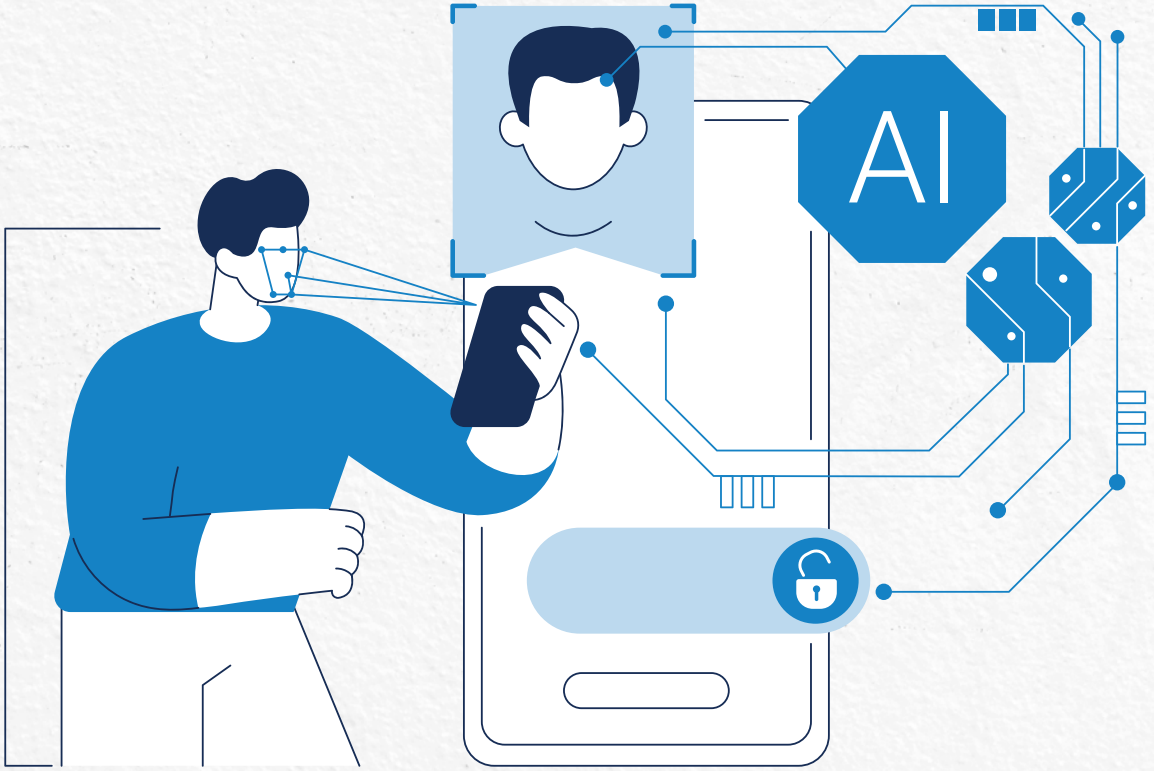
Stay Ahead of Threats with AI-powered Identity Security

A Guide To Securing Your Workforce and Customer Identity

Deepali Sathe, Senior Industry Analyst, Frost & Sullivan
Swetha Krishnamoorthi, Industry Principal, Frost & Sullivan

