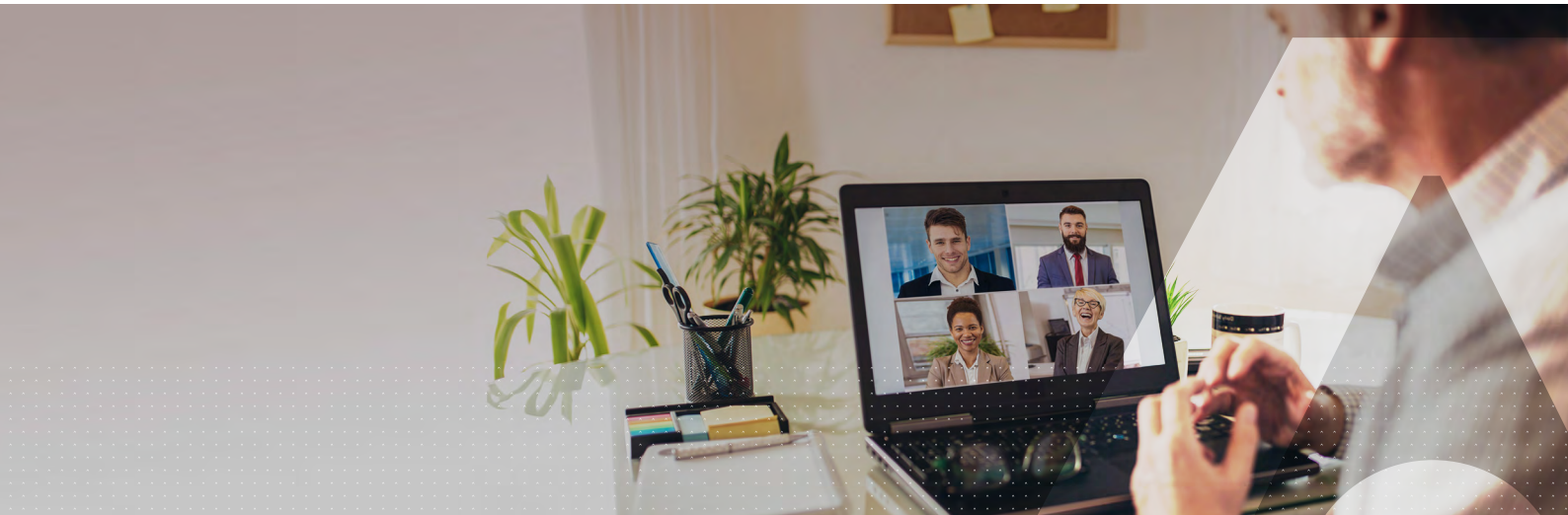


Strong Authentication and Access Management to Address Expanded Threat Landscape



Contents

3 Introduction

3 Top attack vectors

4 Most Targeted Sectors

4 Analysis of attack vectors

4 Malware

4 Web-based Attacks

5 Phishing

5 Web Application Attacks

5 Identity Theft

5 Insider Threat

5 Ransomware

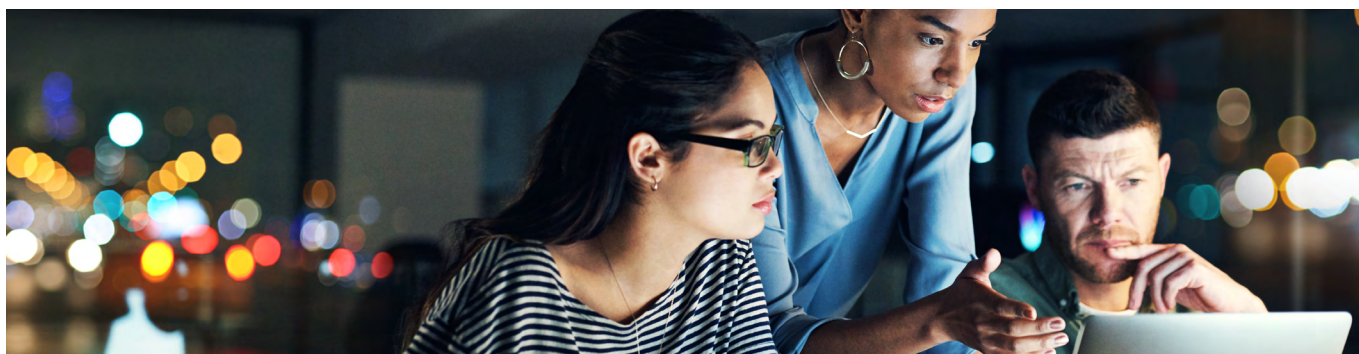
6 How strong authentication and access management can help mitigate these threats

7 How Thales SafeNet Trusted Access can help

7 Thales SafeNet Trusted Access

8 About Thales

Introduction



The last few years have brought significant changes in the cyber threat landscape. The key factors driving these changes were the historically unique, abrupt transformation forces released by the coronavirus pandemic and the continuous increasing trend in the advanced adversary capabilities of threat actors. It is important to note that the latter amplified the impact of the COVID-19 pandemic in an increasingly connected world.

