5 Security Trends to Watch for in 2021:

What Lies Ahead for the Future of Identity Access Management

eBOOKS
by Avatier

5 Security Trends to Watch for in 2021:

What Lies Ahead for the Future of Identity Access Management

Identity management has become the focal point for enterprise security. Of course, IT and infosec managers still need to repel the barbarians at the gates of the enterprise with strong firewalls, malware detection, penetration testing, intrusion detection and other tools to head off hackers and cybercriminals. However, with the 2020 COVID-19 pandemic and the scramble to support work-from-home employees, the real threat to business data assets, whether in the enterprise or the cloud, has become unsecured remote access.

Applying bulletproof identity authentication management (IAM) strategies to protect work-from-home and remote employees has become the number one priority when it comes to enterprise security.

According to research from the Identity Defined Security Alliance[1]:

94% of organizations suffered an identity-related breach at some point

79% suffered an identity related breach within the past two years

66% of respondents say phishing attacks constitute the most common attack vector for identity-related breaches

-50% Less than half of survey respondents have fully implemented key Identity security measures

1 Identity Security: A Work in Progress - https://www.idsalliance.org/identity-security-a-work-in-progress

With the move to support work-from-home, remote employees have become a weak point in enterprise security. When the COVID-19 pandemic struck in March 2020, there was a 667% increase in phishing attacks[2] largely targeting remote workers. At the same time, Bytedefender reports that there were 434 million remote desktop protocol (RDP) attacks before the pandemic, and that number jumped 30% in March 2020.[3]

With the cost of a data breach averaging $8.19 million,[4] it's no wonder that IT and Infosec executives are focusing their attention on securing work-from-home users. Therefore, you can expect security professionals to continue to concentrate their efforts beyond the firewall since the work-from-home phenomenon is expected to continue. According to Gartner, 74% of CFOs plan to make work-from-home a permanent part of their staffing strategy[5].

With increased scrutiny of user authentication and Identity Governance & Administration (IGA), you can expect to see some important changes in the year ahead relating to identity management. Since Avatier has been at the forefront of single sign-on (SSO) and identity management for more than two decades, we wanted to share our predictions of what lies ahead based on what we are seeing from our customers and the security market at large.

2 "Coronavirus-Related Spear Phishing Attacks See 667% Increase in March 2020," Security Magazine, https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in-march-2020

3 Webinar: "Your Long-term WFH cybersecurity strategy. What's next?" Bytedefender, https://businessresources.bitdefender.com/your-long-term-wfh-cybersecurity-strategy

4 "What is the cost of a data breach?", CSO, https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html

5 "Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently, Gartner news release, https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

01

Identity management is moving outside the enterprise

IT managers have less control over remote workers and their computing tools, which means IAM is more important than ever.

According to a LastPass survey, 98% of organizations rely on IAM to secure their businesses, and 96% say remote work has impacted their IAM strategy[6]. More than 62% of IT managers are adopting multifactor authentication (MFA) to combat phishing attacks and double the security of employee logins to protect enterprise resources.

Of those IT professionals surveyed, 35% ranked secure access as their number one priority and 27% ranked it as second. In the same survey, 23% of respondents ranked MFA as their most critical objective and another 23% ranked MFA as number two. Looking ahead to the coming year, 59% of IT decision-makers ranked IAM to improve remote workforce security as a critical priority and 96% say they are adjusting their IAM strategy to ensure that employees can securely work from anywhere.

Top Failed Predictions

"There is no reason anyone would want a computer in their home." Ken Olsen, founder of Digital Equipment Corp., 1977.

"There's no chance that the iPhone is going to get any significant market share. No chance." Steve Ballmer, CEO of Microsoft, 2007.

Titanic's captain, Edward J. Smith, said, "I cannot conceive of any vital disaster happening to this vessel. Modern shipbuilding has gone beyond that." Phillip Franklin, vice president of the White Star Line, which had produced the ship, added, "There is no danger that Titanic will sink."

In 1966, TIME pontificated that remote shopping, while possible, would never become popular because "women like to get out of the house, like to handle the merchandise, like to be able to change their minds."

As part of this renewed focus on securing remote workers, you can expect to see IAM initiatives span all access platforms. In addition to secure workstation access, you can expect the same IAM tools to be deployed for access via web browsers and mobile devices. Identity management solutions are going to come to the market designer to work the way remote workers do. Whether they access enterprise assets via desktop, a web browser or on a mobile device, IAM security will follow them no matter how they log in.

To improve user efficiency, simplify management and ensure corporate compliance, many of these IAM solutions will be integrated into remote access tools. You can expect to see SSO, MFA and identity authentication become part of collaborative tools such as Microsoft Teams and Slack, popular web browsers such as Google Chrome and Microsoft Edge, and mobile platforms such as IoS and Android.

Incorporating IAM into downstream applications will make it easier to effectively apply identity management while enabling centralized management. IT and infosec managers will not only have centralized control, integrated IAM will simplify provisioning from a centralized system, including activation and de-provisioning, and enabling push deployment and messaging.

6 "Why identity and access management is critical to securing a remote workforce,: Security Magazine, July 1, 2020, https://www.securitymagazine.com/articles/92737-why-identity-and-access-management-is-critical-to-securing-a-remote-workforce

02

The continued rise and adoption of SSO

As organizations grow and more cloud applications are added to the infrastructure, frustration over access management and security increases. To eliminate the need for multiple, secure credentials there will be an accelerated adoption of SSO.

Standards and protocols such as SAML, OAuth, and OpenID simplify identity management by enabling a single, secure set of credentials that can follow you, providing secure login access when needed. We have already seen this proliferation in B2C as consumers use their Google or Facebook credentials to log in to various e-commerce sites. Expanding SSO for B2B will simplify identity management while ensuring better user security.

SSO increases efficiency and productivity. Since users need only remember one password to access corporate data assets, that password can be more complex making it more difficult to spoof. It also reduces login time while giving you access to multiple applications.

In 1916, Charlie Chaplin said "The cinema is little more than a fad. It's canned drama. What audiences really want to see is flesh and blood on the stage."

In March 2005, Steve Chen, CTO and co-founder of YouTube expressed concern about his company's long-term viability "There's just not that many videos I want to watch."

"There is not the slightest indication that nuclear energy will ever be obtainable. It would mean that the atom would have to be shattered at will." Albert Einstein, 1932.

"You'll never make any money out of children's books" – Advice to JK Rowling from Barry Cunningham, editor at Bloomsbury Books, 1996

Steve Jobs told Rolling Stone that he didn't think subscription-based music services such as Rhapsody would fly. "I think you could make available the Second Coming in a subscription model and it might not be successful," Jobs said.

"When the Paris Exhibition [of 1878] closes, electric light will close with it and no more will be heard of it," said Oxford professor Erasmus Wilson.

Deploying SSO also is inherently more secure. Not only do SSO logins usually require MFA but using protocols such as Kerberos and Security Access Markup Language (SAML) secures information exchange. SAML, for example, secures communications between the user, the application or service, and an independent identity provider that maintains a directory to authenticate the user. Kerberos uses a ticket-granting ticket (TGT) schema that authenticates the user once, then uses TGT service tickets to grant access to other applications.

SSO also simplifies granting users access to enterprise resources, since a single set of user credentials can be used to manage roles using active directories. IT professionals will also increasingly rely on active directories to handle secure provisioning and de-provisioning using SSO credentials.

You can expect to see new single sign-on technology that makes it easier to authenticate users working anywhere, including clientless SSO that can be deployed by IT instantaneously across various collaboration platforms.

03

Access governance achieves mass adoption

In 1883, Lord Kelvin, Mathematician, Physicist and President of the Royal Society, said "X-rays will prove to be a hoax."

Bill Gates declared in January 2004 at the World Economic Forum in Switzerland that spam would be dead in 24 months.

The Y2K bug spurred massive hysteria about global disaster after midnight 1999.

Prominent futurist Ray Kurzweil predicted that food consumption would be on the way out by 2020. "Billions of tiny nanobots in the digestive tract and bloodstream could intelligently extract the precise nutrients we require," he wrote in his 2004 book "Fantastic Voyage: Live Long Enough to Live Forever."

Ridley Scott's 1982 film "Blade Runner" (and many others since then) predicted flying cars for the year 2019.

It is no longer enough to authenticate who is accessing enterprise assets. You also have to know what they are accessing and when, for regulatory and industrial compliance. This means more workflows and more reporting, which can become an issue as enterprises scale.

IGA is one of the most complex technology implementations, and it becomes even more complicated as identity authentication is used for new cloud applications, mobile apps, machine learning, artificial intelligence, the Internet of Things (IoT) and other technologies requiring cybersecurity protection. As more emerging technologies require IAM, IGA will have to become increasingly sophisticated to secure identities for all users, applications and data assets.

Expect to see a more sophisticated approach to IGA with automated workflows, real-time governance and compliance monitoring and certifications, and smart compliance management systems. As digital attacks become more sophisticated, you need to prove digital compliance to prove you are protecting assets before, during and after an attack, including real-time push notifications when an access review is assigned to a new reviewer, if an exception is allowed, or when a certification campaign starts, pauses or ends.

04

More identity self-management

Predictions from the Simpsons &/or South Park that came true

The Simpsons parodied entertainers Siegfried & Roy in a 1993 episode. During the episode, the magicians are viciously mauled by a trained white tiger while performing in a casino. In 2003, Roy Horn was attacked during a live performance by one of their white tigers.

A Simpsons episode originally aired in 2000 predicted Donald Trump would be president of the United States.

"The Simpsons" introduced the idea of a watch you could use as a phone in an episode aired in 1995, nearly 20 years before the Apple Watch was released.

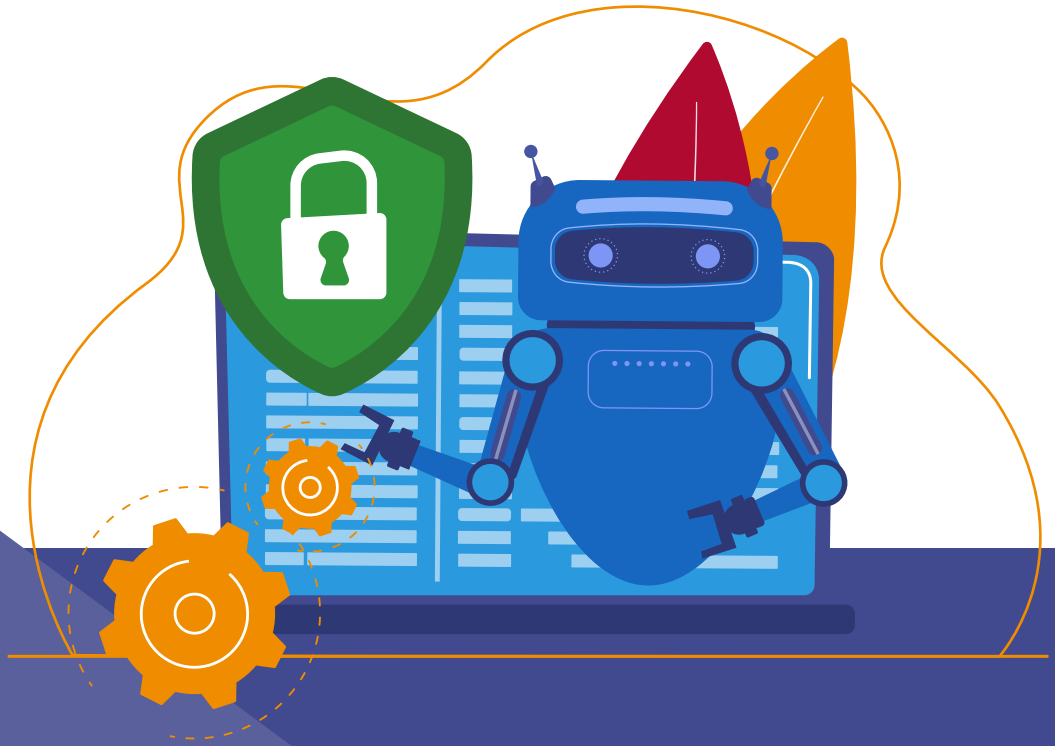
Daenerys Targaryen's big plot twist in 'Game of Thrones' was predicted by The Simpsons in a 2017 episode where Homer revives a dragon that proceeds to incinerate a village.

As a consequence of security management migrating outside the enterprise, users will assume more IAM self-control. Since they will increasingly rely on SSO authentication to ensure secure user access, IT and infosec managers will be offloading routine IAM tasks to users and department managers.

For example, the simplest IAM task to turn over to users is password reset. Forrester estimates that the average cost of help desk labor for a password reset is $70, and some organizations allocate $1 million annually for password support costs[7]. By giving users the ability to reset their own passwords you increase efficiency (since users don't have to wait for the help desk) and save money at the same time. The increase in self-service security will not only increase efficiency, but can have a direct impact on revenue, especially for customer-facing employees.

Applying identity self-management also simplifies provisioning requests. Human Resources or department managers will be able to manage provisioning and de-provisioning requests on their own, without the need for IT intervention. Access requests can be sent as push notifications for approval or rejection. Plus, with consolidated IAM and SSO, access credentials are always up to date since they are matched to active directories. So, when an employee or contract worker leaves the company, all their access credentials are de-provisioned with a single request.

7 "Best Practices: - Selecting, Deploying, and Managing Enterprise Password Managers," Merritt Maxim and Andras Cser, Forrester Research, January 8, 2018, https://www.forrester.com/report/Best+Practices+Selecting+Deploying+And+Managing+Enterprise+Password+Managers/-/E-RES139333#



05

Artificial intelligence (AI) and machine learning (ML) will improve IAM

Staying current with access privileges is an ongoing problem with any enterprise infrastructure. Employees are promoted or leave the company, roles change, contract workers come and go, and collaborative projects are completed. However, too often outdated access privileges remain in place, creating a potential security threat.

Artificial intelligence (AI) and machine learning (ML) are proving to be incredibly valuable for automating IAM. Using analytics and AI can provide contextual insight that helps employees work more efficiently, including managing application access. For example, workers rarely fit into single roles with specific access requirements. To do their jobs, workers may need access to specific applications or data, or perhaps they need to be granted access to resources or collaboration tools to complete a project. The result is a need to manage IAM across all departments, tracking access credentials based on current needs. A poorly managed IAM infrastructure can leave gaping holes in enterprise security.

A 2014 South Park episode explored what could happen if drone warfare could become a reality.

A 1999 South Park episode shows the kids obsessed with a Japanese fad called Chinpokomon. However, it turns out that the Chinpokomon devices track each player's location and send the information back to the Japanese developers — much like Pokémon Go does in real life.

In a South Park episode, Osama was killed on the 13th October 2010 after being shot in the head by a special forces Commando. The real Osama died eight months later, after being shot in the forehead by a Navy SEAL.

Using AI and ML helps automate processes and speed up IAM compliance controls. It can also help spot anomalies and potential threats using contextual analytics, enabling proactive security and identity management rather than simply responding to threats. Using AI makes it easier to monitor everything all the time, creating the level of visibility and transparency required for identity governance.

AI can automate authentication for low-risk requests. Using AI, requests can be assessed based on criteria such as time, device type, location, and requested resources, then apply IAM policies automatically to grant or deny access requests.

Contextual machine learning also can be used to power breach detection and prevention. Using ML to "learn" and identify user patterns and behaviors, such as how different identities interact with the network and enterprise assets, the system can program itself to determine "normal" activity. Using AI and ML, each user's credentials are matched to a set of historic activities, generating a risk score for each user. Any activity that falls outside the bounds set by the risk score is considered unusual behavior, triggering a response such as denied access and issuing an alert to the IT department.

C

Conclusion

As the number of data breaches continue to climb each year, effective identity access management becomes more critical. In 2019, before COVID-19, over 4.1 billion records were exposed as a result of data breaches, making it the worst year to date[8]. Compared to 2018, that represents a 54% increase in reported data breaches and a 52% increase in exposed records. When the report comes in for 2020, the number of reported data breaches will likely be higher as a result of the pandemic and weaknesses in remote identity management.

IT and infosec executives continue to take steps to secure user identity and frustrate cybercriminals, by strengthening SSO, extending MFA, moving away from the principle of least privilege, adopting AI and ML, and implementing other changes to secure access, especially for remote workers. In the months ahead, expect to see new technologies driving best practices for IAM and IGA.

Enterprise security starts with securing identity management, and you can be sure that Avatier will be at the forefront of the newest IAM and IGA solutions.

8 "2019 MidYear QuickView Data Breach Report," Risk Based Security, https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

http://content.time.com/time/specials/packages article/0,28804,2097462_2097456_2097489,00.html

https://www.inc.com/jessica-stillman/12-hilariously-wrong-tech-predictions.html

https://www.fastcompany.com/1706712/timeline-failed-predictions-part-1

https://www.forbes.com/sites/robertszczerba/2015/01/05/15-worst-tech-predictions-of-all-time/#6fcb71712997

https://www.zdnet.com/article/top-10-worst-tech-predictions-of-all-time/

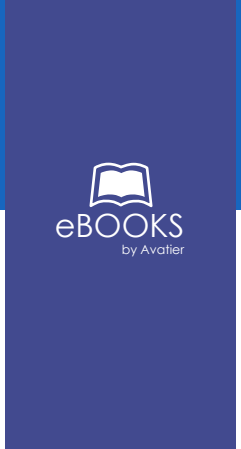
https://www.cnn.com/2020/01/01/tech/2020-predictions-we-got-wrong-scli-intl/index.html

https://www.looper.com/112806/times-south-park-freakishly-predicted-future/

https://www.businessinsider.com/the-simpsons-is-good-at-predicting-the-future-2016-11#18-daenerys-targaryens-big-plot-twist-in-game-of-thrones-season-29-episode-1-18

5 Security Trends to Watch for in 2021:

What Lies Ahead for the Future of Identity Access Management



AVATIER™