FROST & SULLIVAN VBOOK

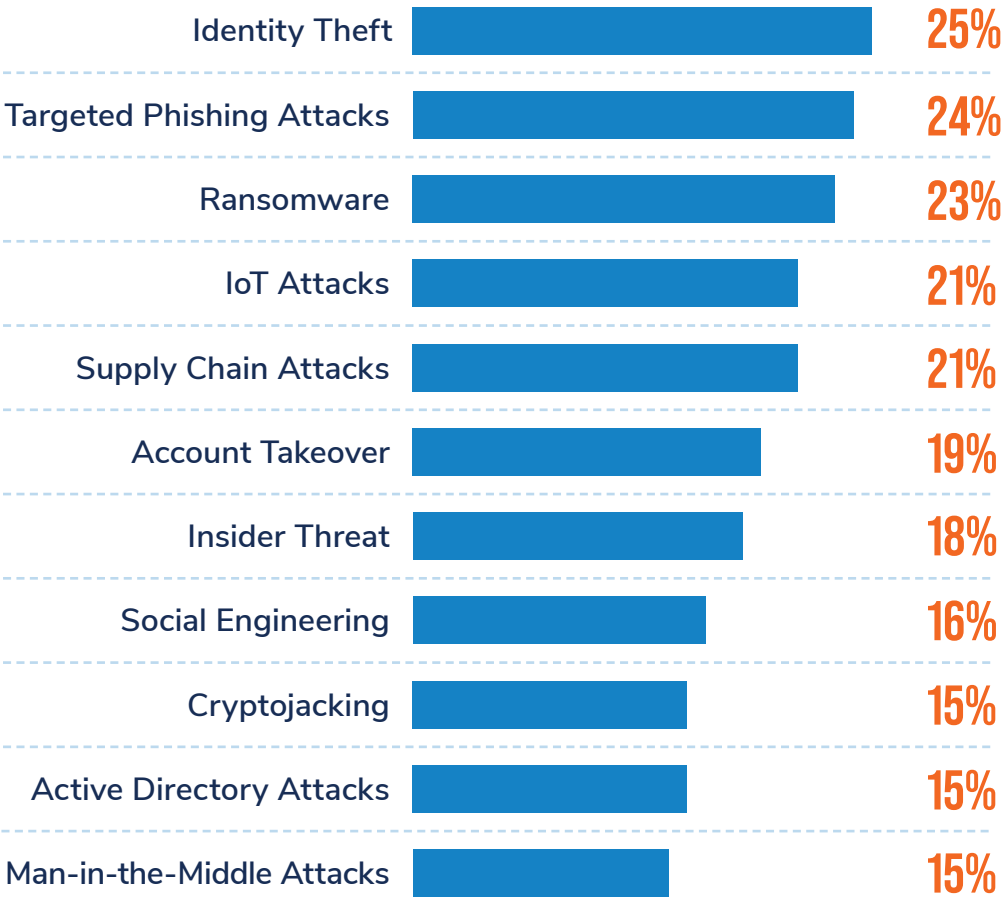
CONTENTS



Growing Volume of Cyberattacks

- **Microsoft, MGM Casino, Fidelity National Financial**—A common thread connecting these three brands is sophisticated cyberattacks that leveraged compromised credentials. While the Microsoft data breach compromised senior leadership emails, the attack on Fidelity National Financial compromised the data of over 1.3 million customers. Similarly, cyber adversaries leveraged the compromised credentials of an employee to disrupt operations, leading to a loss of about $100 million.
- **Over 73% of security practitioners** surveyed as part of Frost & Sullivan's Voice of the Enterprise Security Customer Survey claimed that their organizations faced more than ten successful attacks over the last 12 months. Identity theft and targeted phishing attacks were the biggest cybersecurity concerns for organizations.
- **Credential theft/misuse and identity compromise** play significant roles in enabling cyber adversaries to access the active directory (AD) and, eventually, attack critical assets.

Major Cybersecurity Concerns of Organizations, Global, 2023



Source: Frost & Sullivan 2023 Voice of the Enterprise Security Customer Study; Base: All respondents (n=2,448)
Q10. What are the main cybersecurity concerns of your organization? Please select all that apply.

Identity: A Unifying Thread across Most Sophisticated Cyberattacks

- Compromised identities play a crucial role at different stages of the attack life cycle—be it at the entry point, for privilege escalation, lateral movement, or even for data exfiltration. User credential theft, use of expired digital certificates that secure devices, phishing attacks, misuse of privileges, and social engineering are some tactics, techniques, and procedures (TTPs) cyber adversaries use. These are related to enterprise-wide identities, including user and machine identities.
- Digital transformation expanded the attack surface beyond the network perimeter. Identity has become the new perimeter as organizations embrace remote and hybrid work arrangements, extensively deploy cloud-based applications, and use multiple devices, critical infrastructure, and assets.

Identity's Journey through the Attack Life Cycle

RECONNAISSANCE
Cyber adversaries leverage social engineering techniques and stolen credentials to gather intelligence about an employee or user.

WEAPONIZATION
The intelligence gathered from the compromised identity is used to craft a convincing spear phishing email with malicious links.

DELIVERY
The cyber adversary sends the phishing email from the compromised user's mailbox, thereby increasing the chances of recipients opening the mail.

EXPLOITATION
Once the phishing email is opened, the malware exploits vulnerabilities in the target system.

INSTALLATION
The compromised identity allows the adversary to escalate privileges and install additional tools, such as keyloggers.

COMMAND AND CONTROL
The adversary leverages the stolen credentials to log into systems, issue commands, exfiltrate data, or even evade detection by blending in with legitimate user activity.

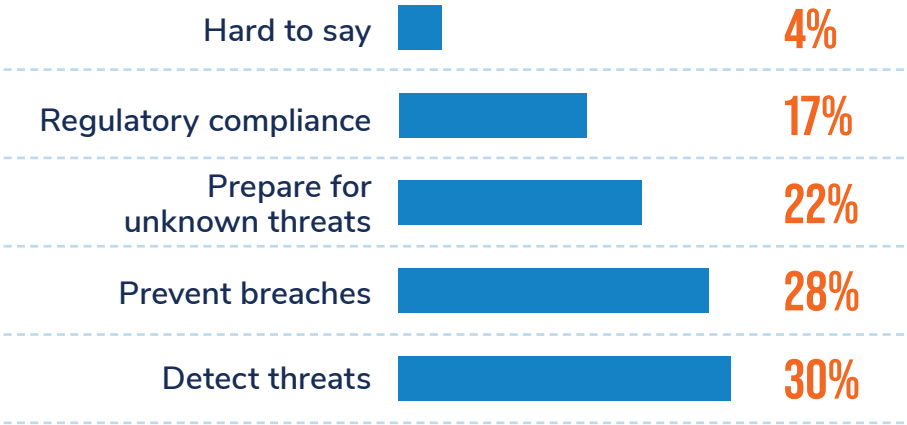
ACTIONS ON OBJECTIVES
The adversary leverages the compromised user's identity to remain hidden while exfiltrating data, conducting financial fraud, or disrupting operations.

Source: Frost & Sullivan

Identity-Centric Security Is Essential for Zero Trust Framework

- Securing all human and non-human identities is vital to ensuring end-to-end enterprise security.
- Once breached, bad actors can move laterally inside the network to quickly access critical systems and data.
- The zero trust framework, built on "never trust, always verify" and "assume breach," recommends strict verification and authentication for all internal and external access requests.
- High-assurance identity security with step-up and certification-based authentication for users and devices enhances secure access.
- CISOs must balance compliance, security, and user experience (UX).

Frost & Sullivan's Voice of the Enterprise Security Customer Survey



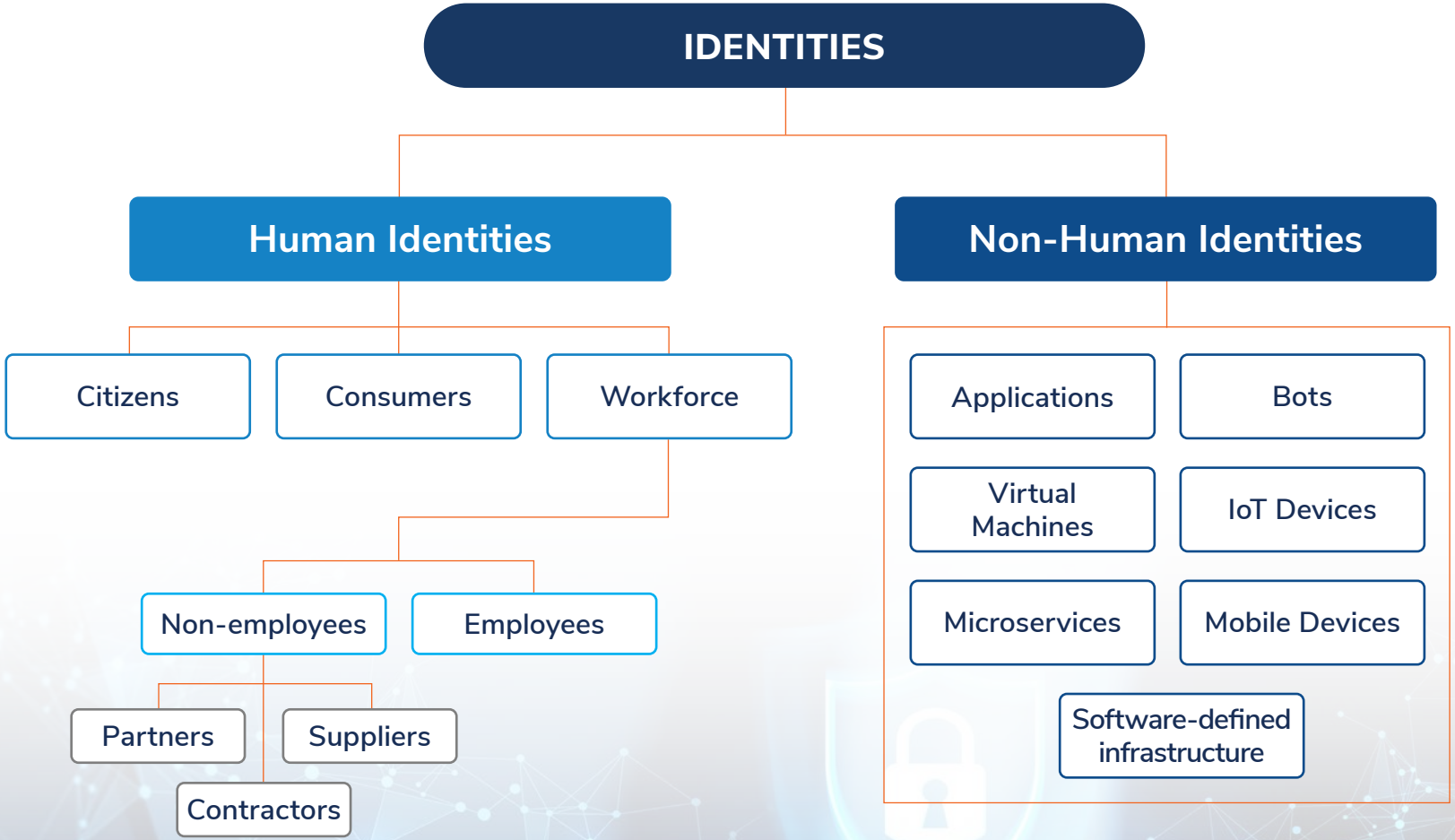
Source: Frost & Sullivan 2023 Voice of the Enterprise Security Customer Study;
Base: All respondents (n=2,099) Q: What is the main objective of using Identity security (People or Things) within your organization?

85%

of organizations will add zero trust framework to security strategy in 2024

Identity-Centric Security Is Essential for Zero Trust Framework (continued)

THE COMPLEX WEB OF IDENTITIES IN ORGANIZATIONS CREATES VULNERABILITIES



Source: Frost & Sullivan

Securing the Human Identity Layer

CHALLENGES

- AI deployment has made cyberattacks more sophisticated and difficult to identify. Opportunistic attacks that dupe people are replacing brute force attacks.
- Generative AI, phishing-as-a-service, multiple attack vectors, social engineering, and deepfakes contribute to the growing volume of relentless cyberattacks targeting humans.
- Research suggests that deepfake attempts increased by 3,000% in 2023 and have the potential to disrupt multiple industries. For instance, the real estate industry is witnessing cases of fraudsters exploiting the lack of adequate checks, digital transactions, and deepfakes to successfully impersonate owners and sell properties without ownership.
- Seemingly secure traditional multi-factor authentication (MFA)-based on SMS one-time passwords is not effective anymore. It introduces additional authentication layers that adversely affect the user experience.

SOLUTIONS

RISK-BASED AUTHENTICATION (RBA) OR ADAPTIVE STEP-UP AUTHENTICATION

- RBA considers contextual data for configurable policies to facilitate authentication decisions.
- RBA ensures seamless UX by escalating friction only upon detection of risky users and suspicious access attempts.