The COVID-19 pandemic forced large-scale adoption of technology to address a variety of critical aspects of the crisis, such as coordination of health services, the international response to contain the virus, adoption of remote working regimes, distance learning, interpersonal communication, control of lockdown measures, teleconferencing and many others.

Cybersecurity has faced a paradox: it has been both the challenge and the opportunity in this transformation. The changes imposed in the information technology (IT) landscape weakened existing cybersecurity measures, turning their speedy adaptation into a challenge. At the same time, cybersecurity is the enabler of trust in emerging use cases for digital services and thus it can facilitate the transformation.

The COVID-19 pandemic showed that malicious actors had a level of capability that allowed them to adapt to this transformation quickly. The adversarial modus operandi focused on the personalization of attack vectors. Advanced credential-stealing methods, credential-stuffing, highly targeted phishing attacks, advanced social engineering attacks, advanced malware obfuscation techniques and more extensive penetration of mobile platforms are the main achievements of adversaries. If cybercriminals start combining these advances with artificial intelligence and machine learning, in the future we will see an increase in successful attacks and undetectable campaigns.

Top attack vectors

To help organizations understand the threat landscape, advance their readiness and target the response better, the European Union Agency for Cybersecurity (ENISA) published in October 2020 the [ENISA Threat Landscape 2020](#) report. The report findings indicate that during the pandemic, cyber criminals have been advancing their capabilities, adapting quickly, and targeting relevant victims more effectively.

The following infographic, [courtesy of ENISA](#), displays the top 15 cyber-attack vectors identified in the Threat Landscape report.



Together with the attack vectors, the report has identified several trends shaping the cyber threat landscape, including:

- The attack surface expands as organizations are pursuing their digital transformation initiatives.
- Social and economic norms are becoming even more dependent on a secure and reliable cyberspace.
- Social media platforms are increasingly targeted as a way for criminals to pivot their malicious actions and reach different domains.
- State-sponsored actors are launching targeted, advanced, and persistent attacks against high-value data and systems.
- Credential theft is the key objective of massively distributed attacks with short duration and wide impact.
- Ransomware remains widespread with costly consequences.
- The number of phishing attacks grows since they exploit the human dimension of cyberspace.

Most Targeted Sectors

The sectors most targeted during this period were digital services, government administration and the technology industry. Attacks on digital service providers - email, social and collaborative platforms and cloud providers - often serve as proxies to reach other, more attractive targets. Government agencies and city administrations were an attractive target because the public sector usually paid the ransoms. In contrast, attacks on the technology industry, mainly through supply chain attacks, allowed malicious actors to compromise the development of software through zero-day exploits and backdoors attacks.

It is important to note that the healthcare sector suffered from an increased number of cyber-attacks, especially at the beginning of the pandemic. Criminals exploited the public's need for access to medical services to contain the virus by initially targeting the hospitals, then the vaccine supply chain.

Analysis of attack vectors

In the following paragraphs we will provide a short analysis of the identified attack vectors that are a threat to user identities and access controls.

Malware

The objectives of malware are information or credential theft, espionage and disruption of businesses. The most common vectors to spread malware are web and email protocols. Using brute force techniques or exploiting system vulnerabilities, certain malware variants were able to spread further inside corporate networks. Although malware detections globally remained at the same levels as in 2018, there was a noticeable shift from consumer to business targets, with education and retail being the most affected sectors. In the banking sector, over one third of the malware attacks targeted corporate users with the intention of compromising their credentials and stealing financial resources.

The most noticeable malware incidents were the following:

- Airbus [suffered a data breach](#) affecting employees in Europe.
- The American Medical Collection Agency suffered a data breach affecting [12 million patients](#) using a card skimming malware.
- A [ransomware attack on the City of Pensacola](#), Florida resulted in 2GB of data being made available online, possibly containing personally identifiable information (PII).

Web-based Attacks

Web-based attacks are an attractive method by which threat actors can delude victims using web systems and services as the threat vector. Web-based attacks can disrupt the availability of web sites, applications and application programming interfaces (APIs) through brute force login attempts, breaching the confidentiality and integrity of data.

