Columbus

WHITEPAPER

The right way to buy Access Management

Access Management is a critical security measure with the purpose of ensuring that only authorized users have access to sensitive data and systems. With the increasing sophistication of cyberattacks, it is more important than ever to choose an Access Management solution that is secure, scalable, and future proof.

Executive Summary

Access Management is a critical security measure with the purpose of ensuring that only authorized users have access to sensitive data and systems. With the increasing sophistication of cyberattacks, it is more important than ever to choose an Access Management solution that is secure, scalable, and future proof.

This whitepaper covers the following features and functionalities relevant for the choice of an Access Management solution:

- **The right persons with the right access at the right time:** Access Management should be able to accurately control who has access to what resources, when they have access, and for how long.
- **Strong features to thwart potential breaches and prevent attacks:** The Access Management solution should have strong features to prevent unauthorized access, such as multi-factor authentication, role-based access control, and least privilege.
- **Proactive risk detection and mitigation:** The Access Management solution should be able to proactively detect and mitigate risks, such as unauthorized access attempts and data breaches.
- **Ability to scale with the organization:** The Access Management solution should be able to scale to meet the needs of the organization as it grows.
- **Future proof solution:** The Access Management solution should be future-proof and able to adapt to new security threats and technologies.

Organizations that carefully consider these factors when choosing an Access Management solution will be better protected from cyberattacks.

In addition to the checklist provided here, the white-paper gives a brief overview of Access Management and its importance for organizations of all sizes. It also discusses the specific industries where Access Management is particularly important.

Author Ashish Bapat, Columbus Security
Editor Gitte Gormsen, Columbus Security
Publisher Columbus Security

The right way to buy Access Management

There exists a plethora of different Access Management platforms on the market, and it can be a hassle to choose which one meets your current needs while staying futureproof and providing good value for your money.

This whitepaper offers a checklist that companies can use when deciding on their Access Management vendor or when seeking consultancy advice prior to buying an Access Management solution.

As technology advances, so do the methods that hackers employ to breach systems and steal data. Every organization has unique needs for Access Management and visions as to how they want to handle security within the company.

That is why choosing an Access Management (AM) solution which can cater for your business needs is a critical step in defining a robust security roadmap.

The right persons with the right access at the right time

Before diving into the checklist, I want to put a few words on Access Management.

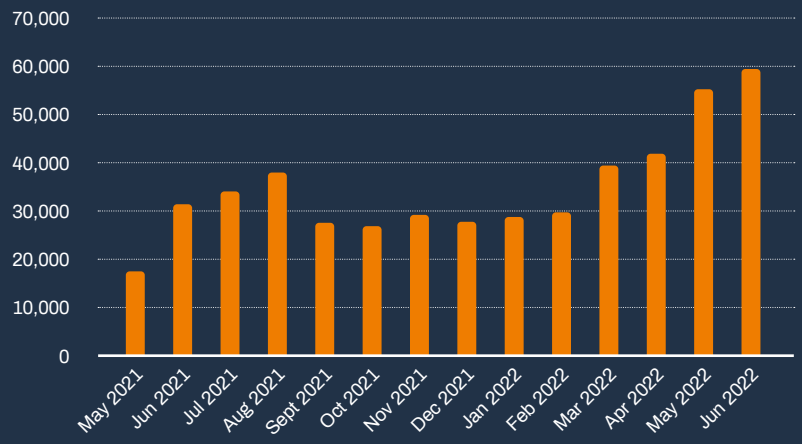
Access Management is a combination of tools and services ensuring that the right person is given the right access at the right time. The strong features of Access Management thwarts potential breaches and prevents attacks. It provides better governance and protect employees, third party contractors, identity and makes sure that access for temporary workforce are secure.

Potential breaches occur due to lack of proper Access Management, lack of strong password policies, lack of proper Multi-Factor Authentication (MFA) and lack of detection methods etc. Strong Access Management also utilizes analytics and monitoring to ensure that potential risks are caught and highlighted pro-actively.

With the help of Microsoft Digital Defense Report 2022, let us have a closer look at the latest cybersecurity trends, and why Identity and Access Management are paramount in today's security landscape:

- Password-based attacks are still common, and over 90 percent of accounts compromised via these methods are not protected with strong authentication.
- We have seen a rise in targeted password spray attacks, with very large spikes in volume of attacker traffic spread across thousands of IP adresses

VOLUME OF DETECTED TOKEN REPLAY ATTACKS



Detected token replay attacks per month. Source: Azure AD Identity Protection, unique sessions flagged by the anomalous token detection

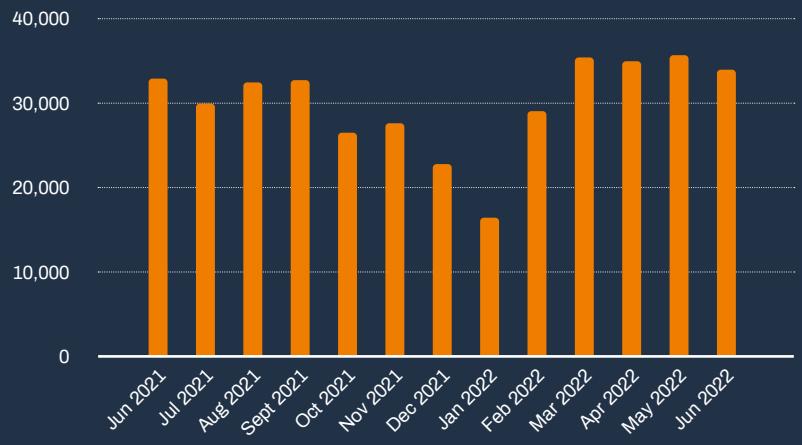
Access tokens are the ticket provided to the applications to access specific functionalities for the particular application / API.

Microsoft documents that there is potential increase in number of attacks related to tokens.

Attacker acquire access to these tokens and replays them acting as imposter (presenting themselves as genuine users).

These attacks have potential to compromise business critical applications and can incur heavy losses to business.

ESTIMATED INSTANCES OF MFA FATIGUE ATTACKS



Source: Azure AD Identity Protection

A multi factor authentication (MFA) fatigue is a very sophisticated attack where attackers repeatedly push second factor authentication requests to target victim's email, phone, or registered devices.

These push notifications are not generated by legitimate users. The goal is to force the users to accept the notifications and getting illegitimate access.

These attacks are on the rise and need strong detection and remediation

Key issues impacting cyber resilience as seen from an Access Management perspective:

- Legacy authentication protocols
- No MFA or Lack of proper MFA implementation
- Directory misconfigurations
- Identity provider misconfigurations
- No Zero trust adoption
- Low maturity Security operations
- Security monitoring gaps
- No SIEM solutions
- Insecure designs for cloud and legacy application authentications

Source: Microsoft Digital Defense Report 2022

Access Management as part of your security hygiene

Access Management is a crucial tool when it comes to a company's overall security. Strong Access Management tools, techniques and workflows help secure the organizational assets and prevent attacks.

Microsoft Digital Defense Report 2022 documents that lack of proper Access Management techniques like MFA, Zero Trust, principle of least privilege etc. are among the predominant causes of potential breaches.