CERTIFICATE-BASED AUTHENTICATION (CBA) OR PASSWORDLESS AUTHENTICATION

- CBA provisions a digital certificate onto a user's device (e.g., mobile smart credential) and uses Bluetooth or near-field communication (NFC) to enable passwordless login. Using a face ID, a fingerprint, or a PIN on laptops or personal computers completes the process.
- Certificates for users and devices ensure a higher level of security.

AI-BASED BIOMETRIC VERIFICATION

- Credentials and continuous authentication are driven by contextual factors, such as user behavior, device information, and geolocation.
- Biometrics use morphological traits (face/ fingerprint), behavioral metrics (keystroke/ gesture), or multimodal methods for authentication.

Source: Frost & Sullivan

Securing the Non-Human Identity (NHI) Layer

CHALLENGES

- NHIs have grown exponentially in the last few years with the advent of automation, machine-to-machine communication, IoT, and other connected devices. For every human identity, there are nearly 50 NHIs.
- Many factors contribute to the challenge of securing NHIs:
  - Limited visibility of NHIs within an enterprise and beyond to account for non-employee identities
  - Excessive permissions, which increase the attack surface
  - A lack of compatibility of legacy machines or devices with updated security systems
- Growing cloud adoption will increase the scale of NHIs exponentially.
- Manual certificate life cycle management is unsustainable due to its lack of visibility, the rise in the volume of private and high-assurance public certificates used to encrypt devices, and the shortening life span of certificates.

SOLUTIONS

- NHIs require different rules and methods to manage the authentication, scale, ownership, and changes.
- While NHIs must be "secure by design," NHI security solutions can contribute by tracking, verifying, and managing identities. These solutions also improve operations, efficiency, and compliance.
- Centralized and automated certificate life cycle management makes certificate overview and control more intuitive, scalable, and user-friendly.
- NHI security solutions also enable governing unique machine identities that require keys, certificates, and tools to manage information flow and confidentiality.
- NHI security solutions can facilitate cryptographic transitions, such as from SHA-1 to SHA-2 or from traditional public key crypto to quantum-safe.

Source: Frost & Sullivan

Securing the Data Layer

CHALLENGES

- Privacy laws like GDPR, CCPA, eIDAS2, NIS2, DORA, NIST 800-53, and HIPAA require organizations to implement robust data protection practices. Ensuring compliance with these diverse regulations necessitates strategic investment in time, budget, and tools.
- Current certificate-based encryption solutions are only as effective as the security of underlying cryptographic assets, such as keys and secrets. Managing an exponentially growing volume of keys and secrets is an arduous task for most organizations.
- The cryptographic algorithms in use today, such as RSA and ECC, are secure only because it takes thousands of years to break the keys using existing systems. However, if large-scale quantum computers become a reality, the existing cryptographic keys could be deciphered in no time.

SOLUTIONS

- A robust key management system that provides secure storage, full control and visibility, and simplified risk reporting will improve the efficiency of IT and compliance teams. Enterprises must also invest in key management systems that comply with data sovereignty mandates across regions.
- A centralized decentralized security (CeDeSec) approach leveraging Public Key Infrastructure (PKI) and machine identity management will ensure that enterprises have centralized visibility and control across a distributed IT architecture.
- Investing in Federal Information Processing Standard (FIPS) Level 3-certified hardware security modules (HSMs) will secure encryption keys and secrets with a high assurance root of trust.
- Enterprises must invest in post-quantum-ready security solutions to safeguard and future-proof the organization from adversary activity.

Source: Frost & Sullivan

Entrust's Holistic Identity Security Portfolio

Entrust's Diverse Portfolio

- IDaaS
- PKIaaS
- Onfido Real Identity Platform
- Digital Signing as a Service
- Signhost
- TLS/SSL Certificates
- Certificate Life Cycle Management
- nShield Hardware Security Modules
- Entrust KeyControl
- nShield as a Service