Web-based attacks are delivered by:

- Drive-by downloads, where the user visits a legitimate website that has been compromised and unwittingly downloads malicious content to their device.
- Watering hole attacks, which is used for targeted attacks using malicious content, such as scripts or ads.
- Formjacking, where adversaries inject malicious code into legitimate payment forms. This type of attack is used to capture banking and other personal or sensitive information, which are then leveraged for further criminal purposes.
- Malicious URL, which involves social engineering techniques to persuade the victim into clicking the URL to deliver malicious content and compromise the victim's device.

Phishing

Phishing attacks attempt to steal personal data such as login credentials, credit card information or even money using social engineering techniques. The most targeted types of services are [SaaS and webmail platforms, as well as payment services](#). Phishing attacks create many cascading effects, impacting businesses and individuals in many ways.

One variant of phishing is Business Email Compromise (BEC) attacks, which resulted in [\\$26.2 billion of losses in 2019 alone](#). The majority of phishing mails contain an infected Microsoft Office attachment, while [Monday](#) is the preferred day for sending such scam mails. It is important also to note that more than two thirds of phishing sites, where the victims are being redirected, are [using HTTPS to disguise](#) as legitimate websites.

Some notable phishing attacks include:

- A phishing attack on [Lancaster University](#) students resulted in the loss of personal data.
- A [car manufacturer subsidiary](#) lost \$37 million (ca. €31 million) due to a BEC scam.

Web Application Attacks

While organizations are developing more consistent automation in their web application lifecycle, security is becoming an essential part of their offering. The introduction of complex environments drives the adoption of new services such as Application Programming Interfaces (APIs), which create new challenges for web application security. SQL injection and cross-site scripting (XSS) attacks are the most common types of threats against cloud-based apps.

Configuration errors and lack of security testing are key roots for insecure application development and deployment. These flaws lead to authorization and authentication failures, which malicious actors leverage to compromise credentials and gain access to critical information. As a result, data breaches are the second most pressing concern to web application security.

Identity Theft

Identity theft or identify fraud is the illicit use of a victim's personal identifiable information (PII) by an impostor to impersonate that person and gain a financial advantage and other benefits. Identity theft is a growing threat for businesses and individuals alike, with more than 4.1 billion records exposed during 2019, including:

- The exposure of nearly 106 million American and Canadian bank customers' personal information from the Capital One data breach incident in March 2019.
- The exposure of 170 million usernames and passwords used by digital game developer Zynga in September 2019.
- Theft of 9 million personal records from EasyJet customers including identity cards and credit cards.

While the prime motivation is financial gain, data breaches expose emails (70%) and passwords or other login credentials (64%). It is important for businesses to understand that data breaches cost organizations millions and these costs span over many years. These costs might become even higher if we add the penalties incurred in highly regulated organizations for failing to maintain compliance.

Business email compromise (BEC) is a growing threat because of the vast amount of credentials and personal information stolen. Companies experience an average of 12 credential-stuffing attacks each month, wherein the attacker can identify valid credentials.

SIM-swapping is another trending technique, used mainly against high-profile accounts, such as the case with the [Twitter CEO Jack Dorsey](#), or in [Brazil where 5,000 victims](#), mainly politicians, ministers and governors had their accounts hacked by an organized gang.

Insider Threat

Insiders, whether negligent or malicious, are a serious threat to businesses since they are abusing privileges and trust which grant them access to critical information. Insiders are a [cause for alarm for 88% of organizations](#) because it is difficult to distinguish between legitimate and malicious access to applications, data and systems.

Poor or legacy access controls, such as weak or reused passwords, and orphaned accounts are vulnerabilities in identity and access management programs that insiders leverage to cause harm.

Ransomware

Ransomware continues to generate substantial financial rewards for malicious actors and losses for their victims. Victims may suffer economic losses either by paying the ransom or by paying the cost of recovering from the loss. For example, the city of Baltimore in Maryland, USA, is expected to pay up to \$18.2 million to recover from a ransomware attack.

A [recent study](#) identified human-operated ransomware campaigns, in which adversaries employ credential theft and lateral movement methods traditionally associated with targeted attacks such as those from nation-state actors.

Several successful [ransomware families target RDP servers](#) to initiate an attack. Unfortunately, many organizations still use RDP instead of the more secure Virtual Private Network (VPN) for remote access. The problem with the RDP is that it suffers from vulnerabilities that can be exploited and the RDP service may rely on internet-facing servers which are easily accessed.

Many of the above threat vectors are executed in a layered approach leading to lateral attacks within organizations. For example: Phishing can lead to identity compromise which enables malicious actors to more easily embed malware within a network.

How strong authentication and access management can help mitigate these threats

As enterprises embrace modern technology trends and cloud computing, security becomes a top concern. This is especially evident in the surge in various attack vectors against cloud and on-premises infrastructures, many of which have led to massive data breaches. As a result, IT teams are seeking streamlined methods of centrally defining and enforcing access controls to manage security and compliance in a consistent manner across their cloud and on-premises applications. Securing access to these deployments is critical especially for ensuring business continuity in emergency situations which disrupt normal workflows.

Identity is the new perimeter in a perimeter-less business environment. With apps, services and data in the cloud, everyone is literally an outsider. Establishing and enforcing a robust identity and access security policy benefits businesses to safeguard the confidentiality, integrity, and availability of their assets both in the cloud and on-premises. At the same time, they can protect the privacy of their customers' personal data and sustain compliance with a growing number of security and privacy regulations, laws, and jurisdictions.

Before selecting an authentication and access management solution, it is important to have a thorough understanding of the threat landscape. Cyber threat intelligence combined with traditional intelligence can become the most valuable asset in an organization's arsenal to assess and mitigate emerging threats to user authentication. Organizations and agencies such as CISA and ENISA provide a taxonomy of the most predominant and noteworthy attack vectors.

These vectors are "yet another example of how integral strong identity and access management are to cloud security," [notes](#) Dirk Geeraerts, VP EMEA Access Management at Thales. To determine the appropriate authentication and access security solution, enterprises must assess the potential risks and sensitivity of the resource, as well as compliance regulations related to the type of data being accessed.

In addition to assessing the risk environment, the selection of an authentication and access management solution should involve maintaining a balance between trust, user experience and total cost of ownership. The table below summarizes the considerations for selecting an authentication and access security platform.

Topic	Considerations
Principles	<ul style="list-style-type: none">• Risk-appropriate authentication• End-to-end security: how to protect your users and the authentication infrastructure• Low friction and superior user experience• Minimalism: a single authentication method for all use cases with similar characteristics
Authentication Requirements	<ul style="list-style-type: none">• Authentication scenarios• Adaptive access• End-user devices: desktop vs mobile device, Windows vs MacOS, BYOD vs Corporate-owned, etc.
Constraints	<ul style="list-style-type: none">• Compliance• User experience• Integration with application architecture• User constituencies (management, office workers, contractors, privileged users, etc.)

An additional point for consideration is the risks of vendor lock-in. Cloud service providers have developed their native identity and access management solutions. However, these solutions are vulnerable to various threats.

“...it’s worth reminding businesses that separating their cloud provider and access management solution is imperative in ensuring robust security. In the event that malicious actors are able to gain access to the back-end of a cloud provider – potentially even viewing source code – all applications and data could suddenly be at risk. Having a separate and isolated access management solution is the differentiator between a business being able to control its own access security, or hackers taking it over,” underpins Dirk Geeraerts.

Organizations can leverage the benefits of the shared security responsibility principle in the cloud and select the best in class, cloud-neutral identity and access management (IAM) solution. Modern Access Management as a Service, cloud-based solutions allow organizations to use single-sign on, authentication and access controls to provide secure access directly to cloud services. These solutions offer a variety of advantages, including:




- Reduced breach risk by protecting enterprise and cloud apps at the access point.
- Reduced identity management complexity by offering seamless access into the required apps either from home or any other location outside the business premises.
- Ease of deployment, taking advantage of cloud-based delivery.
- Increased time to value and cost savings, without investing in servers to support access management functions in a sustainable manner.
- High availability and reliability since the IAM services are offered in the cloud, thus avoiding single-points of failure.
- Frequent and easy-to-consume functional upgrades.

How Thales SafeNet Trusted Access can help

Thales SafeNet Trusted Access enables organizations to protect enterprise applications and scale securely in the cloud with a broad range of authentication capabilities, while ensuring security with smart single-sign on and policy driven access controls.

Thales SafeNet Trusted Access

Universal authentication methods

 PKI	 Hardware	 3rd Party	 OTP Push	 Voice
 FIDO	 Pattern Based	 Passwordless	 Biometric	 Password
 Google Authenticator	 SMS	 eMail		

Deploy secure access quickly & efficiently

Avoid vendor lock-in & keep control of your access security

Prevent breaches and avoid financial liability & penalties

Meet budget & business goals

The ability to scale securely in the cloud, enable employees to work from home, improve productivity and efficiency, and reduce costs is now more critical than ever. Continued adherence to legacy identity and access management tools will not be sufficient to support modern architectures and enable organizations to benefit fully from cloud efficiencies. By implementing a modern, cloud-based access management platform such as Thales SafeNet Trusted Access, organizations can accelerate their business evolution and reduce the risk of data breaches, while ensuring agility and cost savings.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.



Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <

