PIPER | SANDLER

INDUSTRY NOTE
May 23, 2022

Security & Infrastructure Software

Tech Decoded: IAM Renaissance | “Who are you? Who, who, who, who?”

CONCLUSION

Identity security is more essential than ever. The market for IAM solutions is growing quickly, aided by the increase in cybersecurity breaches and digital transformation initiatives globally. Gartner estimates spend on IAM products to grow at a 14.8% CAGR from 2020-2025, reaching $25.3B compared to $12.7B in 2020. Public company TAM estimates for the market range from $20B-$80B depending on how many IAM sub-segments the company addresses.

- **The threat landscape is growing in impact, sophistication and complexity:** Cyber breaches across major enterprises and governments have proliferated in recent years, helping cybersecurity become a more relevant issue than ever. Ransomware data leaks increased 82% between 2020 and 2021 with an annual ransomware cost of $42B. Zero-day exploits and stolen credentials continue to be some of the most common methods for attackers to use. Security solutions addressing access to IT assets and threat detection capabilities are key in detecting these attacks.

- **Poor Identity Access Management equals security breaches:** According to a recent Identity Defined Security Alliance (IDSA) report, 95% of surveyed enterprises have experienced identity-related breaches. Most enterprises house thousands to millions of identities, each with varying access requirements that change constantly based on business needs. Customers are challenged with more applications than ever that must be connected and governed. It takes is one breach to cause major problems—and all it takes for a breach is one unsecured identity.

- **IAM tops the priority list for security spending in the 2022 PSC CIO survey:** Security topped CIO spending priorities in our 2022 Piper Sandler CIO survey. CIOs intend to increase spend across security in 2022 with 80% of responding CIOs expecting to specifically increase spending on IAM. We expect sustained demand for IAM solutions driven by a rise in ransomware attacks, an ever-expanding threat landscape, and organizations moving to cloud-based solutions as part of their digital transformation.

- **Zero Trust, WFH and cloud migrations are all durable IAM tailwinds:** Identity is an essential part of the digital economy and is constantly evolving. As organizations increasingly adopt cloud, hybrid WFH policies, and Zero Trust initiatives, meet regulatory demands and compliance, automate through non-human interactions (APIs, IoT, Industry 4.0), the need to be able to identify, affirm, and govern, identities with speed and scale is paramount to a sound security strategy and future proofing the organization.

- **Challenge of securing non-human identities reveals untapped growth vector:** Due to digital transformation, there are far more non-person identities than person identities, increasing the risk profile (e.g.- 42T API calls by 2024E; 25B Global IoT devices in use by 2025E). Non-human identities can take many forms (serverless functions, databases or data stores, applications/bots, containers, connected devices, etc.) and organizations are only now understanding that every time you implement a new technology solution, you introduce a unique identity to the business, with its own set of risks.

Rob D. Owens
Sr. Research Analyst, Piper Sandler & Co.

Brent A. Bracelin
Sr. Research Analyst, Piper Sandler & Co.

Clarke Jeffries
Sr. Research Analyst, Piper Sandler & Co.

Ben D. Schmidt, CFA
Research Analyst, Piper Sandler & Co.

Justin T. Roach
Research Analyst, Piper Sandler & Co.

Hannah Rudoff
Research Analyst, Piper Sandler & Co.

Mauro Molina
Research Analyst, Piper Sandler & Co.

Related Companies:	Share Price:
CSCO	42.94
CYBR	132.67
FORG	17.70
MSFT	252.56
OKTA	84.22
ORCL	68.63
PING	18.84
SAIL	62.33

INDUSTRY RISKS

Macroeconomic risk, competitive dynamics, cybersecurity risk, subdued breach risk, geopolitical risk.

Piper Sandler does and seeks to do business with companies covered in its research reports. As a result, investors should be aware that the firm may have a conflict of interest that could affect the objectivity of this report. Investors should consider this report as only a single factor in making their investment decisions. This report should be read in conjunction with important disclosure information, including an attestation under Regulation Analyst Certification, found on pages 44 - 45 of this report or at the following site: http://www.pipersandler.com/researchdisclosures.

PIPER | SANDLER

Tech Decoded

MAY 23, 2022

IAM Renaissance | “Who are you? Who, who, who, who?”

Rob Owens
SR. RESEARCH ANALYST

Brent Bracelin
SR. RESEARCH ANALYST

Contents

01. Executive Summary

02. Ransomware Renaissance

02.1 Today’s Threat Landscape

02.2 Durable Security Demand

03. IAM & SIEM in the Limelight

03.1 IAM Landscape

03.2 IAM Market Sizing

04. Beneficiaries to Watch

04.1 Public IAM Beneficiaries to Watch

04.2 Private IAM Beneficiaries to Watch

01.

Executive Summary

Executive Summary (Page 1 of 3): Conclusion

Tech Decoded – Ransomware Renaissance | IAM What IAM. We are publishing the next iteration of the Piper Sandler Tech Decoded report on the Identity Access Management (IAM) industry. With high profile ransomware attacks and cybersecurity breaches headlining news over the past years, investment in cybersecurity software has accelerated as CIOs and CISOs work to protect their organization from breaches as they also shift to a cloud-first future. As indicated by the 2022 PSC CIO survey, IAM was noted as the top area for increased security investment given its critical positioning in combating ransomware attacks and enabling Zero Trust frameworks. We outline six stocks in our coverage (MSFT, OKTA, SAIL, FORG, CYBR, PING) that appear best positioned to take advantage of the favorable demand environment going forward, in addition to 15 privates companies to watch in this space.

Defining the Terms. We view the Identity Access Management (IAM) market as the culmination of five inter-related sub-segments: Customer Identity and Access Management (CIAM), Workforce Access Management, Identity Governance and Administration (IGA), Privileged Access Management (PAM) and Non-Human Identity Management.

Identity security is more essential than ever. “Many companies are only scratching the surface of identity security, focused only on granting access. That may have been good enough a couple of years ago, but today the stakes have never been higher for enterprise security. ‘Good enough’ is no longer enough.” - Matt Mills, President of Worldwide Operations, SailPoint

Sizing the Market. The market for IAM solutions is growing quickly, aided by the increase in cybersecurity breaches and digital transformation initiatives globally. Gartner estimates spend on IAM products to grow at a 14.8% CAGR from 2020-2025, reaching $25.3B compared to $12.7B in 2020. Public company TAM estimates for the market range from $20B-$80B depending on how many IAM sub-segments the company addresses.

Beneficiaries to Watch

CIAM & Workforce:

Publics | MSFT, OKTA, FORG, PING

Privates | Transmit Security, Incode, Stytch, Socure, Trulioo, Beyond Identity, 1Password

IGA & PAM:

Publics | CYBR, SAIL, MSFT, OKTA, FORG

Privates | Saviynt, Delinea, One Identity, Beyond Trust

Non-Human Identities:

Publics | OKTA, FORG, PING
Privates | Venafi, Teleport, Ermetic

Source: Gartner, Piper Sandler Research.

Executive Summary (Page 2 of 3): Conclusion

1

The threat landscape is growing in impact, sophistication and complexity

Cyber breaches across major enterprises and governments have proliferated in recent years, helping cybersecurity become a more relevant issue than ever. Ransomware data leaks increased 82% between 2020 and 2021 with an annual ransomware cost of $42B. Zero-day exploits and stolen credentials continue to be some of the most common methods for attackers to use. Security solutions addressing access to IT assets and threat detection capabilities are key in detecting these attacks.

2

Poor Identity Access Management equals security breaches

According to a recent Identity Defined Security Alliance (IDSA) report, 95% of surveyed enterprises have experienced identity-related breaches. Most enterprises house thousands to millions of identities, each with varying access requirements that change constantly based on business needs. Customers are challenged with more applications than ever that must be connected and governed. All it takes is one breach to cause major problems—and all it takes for a breach is one unsecured identity.

3

IAM tops the priority list for security spending in the 2022 PSC CIO survey

Security topped CIO spending priorities in our 2022 Piper Sandler CIO survey. CIOs intend to increase spend across security in 2022 with 80% of responding CIOs expecting to specifically increase spending on IAM. We expect sustained demand for IAM solutions driven by a rise in ransomware attacks, an ever-expanding threat landscape, and organizations moving to cloud-based solutions as part of their digital transformation.

4

Zero Trust, WFH and cloud migrations are all durable IAM tailwinds

Identity is an essential part of the digital economy and is constantly evolving. As organizations increasingly adopt cloud, hybrid WFH policies, and Zero Trust initiatives, meet regulatory demands and compliance, automate through non-human interactions (APIs, IoT, Industry 4.0), the need to be able to identify, affirm, and govern, identities with speed and scale is paramount to a sound security strategy and future-proofing the organization.

5

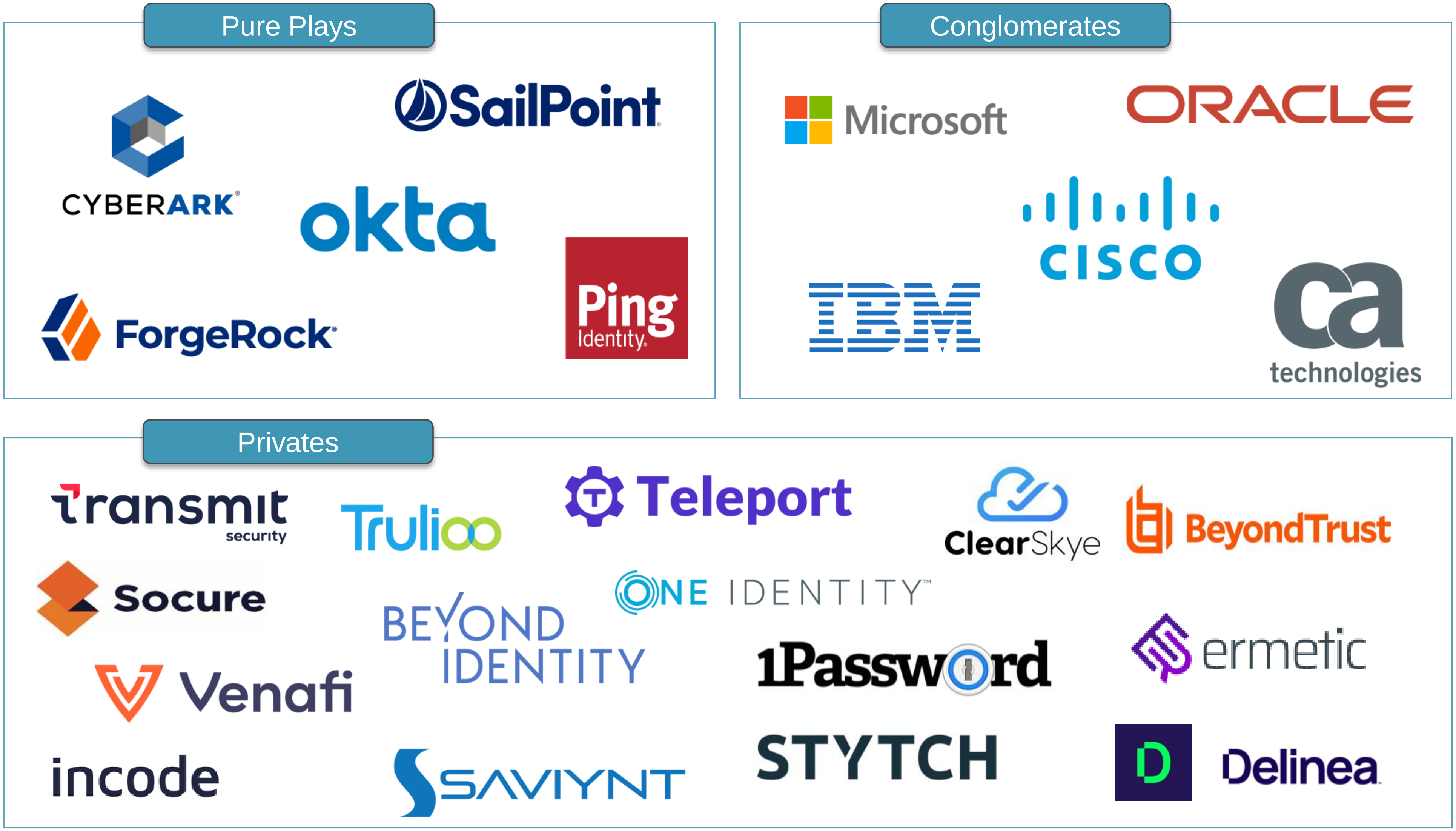
Challenge of securing non-human identities reveals untapped growth vector

Due to digital transformation, there are far more non-person identities than person identities, increasing the risk profile (e.g.- 42T API calls by 2024E; 25B Global IoT devices in use by 2025E). Non-human identities can take many forms (serverless functions, databases or data stores, applications/bots, containers, connected devices, etc.) and organizations are only now understanding that every time you implement a new technology solution, you introduce a unique identity to the business, with its own set of risks.

Source: Gartner, Piper Sandler Research.

Executive Summary (Page 3 of 3): Key Public and Private Players Profiled in This Report

We profile 21 of the companies shown below in detail within Section 4 of this report.



Pure Plays

Conglomerates

Privates

Source: Company Websites, Piper Sandler Research

Connect with your Piper Sandler
representative to view full report.