Augmented With Technology

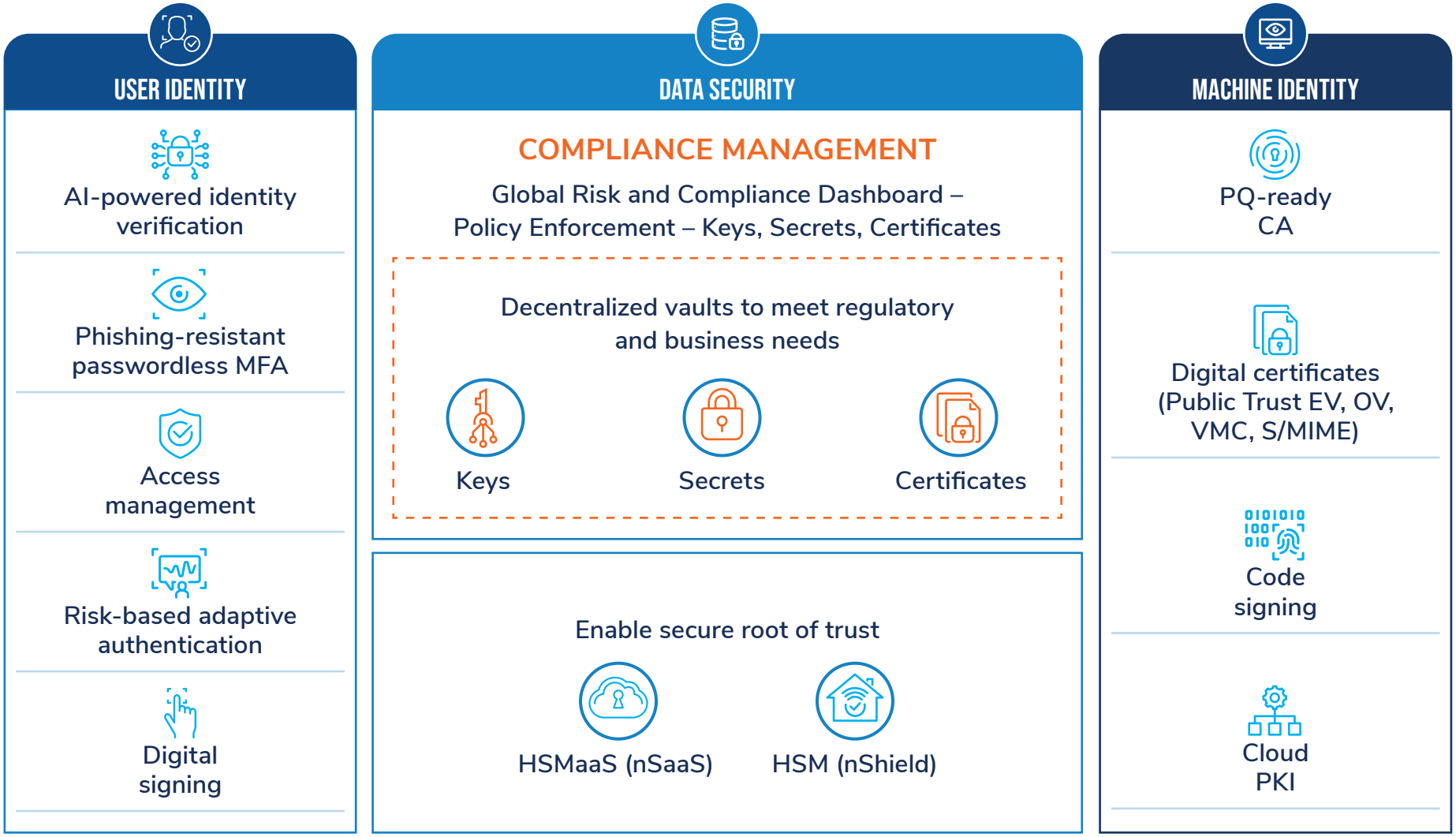
- Low-code, no-code orchestration platforms
- Multi-cloud environment support
- AI-driven authentication and biometrics
- Cloud-based digital signing using federated identities and high-assurance eSignatures
- Automated certificate/ machine identity life cycles
- Post-quantum cryptography