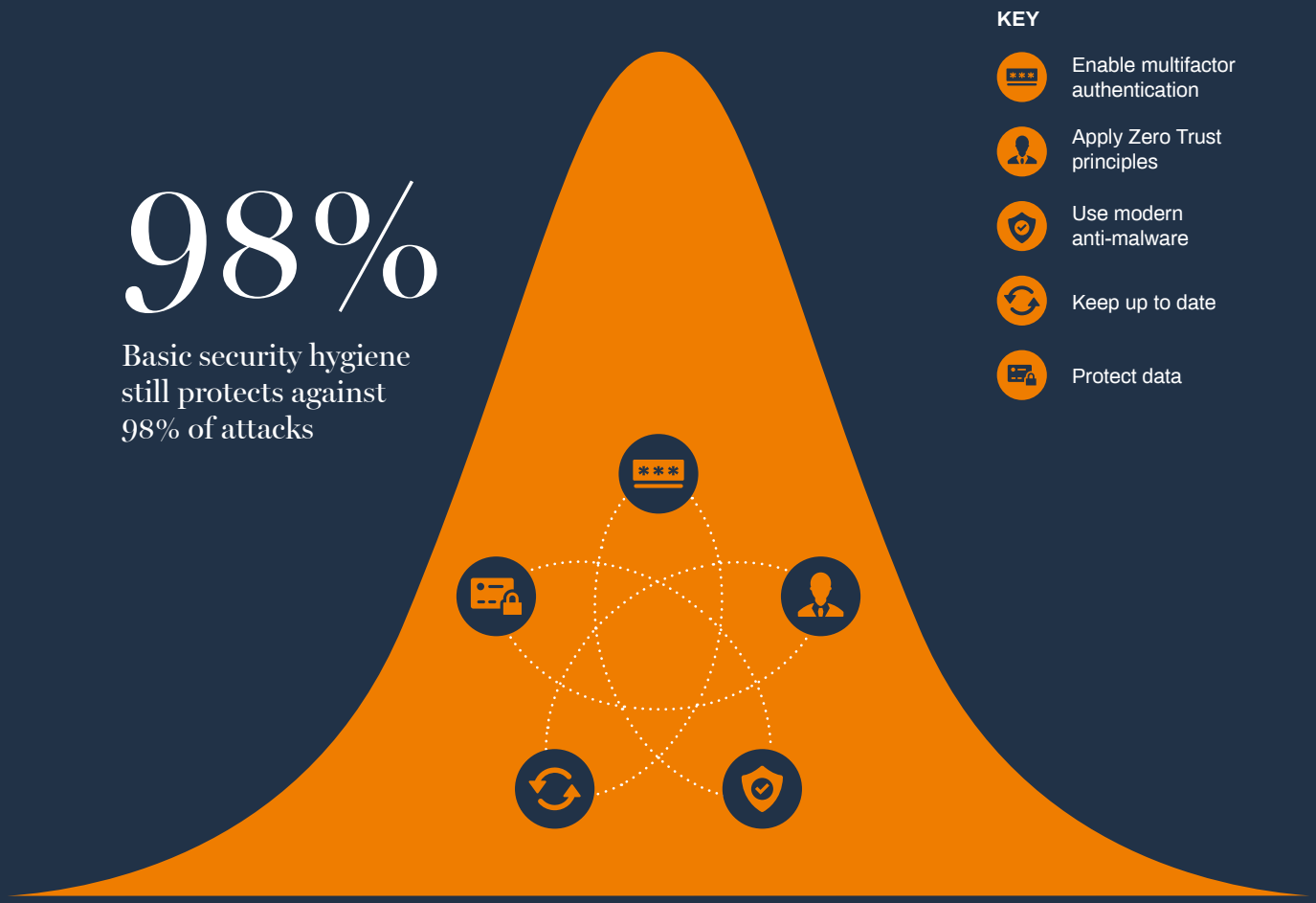
Basic security hygiene can hinder 98% of these attacks and strong Access Management plays an important role in achieving the same goal.

The cyber resiliencebell curve

Resilience success factors every organization should adopt

As we have seen, many cyberattacks are successful simply because basic security hygiene has not been followed. The minimum standards every organization should adopt are:

- **Enable multifactor authentication (MFA):** To protect against compromised user passwords and helps to provide extra resilience for identities.
- **Apply Zero Trust principles:** The cornerstone of any resilience plan limiting the impact on an organization. These principles are:
  - Explicitly verify—ensure users and devices are in a good state before allowing access to resources.
  - Use least privilege access—only allow the privilege that is needed for access to a resource and no more.
  - Assume breach—assume system defenses have been breached and systems might be compromised. This means constantly monitoring the environment for possibel attack.
- **Use extended detection and response anti-malware:** Implement software to detect and automatically block attacks and provide insights to the security operations. Monitoring insights from threat detection systems is essential to being able to respond to threats in a timely fashion.
- **Keep up to date:** Unpatched and out of date systems are a key reason many organizations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system and applications.
- **Protect data:** Knowing your important data, where it is located and whether the right systems are implemented is crucial to implementingthe appropriate protection.



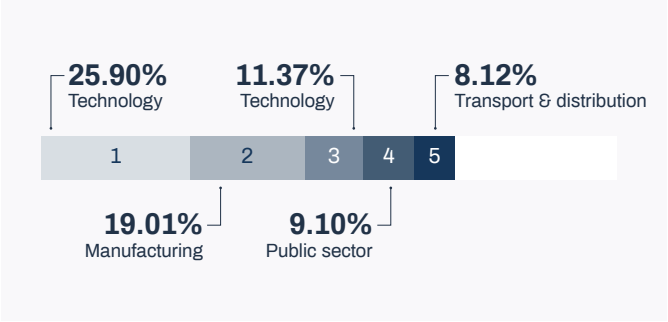
Industries where Access Management applies

It is fair to say that strong Access Management is important in all industries, be it Finance, Retail, Food & Beverages, Transport, Telecom etc. Strong security policies and prevention of identity theft is extremely important for any business since many different industries have been attacked over the years.

The NTT – 2023 Global Threat Intelligence Report documents that Critical Infrastructure and Supply Chain remains high-value targets. Since Technology, Manufacturing, and Transport/Distribution rely heavily on these infrastructures and supply aspects of day-today life, those industries remained in our top 5 most-attacked sectors.

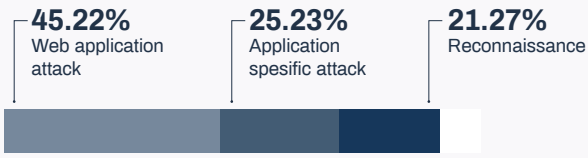
The Public Sector made the biggest jump in the past year, moving from #6 in 2021 to #4 in 2022.

Education remained in the top 5, largely due to crypto mining stemming from student devices and more open networks on many campuses.



Web applications, cloud and SaaS have been the focus of the attacks which calls for strong Access Management solutions.

As anticipated, attacks on cloud and SaaS continued to increase based on Global Threat Intelligence Center's (GTIC) telemetry. Web-based application and desktop application threats made up over 70% of attacks. Content Managemant System (CMS) software such as WordPress, Apache products and utilities like Log4J and Atlassian products such as Confluence combined to form a total of 80% of web-hosted targets. This trend was further highlighted by critical vulnerabilities in products such as JIRA, Confluence and Bitbucket which were patched throughout the year but could lead to account takeover.



How to choose a future-proof Access Management solution

Investing in Access Management can be a costly affair if not analyzed properly. But if you spend sufficient time digging into the details and particularities of Access Management, you will be able to reap great return of investment.

The below checklist includes aspects that – if considered by you when selecting your Access Management vendor – will ensure your Access Management solution meets not only your organization's current needs, but also your long-term strategy and vision.

> **If you spend sufficient time digging into the details and particularities of Access Management, you will be able to reap great return of investment.**

https://www.security.ntt/global-threat-intelligence-report-2023

The Access Management Checklist

Here is your list of important aspects to consider during your Access Management vendor selection.

FUNCTIONALITY	QUESTIONS TO ASK
Access governance and audit requirements	Does the product cater for: • Auditing requirements. • Automated and manual reports for audits. • Access governance features and capability of extracting various reports like risky sign ins, account lockouts, failed logins, usage details, traffic patterns etc.)
Adherence to regulatory requirements	Does the product support: • GDPR, NIS2, Schrems II guidelines • Industry specific adherence (HIPPA, PCI-DSS etc.) • Ability to conduct audits for system security, troubleshooting, usage analytics, and regulatory compliance?
Alerting mechanisms, integration with organizational ticketing systems	Does the product support direct integrations with enterprise ticketing systems like ServiceNow, BMC remedy for auto generation of tickets, SNMP alerts etc.?
Analytics	Does the product support integration with analytics and designing authentication flows based on user behavior analytics.
API protection	Does the product support: • Mechanism to protect APIs and micro services. • Integration with API gateways, Support rest API. • Webservices in authentication flows.
Application Integrations	Does the product provide: • Standard application onboarding factory. • Robust product documentation for integrations with multiple applications. • Standard out of the box connectors for widely used applications across the organization.
BYOD / BYOI functionalities	Does the product support: • Bring your own desktop. • Bring your own identity. • Authentication methods supporting the same.
Compromised accounts Handling	Can the product handle workflows for compromised accounts and password reset flows based on conditional access policies?
Conditional Access policies	Does the product support: • Risk-based access policies. • Authentication workflows based on user context (Location, IP, country, time of login etc.). • Adaptive authentication.
Data security, Security at Rest and in Transit	Does the product adhere to Standard Security guidelines (NIST) like data security at rest, in transit etc.

>>>

FUNCTIONALITY	QUESTIONS TO ASK
Delegated Administration capabilities	Does the product support: • Delegated administration. • Impersonation capabilities. • Handling of temporary workers, contractors, partners identities and access.
Deployment options	Does the product support: • Cloud deployment. • On-premises deployment. • Hybrid deployment. • Are SaaS offerings available and are they exactly similar to on-premises offering. • Customizations support.
Device authentication	Does the product support: • Device authentication. • Device registration/de-registration. • Device management. • Remember my device functionality.
DevOps friendly architecture	Does the product support: • DevOps approaches with containerization and orchestration technologies, such as Docker and Kubernetes. • Does it support securing micro services. • Integration into micro service architecture.
Different authentication mechanisms support	Does product support: • Multiple options for authentication including MFA and multiple options for MFA (Biometric, OTP, YubiKey etc.). • Support for API and microservices authentication.
Inbound and Outbound Provisioning, JIT	Does the product support: • Inbound and outbound provisioning. • Just-in-time provisioning. • Support of provisioning mechanisms via Rest APIs, SCIM functionality etc.
Integration Partners	Does the product have: • Integration partners available in the region. • Maintenance, support 24*7 facilities available. • Escalation procedures defined, SLAs for problem resolutions based on issue criticality.
IOT support, Detection of Bots	Does the product support: • Detection of Bots. • Google Captcha features. • IOT identities protection.
Licensing cost Vs Features	• Is the product license mechanism too complex vs the features? • Does the product provide features which require additional license cost? • Which products are covered in the Enterprise license and which ones are licensed separately? • What is the License model (how is License calculated, is it per user per service, or per user any service or based on transactions etc.)

>>>

FUNCTIONALITY	QUESTIONS TO ASK
Logging, monitoring capabilities	Does the product: • Have robust logging for troubleshooting and monitoring capabilities. • Provide integration with Splunk, QRadar etc. • Have ability for fixing vulnerabilities. What are patching schedules.
Open Standards	Does the product support open standards like: • SAML. • OIDC. • WS-Fed. • Different OAuth grant mechanisms.
Password Functionalities	Does the product: • Support strong password policies. • Include password compositions, history, banned common passwords, user inactivity etc.
Product upgrades, maintenance, and vulnerability management	How frequently must clients perform product version upgrades? Are automated upgrades available? How does the product patching schedule work? What are the communication strategies for issues, patches? How does the product handle vulnerability management, zero-day attacks, critical patches?
Scalability and Availability	Is the product scalable? • Does it support vertical and horizontal scaling? • What KPIs are available in the product? • Does the product support automatic disaster recovery?
Self Service Functionality	Does the product support self-service functionalities like: • Password reset. • Forgot password. • Unlocking of accounts using various mechanisms.
Single Sign On & Federation	Does the product support single sign on capabilities with standard protocols like SAML, OIDC, OAuth.
Strong Authorization mechanisms	Does the product support: • Strong authorization mechanisms. • Fine grained authorization. • Attribute-based authorization. • Step up authentications.
Support for Legacy Applications	Does the product have capability to protect: • Legacy systems. • Applications. • Interaction of modern systems with legacy systems and vice versa.
Support for mobile and modern applications	Does the product provide SDKs to integrate with native mobile apps including support for APIs, micro services architecture, OIDC and oauth protocols?
Zero Trust, MFA options	• Which MFA options does the product support? • Does the product support Zero trust and how it is achieved in the product?

Conclusion

Selecting the right Access Management solution is a pivotal step in ensuring the security and longevity of your organization's digital assets. The diverse landscape of Access Management platforms demands careful consideration, and this whitepaper provides a valuable checklist to guide your decision-making process. As technology continues to evolve, the threats posed by hackers become increasingly sophisticated. Access Management stands as a vital defense, ensuring that the right individuals have the right access at the right time.

Effective Access Management not only thwarts potential breaches and attacks but also enhances governance and safeguards your employees, contractors, and identities. Furthermore, it secures access for temporary workers and employs proactive analytics and monitoring to identify and address potential risks.

The absence of robust Access Management techniques, such as Multi-Factor Authentication (MFA) and the principle of least privilege, has been identified as a significant contributor to potential breaches. Basic security measures can prevent a substantial majority of such attacks, emphasizing the critical role Access Management plays in fortifying your organization's security posture.

Access Management is indispensable across various industries, including Finance, Retail, Food & Beverages, Transport, and Telecom, as the threat landscape remains relentless. Critical Infrastructure and Supply Chain sectors continue to be prime t argets, while the Public Sector and Education have also witnessed increased cyber threats.

Investing in Access Management necessitates careful analysis to avoid unnecessary costs. By delving into the details and aligning your choice with your organization's long-term strategy, you can maximize the return on investment. The provided checklist serves as a valuable resource to ensure that your Access Management solution not only meets your current needs but also aligns with your future vision and goals. In an ever-evolving digital landscape, making the right choice in Access Management is a critical step towards safeguarding your organization's digital assets and maintaining robust security.

Contact details:

Ashish Bapat
ashish.bapat@columbusglobal.com

Columbus

kontakt.dk@columbusglobal.com