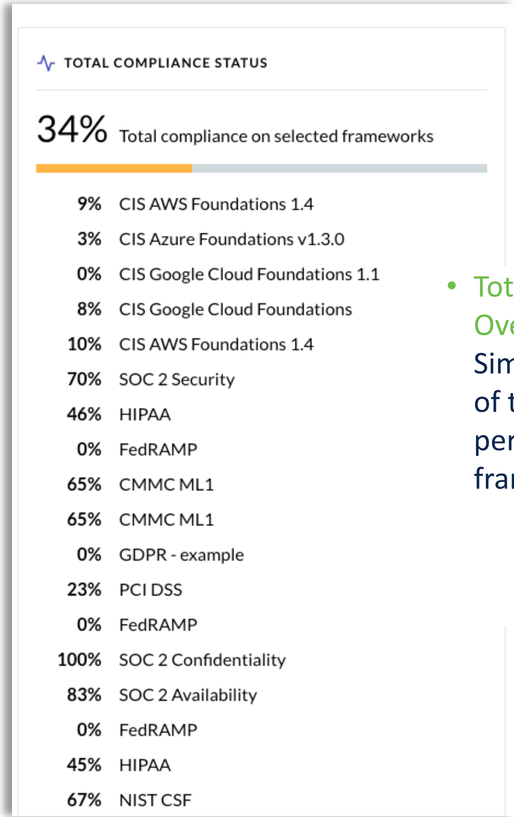
Stop guessing capacity

Manage change automation

Remediation:

- Backup strategy
- Test reliability
- Create and test DR

Compliance Status Overview

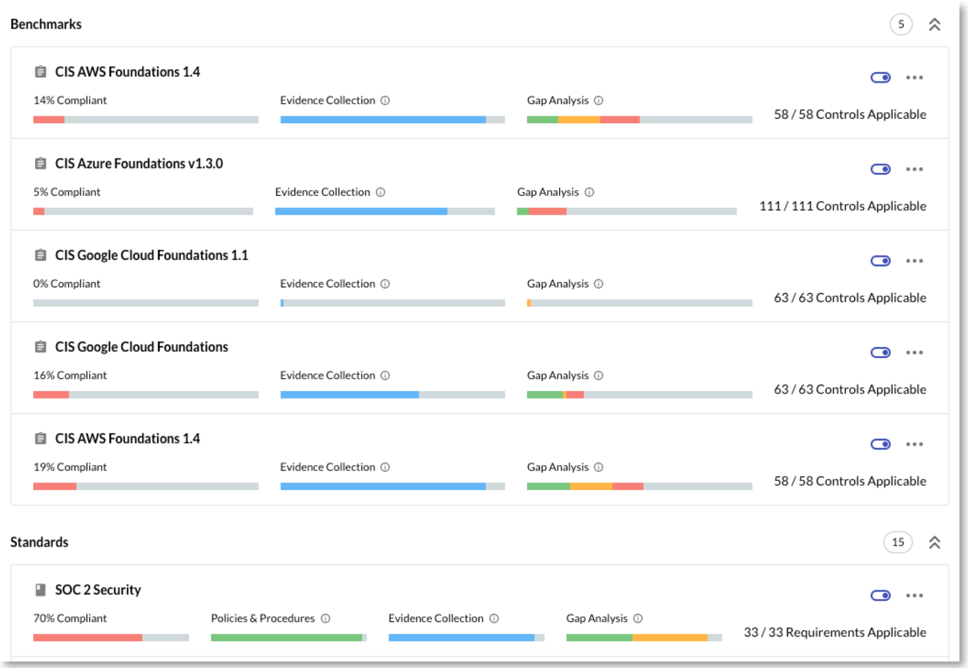


TOTAL COMPLIANCE STATUS

34% Total compliance on selected frameworks

9%	CIS AWS Foundations 1.4
3%	CIS Azure Foundations v1.3.0
0%	CIS Google Cloud Foundations 1.1
8%	CIS Google Cloud Foundations
10%	CIS AWS Foundations 1.4
70%	SOC 2 Security
46%	HIPAA
0%	FedRAMP
65%	CMMC ML1
65%	CMMC ML1
0%	GDPR - example
23%	PCI DSS
0%	FedRAMP
100%	SOC 2 Confidentiality
83%	SOC 2 Availability
0%	FedRAMP
45%	HIPAA
67%	NIST CSF

- **Total Compliance Overview**
  Simple compliance view of the environment and per adopted standard, framework or benchmark



Benchmarks 5

CIS AWS Foundations 1.4
14% Compliant — Evidence Collection ⓘ — Gap Analysis ⓘ — 58 / 58 Controls Applicable

CIS Azure Foundations v1.3.0
5% Compliant — Evidence Collection ⓘ — Gap Analysis ⓘ — 111 / 111 Controls Applicable

CIS Google Cloud Foundations 1.1
0% Compliant — Evidence Collection ⓘ — Gap Analysis ⓘ — 63 / 63 Controls Applicable

CIS Google Cloud Foundations
16% Compliant — Evidence Collection ⓘ — Gap Analysis ⓘ — 63 / 63 Controls Applicable

CIS AWS Foundations 1.4
19% Compliant — Evidence Collection ⓘ — Gap Analysis ⓘ — 58 / 58 Controls Applicable

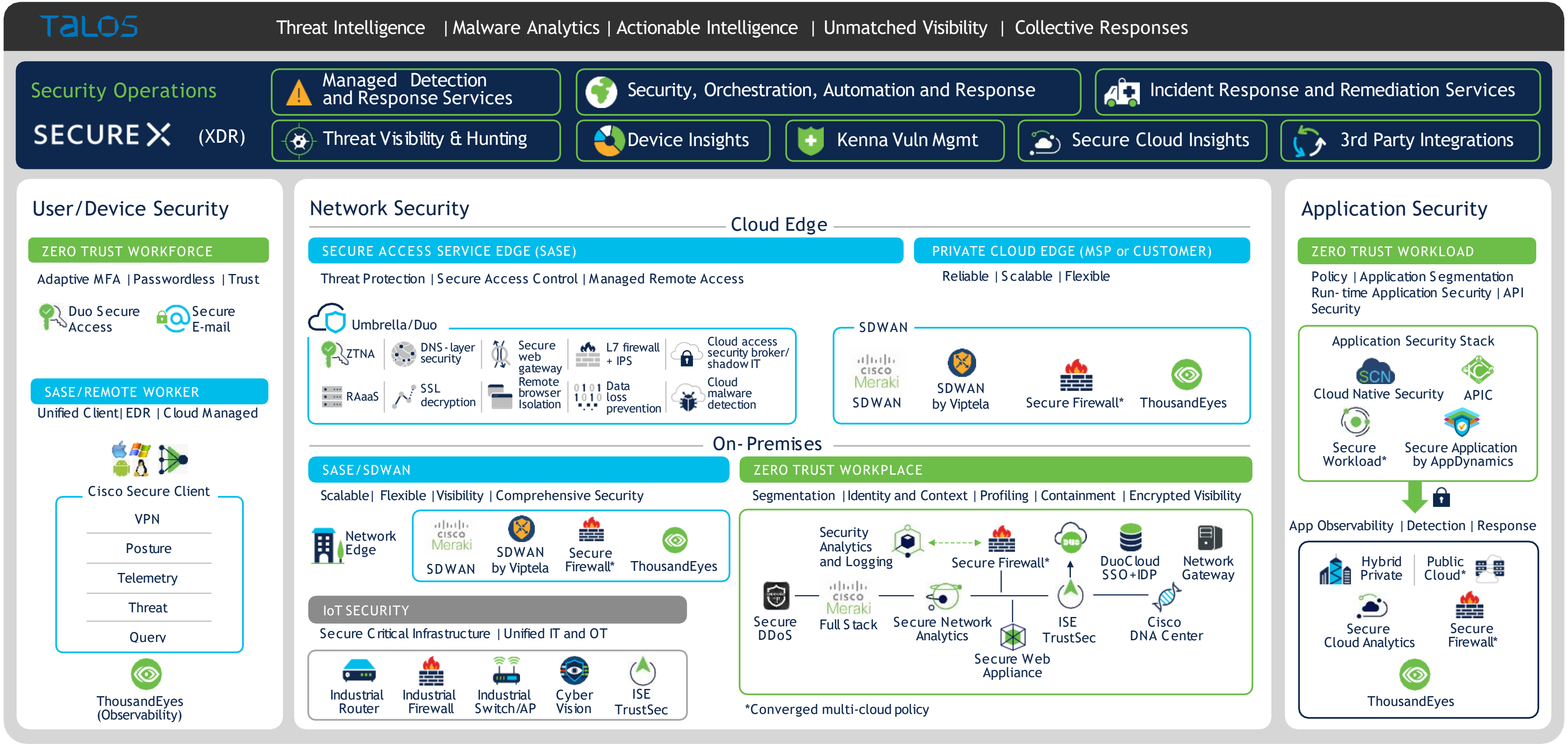
Standards 15

SOC 2 Security
70% Compliant — Policies & Procedures ⓘ — Evidence Collection ⓘ — Gap Analysis ⓘ — 33 / 33 Requirements Applicable

- **Per Framework View**
  Simplified per framework compliance view

CISCO SECURE

Reference Security Architecture v2.0



TALOS Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECUREX (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client| EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Observability)

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo

ZTNA, DNS-layer security, Secure web gateway, L7 firewall + IPS, Cloud access security broker/ shadow IT, RAaaS, SSL decryption, Remote browser Isolation, Data loss prevention, Cloud malware detection

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

SDWAN

Cisco Meraki SDWAN, SDWAN by Viptela, Secure Firewall*, ThousandEyes

On-Premises

SASE/SDWAN

Scalable| Flexible |Visibility | Comprehensive Security

Network Edge

Cisco Meraki SDWAN, SDWAN by Viptela, Secure Firewall*, ThousandEyes

IoT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router, Industrial Firewall, Industrial Switch/AP, Cyber Vision, ISE TrustSec

ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

Security Analytics and Logging, Secure Firewall*, DuoCloud SSO+IDP, Network Gateway, Secure DDoS, Cisco Meraki Full Stack, Secure Network Analytics, ISE TrustSec, Cisco DNA Center, Secure Web Appliance

*Converged multi-cloud policy

Application Security

ZERO TRUST WORKLOAD

Policy | Application Segmentation
Run-time Application Security | API Security

Application Security Stack

Cloud Native Security, APIC, Secure Workload*, Secure Application by AppDynamics

App Observability | Detection | Response

Hybrid Private, Public Cloud*, Secure Cloud Analytics, Secure Firewall*, ThousandEyes