Enhances Outcomes Across Use Cases

- Customizable and easy-to-configure workflows
- Remote verification and global IDV to onboard and secure privileged action, such as access to critical resources and resetting credentials
- Broad range of advanced and scalable authenticators, such as passwordless, step-up, certificate-based, and biometric-based
- End-to-end digital onboarding for use cases, such as customer identity and access management (CIAM) and IDaaS
- Secure and seamless customer engagement, aligned with zero trust and know your customer (KYC), and offering phishing-resistant MFA
- PKIaaS and hybrid approach to the transition to quantum-safe data protection

Source: Frost & Sullivan

Entrust's Identity-Centric Security



Source: Frost & Sullivan

Note: PQ – Post quantum, CA – Cryptography assessment, HSM – Hardware security modules, VMC – Verified mark certificates, PKI – Public key infrastructure, OV – Organization validation, EV – Extended validation

Successful Deployment of Entrust Solutions

Upgrading Carhartt WIP's IAM Cost-effectively for Global Use

- Work in Progress Textilhandels GmbH collaborates with Carhartt, US, to design and distribute textiles. As a global company, it required a cost-effective IAM solution that would fit its international structure and modern IT infrastructure.
- WIP needed a passwordless, cloud-based authentication solution to enable user account access via SSL VPN and Citrix.

ENTRUST SOLUTION

- Entrust Identity as a Service (IDaaS)

ONE PLATFORM FOR BENEFITS ACROSS USE CASES

- The solution balanced UX and access security, ensuring user satisfaction, seamless transition, and enhanced security in a live system.
- Entrust IDaaS simplified MFA, managing use cases from simple desktop login and SSO to privileged access for user groups across all locations with soft tokens. Its virtual smart cards on devices and adaptive risk-based authentication (RBA)/digital certificates enhanced security. WIP can use multiple authenticators, like grid cards, OTP, SMS, and email.

Managing BancoEstado's Authentication Challenge

- BancoEstado, a Chilean public bank, wanted to migrate 6.5 million mobile banking customers to cloud-based advanced authentication solutions.
- The bank wanted to replace the compromised incumbent on-premises financial issuance solution with secure cloud-based instant issuance to deliver government benefits to citizens.

ENTRUST SOLUTION

- Entrust IDaaS
- Instant Financial Issuance as a Service

RAPID IMPLEMENTATION

- In only a few months, the bank's mobile banking customers were migrated to its cloud-based IDaaS authentication solution, which enabled adaptive RBA and FIDO tokens for passwordless access. The smart soft tokens embedded within the app reduced the bank's total cost of ownership.
- Entrust's Financial Issuance as a Service helped BancoEstado print 1 million cards within 60 days across 500 branches and increased uptime availability to 99.5%.

Source: Frost & Sullivan

The Final Word

END-TO-END SECURITY

Identities have evolved beyond employees and consumers to include all non-human touchpoints involved in a transaction. To enhance security posture, an end-to-end solution that can integrate and communicate with other security systems is needed.

SECURE PERIMETER

Securing the identity perimeter—be it at the human, non-human, or data layer, is paramount amidst a growing volume of cyberattacks leveraging compromised identities. Every identity must be validated continuously. Otherwise, other security controls could allow attackers through based on identity forgery, impersonation, or abuse.

AI AND ML

The frequency, volume, and sophistication of attacks made the use of AI and ML vital to identity security solutions.

ZERO TRUST

Identity assurance is a critical element in achieving zero trust security. In addition to verifying identities explicitly, zero trust security demands the use of least privileged access. A robust identity security perimeter empowers organizations to achieve zero trust security.

Evaluate your Identity Security Posture

If you answer "yes" to more than two questions, consider upgrading your Identity security platform/service to enable holistic, integrated, and intelligent security capabilities.

Does your organization...	Yes	No
...plan to incorporate zero trust principles in its security ecosystem?		
...have a sprawling technology stack that supports remote and hybrid work arrangements, multi-cloud applications, and generative AI use cases?		
...lack visibility into all identity security to protect against attacks?		
...have identity security limited to traditional MFA solutions?		
...need the ability to detect suspicious identity and privileged account activity in real time?		
...monitor AD event logs but fail to gain contextual insights related to identity misconfigurations and attacks?		

Source: Frost & Sullivan

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey.