FORRESTER®

Identity And Access Management In A Post-Pandemic World

How ANZ And SEA Organisations Can Further Enhance IT Security In The “New Normal”

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY LOGMEIN | MARCH 2021

Overview
Pre-Pandemic
Pandemic Era
Post-Pandemic Needs
Conclusion

New World Demands A New Look At Identity And Access Management

As organisations move beyond the pandemic, they must contend with two new realities: 1) a growing number of employees looking to work remotely and 2) an increase in digital threats, enabled by employees connecting to work applications on their own devices (BYOD) and from outside the company network.

This crossroad poses a particular risk for organisations that have not adopted an effective identity and access management (IAM) practice. Our study of 270 business and technology decision-makers and influencers involved in and responsible for privacy and/or security at their organisations across ANZ and SEA found that firms must do more to meet the IAM and security demands of the new remote-centric world. Those that fall behind will find themselves in perpetual danger of data breaches and the business and financial repercussions that follow.

Key Findings

Decision-makers recognised the importance of IAM even before the COVID-19 pandemic. The rise in digital adoption over the past few years has exposed firms to an increase in security challenges.

The shift to remote work has further accelerated the need for more sophisticated and streamlined IAM practices. Organisations today face a greater volume of internal IAM-related security threats.

Business leaders expect IAM will grow as a priority over the next two years; they are exploring emerging practices, such as passwordless authentication, to enhance both security and employee experiences.

Overview
Pre-Pandemic
Pandemic Era
Post-Pandemic Needs
Conclusion

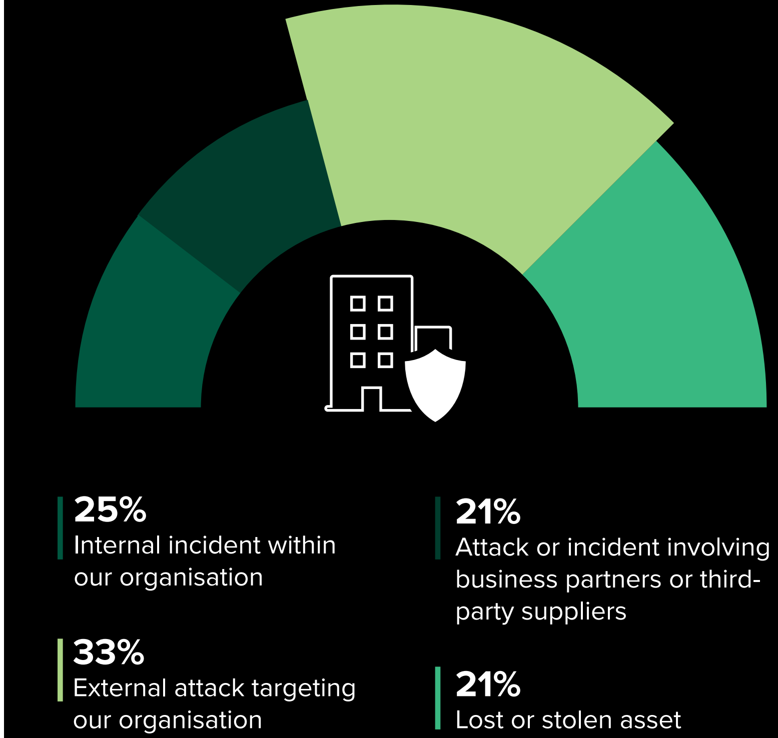
Increased Digital Adoption Has Exposed Organisations To More Security Threats

As firms exploit digital technologies to increase their operational agility and create new sources of engagement and value for their customers, vital business processes have invariably begun to traverse more customer, employee, and partner environments.

In a separate Forrester Analytics Business Technographics® survey of 629 decision-makers whose firms had experienced at least a breach within the past 12 months, Forrester found that 67% of breaches were a result of internal-related incidents, incidents with partners/third-party suppliers, or incidents with lost/stolen assets.[1]

Our study found that organisations have responded by seeking enhanced internal security controls, with 66% of decision-makers across ANZ and SEA identifying IAM as a strategic priority, even before the COVID-19 pandemic.

"Which of the following categories did the breach(es) you experienced fall into?"



Base: 3,594 breaches confirmed by 629 security decision-makers with network, data center, app security, or security ops responsibilities whose firms experienced a breach in the past 12 months
Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

Overview
Pre-Pandemic
Pandemic Era
Post-Pandemic Needs
Conclusion

Firms Established A Broad Set Of IAM Practices

Even prior to the COVID-19 pandemic and the resulting mass migration to remote workspaces, 65% of decision-makers reported more than 50 threats per month; the most common threats included phishing (54%), password spraying (50%), and spear phishing (44%).

In response to those chronic and ongoing threats, organisations have adopted a broad set of IAM practices. Eighty-seven percent of surveyed respondents across ANZ and SEA recorded adoption of at least eight IAM practices before the pandemic, with multifactor authentication (94%), virtual cloud-based directories for managing user identities (91%), and enterprise password managers (90%) as the top three most adopted practices.

"Which of the following approaches to IAM were adopted at your organisation prior to COVID-19?" (Only "Partially adopted" and "Fully adopted" responses shown)

Multifactor authentication (MFA)	**94%**
Virtual, cloud-based directory for managing user identities	**91%**
Enterprise password managers	**90%**
SMS-based two-factor authentication (2FA)	**90%**
Single sign-on (SSO)	**90%**
Identity as a service (IDaaS)	**90%**
Risk-based authentication (RBA)	**88%**
Adaptive or conditional authentication	**84%**

BUT WHY HAVE SO MANY PRACTICES?

"From a security point of view, having more layers only increases security efficacy."

- Executive manager of identity and access controls, financial services company, Australia

Base: 270 business and technology decision-makers and influencers involved in and responsible for privacy and/or security at their organisations
Source: A commissioned study conducted by Forrester Consulting on behalf of LogMeIn, December 2020

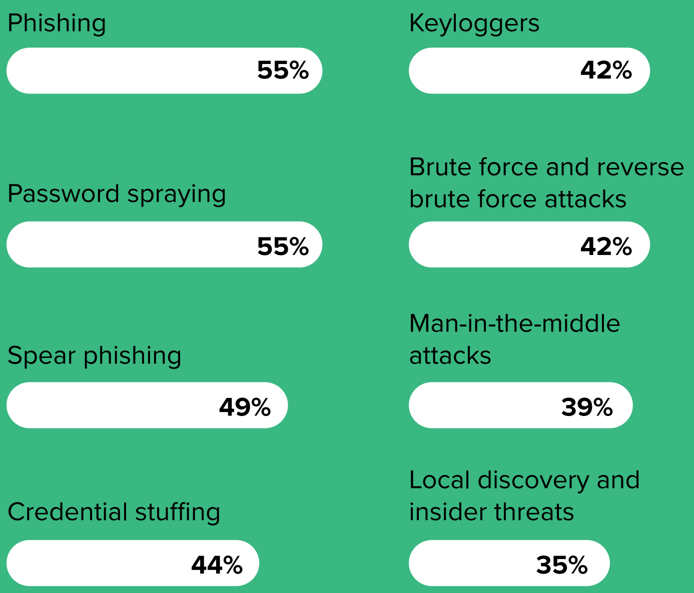
Overview
Pre-Pandemic
Pandemic Era
Post-Pandemic Needs
Conclusion

The Pandemic Has Exacerbated The Threat Landscape

With the influx of remote work, the security threat landscape has expanded greatly. A senior manager of information security at a consumer company in the Philippines told us: “Working remotely means workers can access the internet from anywhere — whether it be at home or at a café. We have been introduced to new vectors of attack.”

Financial distress, fear of layoffs, and disgruntlement toward employers at this time have also created a perfect environment for insider threats. Organisations have seen a dramatic increase in the number and sophistication of threats, with 83% of decision-makers detecting more threats since the pandemic. The biggest increases are being recorded in phishing (55%), password spraying (55%), and spear phishing (49%).

“What type of IAM-related security threats has your organisation been seeing more of since COVID-19?”



37% of decision-makers recorded a jump to more than 200 threats per month.

Base: 270 business and technology decision-makers and influencers involved in and responsible for privacy and/or security at their organisations
Source: A commissioned study conducted by Forrester Consulting on behalf of LogMeIn, December 2020

Strategic Identity And Access Management Is Paramount

While a wide range of IAM techniques were already in place, the pandemic called for more comprehensive preventive measures to counter the increase in threats. In response, organisations accelerated the adoption of IAM practices such as multifactor authentication (90%), enterprise password managers (81%), and two-factor authentication (75%); over 60% reported effectiveness in enhancing their organisations' security posture.[2]

Compliance, risk mitigation, and secure access controls have always been cornerstones of IAM. However, the pandemic has initiated a shift toward IAM as a strategic priority. Beyond security, IAM also plays an important role as a business enabler. In addition to security-related outcomes, business leaders cite increasing organisationwide productivity as a top five expected result from IAM strategy and practices.

"Which of the following are the most important outcomes that you expect from your organisation's IAM strategy and practices?"

1. REDUCED OVERALL RISK
2. IMPROVED ABILITY TO DETECT BREACHES
3. IMPROVED ACCESS CONTROL
4. IMPROVED ABILITY TO PREVENT BREACHES
5. INCREASED ORGANISATIONWIDE PRODUCTIVITY

Improving organisationwide productivity has now become a top 5 outcome organisations expect from their IAM practices.

Base: 270 business and technology decision-makers and influencers involved in and responsible for privacy and/or security at their organisations
Source: A commissioned study conducted by Forrester Consulting on behalf of LogMeIn, December 2020

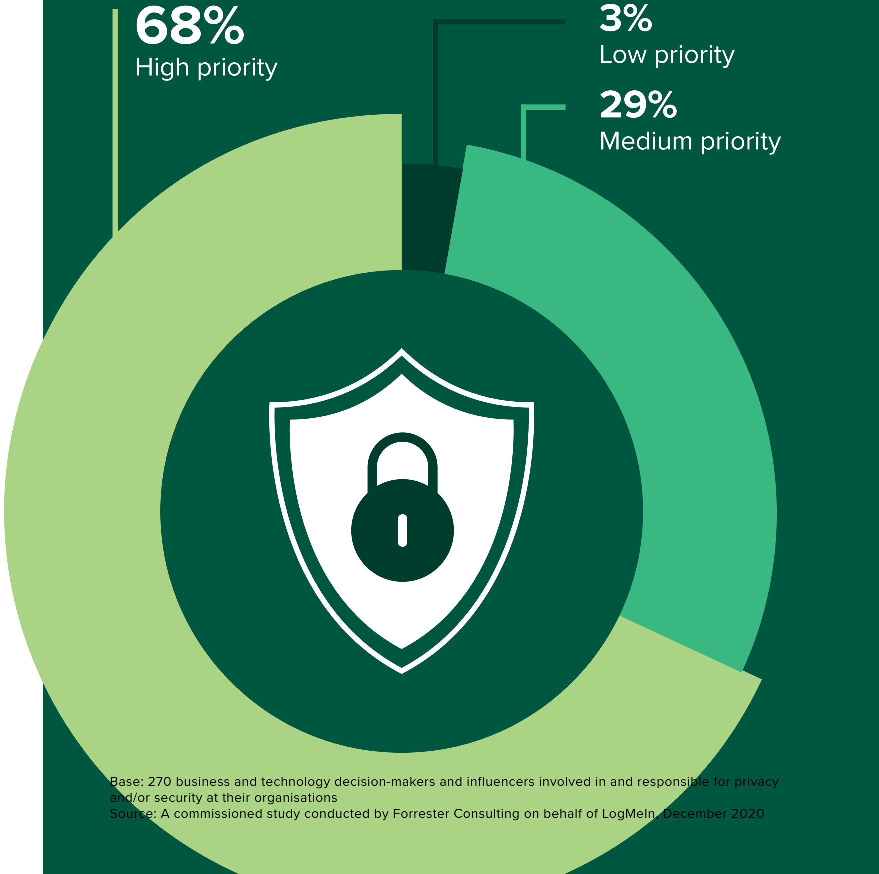
Overview
Pre-Pandemic
Pandemic Era
Post-Pandemic Needs
Conclusion

Executive Support Powers The Future Of Identity And Access Management

Security and IAM requirements have grown more complex because of the pandemic. Adapting to new vectors of attack introduced by remote work and increasingly sophisticated attacks have brought IAM as a practice to the forefront of organisations across ANZ and SEA. Moving forward, 68% of decision-makers report IAM as a high priority.

Having garnered executive support, 79% of decision-makers expect an increase in IAM budget over the coming year, with 17% expecting a more than 20% increase in budget — bolstering confidence in IAM programs (75%) across the board. An executive manager of identity and access controls at a financial services company explained, “Our IAM practice is maturing, and it is because there is now an understanding at the executive level that managing access is a business problem, not just a technology problem.”

“How important will IAM be to your organisation’s overall privacy and security strategy moving forward?”



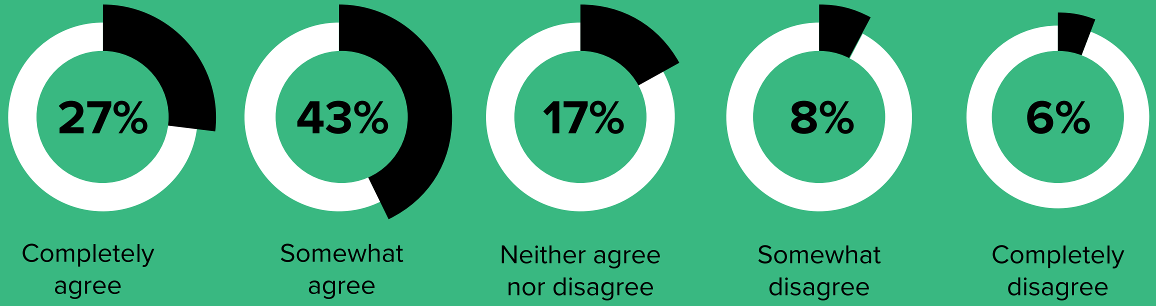
Base: 270 business and technology decision-makers and influencers involved in and responsible for privacy and/or security at their organisations
Source: A commissioned study conducted by Forrester Consulting on behalf of LogMeIn, December 2020

The Future Of IAM Requires A Set Of Simplified And Better Integrated Tools

Most (77%) decision-makers expect IAM to become less complex over the next two years and drive organisationwide productivity. IAM requirements have evolved; the traditional monolithic IAM suite approach is no longer an option. As organisations look to create more seamless IAM practices, emerging practices like passwordless authentication will grow as a priority; 70% of decision-makers already agree on the viability of passwordless authentication for their firms' future.

Firms must work with vendors offering simplified, better integrated tools through loosely coupled, API-based IAM microservices-oriented solutions that will position them to meet increasing security requirements. Firms should enhance, not compromise, employee experience, and meet demands for IAM flows that are seamless and secure and empower productivity.

"How much do you agree that passwordless authentication is the future for your organisation?"



"Decoupling IAM from passwords will be an important step toward more secure IAM flows."

- Senior manager, technology services company, Australia

Base: 270 business and technology decision-makers and influencers involved in and responsible for privacy and/or security at their organisations
Note: Percentages do not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of LogMeIn, December 2020

Conclusion

The pandemic has brought IAM into the limelight. While most organisations have already developed a strong IAM portfolio, they have more to do to meet the IAM and security demands of the new world.

Choose the right practices. Each IAM practice is best suited for a specific role. Be purposeful in how you align your IAM practices to specific workflows, policies, user populations, and technology integration requirements.

Pay attention to emerging IAM practices. Decision-makers agree that decoupling passwords from IAM will be an important step toward more secure IAM flows. Device/certificate-based authentication and biometrics offer both security and usability advantages over passwords.

Adopt a set of simplified and deeply integrated IAM practices. This will ensure that authentication methods can map to business policies and adapt to different risk levels without inhibiting user productivity.

Project Director:

Yi Qin Teow, Market Impact Consultant

Project Support:

Leon Zhang, Market Impact Consultant

Contributing Research:

Forrester’s Security & Risk research group

Overview
Pre-Pandemic
Pandemic Era
Post-Pandemic Needs
Conclusion

Methodology

This Opportunity Snapshot was commissioned by LogMeIn. To create this profile, Forrester Consulting supplemented this research with three custom interviews and custom survey questions asked of 270 business and technology decision-makers and influencers involved in and responsible for privacy and/or security at their organisations across ANZ and SEA. The custom survey began and was completed in December 2020. The interviews began in December 2020 and were completed in January 2021.

ENDNOTES

[1] Source: Forrester Analytics Business Technographics® Security Survey, 2019.

[2] Two-factor authentication is a subset of multifactor authentication. Two-factor authentication involves just one other factor, typically a one-time password sent to mobile via SMS, which is relatively cheap and easy to deploy. Multifactor authentication involves two to three factors (e.g., biometrics, authenticator app), making it more sophisticated and expensive.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organisations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Demographics

GEOGRAPHY

- Australia: 103
- Indonesia: 46
- New Zealand: 53
- Philippines: 32
- Singapore: 36

INTERVIEW RESPONDENTS

- Director, technology services company, Australia
- Senior manager, consumer goods company, Philippines
- Executive manager, financial services company, Australia

INDUSTRY

- Technology: 31%
- FSI: 23%
- Retail: 11%
- Manufacturing and materials: 8%
- Other: 27%

FORRESTER®