IEEE SA
STANDARDS
ASSOCIATION

INDUSTRY CONNECTIONS
REPORT

CYBERSECURITY IN AGILE CLOUD COMPUTING

CYBERSECURITY GUIDELINES FOR CLOUD ACCESS

Authored by

David Tayouri
ELTA Systems Ltd.

Snir Hassidim
Check Point

Alex Smirnov
Oracle

Asaf Shabtai
Ben-Gurion University of the Negev

IEEE

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

PDF: STDVA25642 978- 1-5044-8996-6

Find IEEE standards and standards-related product listings at: http://standards.ieee.org.

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA INDUSTRY CONNECTIONS DOCUMENTS

This IEEE Standards Association ("IEEE SA") Industry Connections publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable and reviewed by members of the IEEE SA Industry Connections activity that produced this Work. IEEE and the IEEE SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE SA Industry Connections activity members disclaim any and all conditions relating to: results; and workmanlike effort. This IEEE SA Industry Connections document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at https://standards.ieee.org/about/bog/iccom/.

This Work is published with the understanding that IEEE and the IEEE SA Industry Connections activity members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

TABLE OF CONTENTS

CYBERSECURITY GUIDELINES FOR CLOUD ACCESS

ABSTRACT

The enterprises' network and network security architectures cannot effectively serve digital businesses' dynamic, secure access requirements. The enterprise data center is no longer the center of access requirements for users and devices. Organizations demand immediate, uninterrupted access for their users, no matter where they are located. Digital business transformation efforts, adopting Software as a Service (SaaS), working from home (especially following the COVID-19 pandemic), and emerging edge computing platforms have changed how enterprises work. Digital business transformation requires anywhere, anytime access to applications and services—many of which are located in the cloud.

The enterprise perimeter can now be everywhere—a dynamically created, policy-based secure access service edge. Enterprises want to protect their assets from unauthorized entities. Still, they also want to keep business continuity by allowing trusted devices and users to access applications hosted on-premises or in the cloud. To achieve this, one of the most critical security layers is secure remote access. This paper presents the cloud security guidelines and best practices, emphasizing secure remote access.

1. INTRODUCTION

In previous work, the technologies relevant to secure remote access were surveyed, and it was decided that the focus should be on the technologies highlighted with green in FIGURE 1, FIGURE 2, FIGURE 3, and FIGURE 4. These technologies are considered the most pertinent to securing remote access. This paper presents the guidelines and best practices for the selected technologies.

FIGURE 1 Cloud Access Infrastructure—Basic Security Components

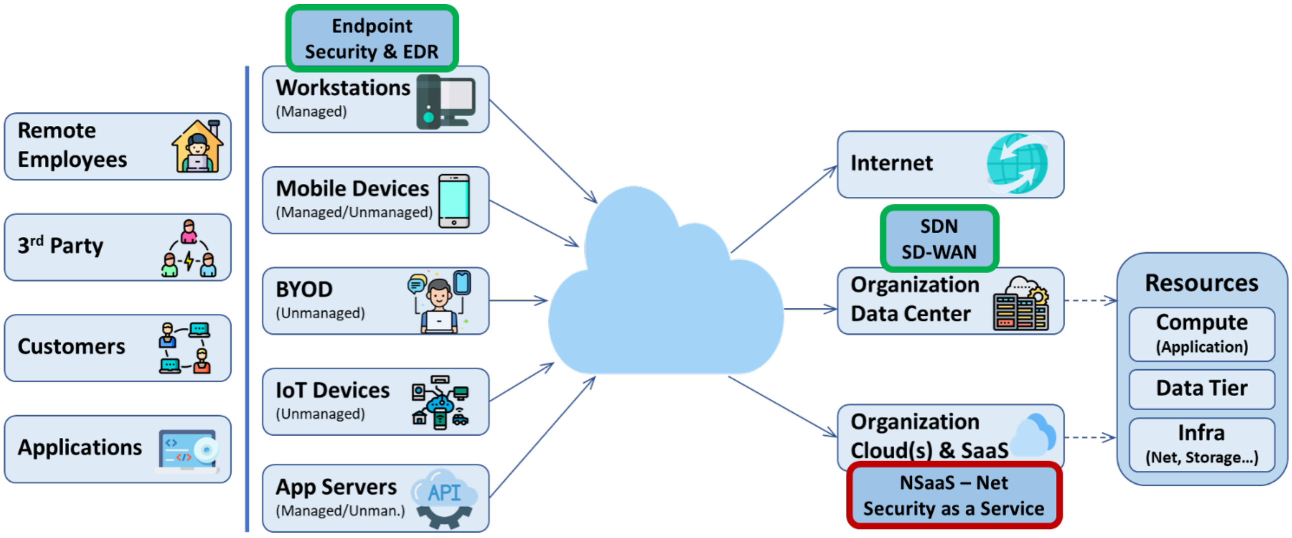


FIGURE 2 Cloud Access Infrastructure—Access Control

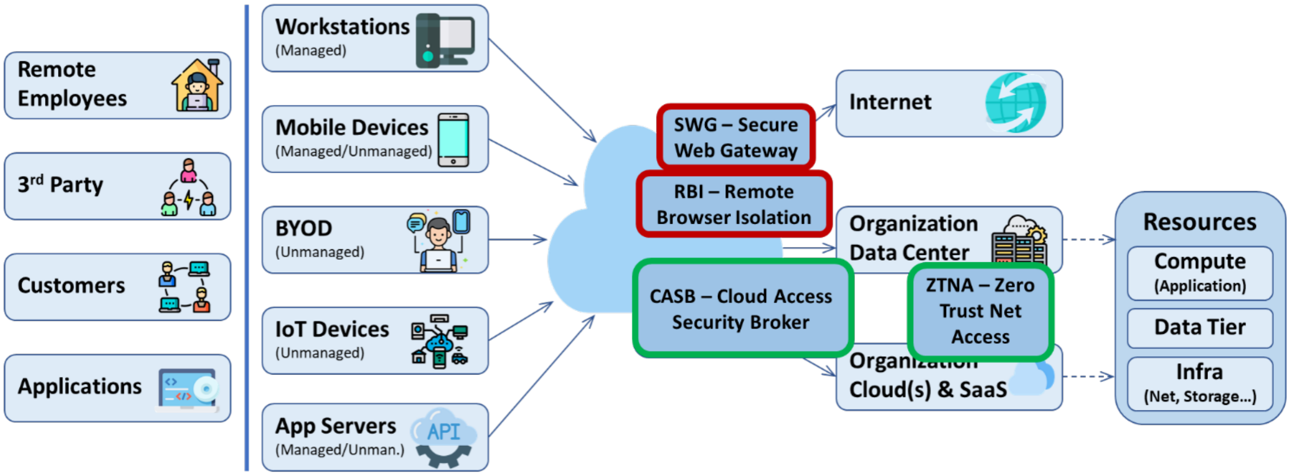


FIGURE 3 **Cloud Access Infrastructure—Identity and Authentication**

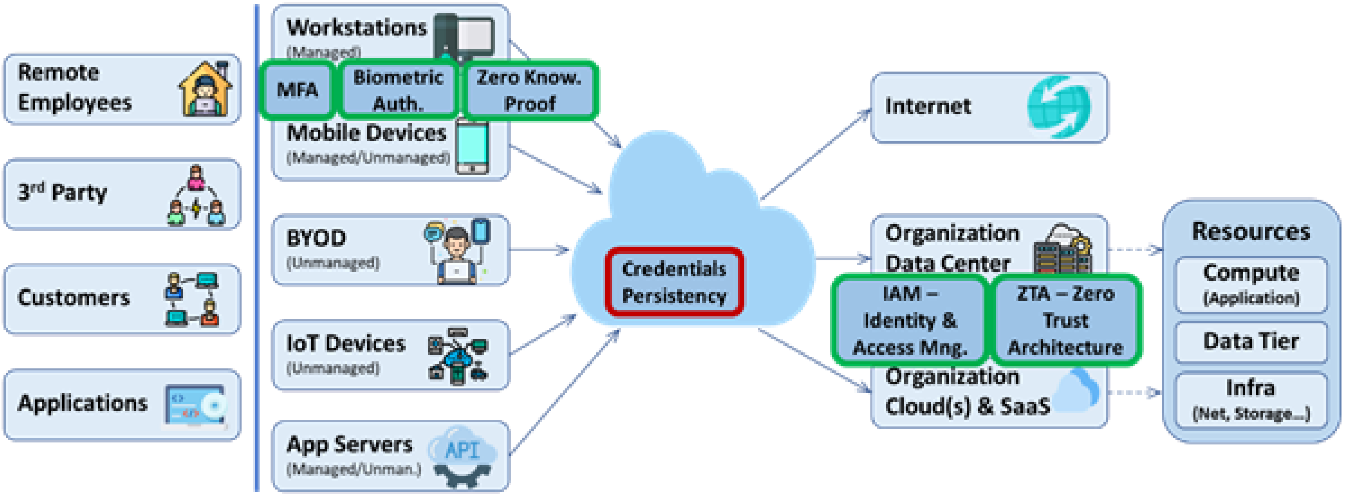
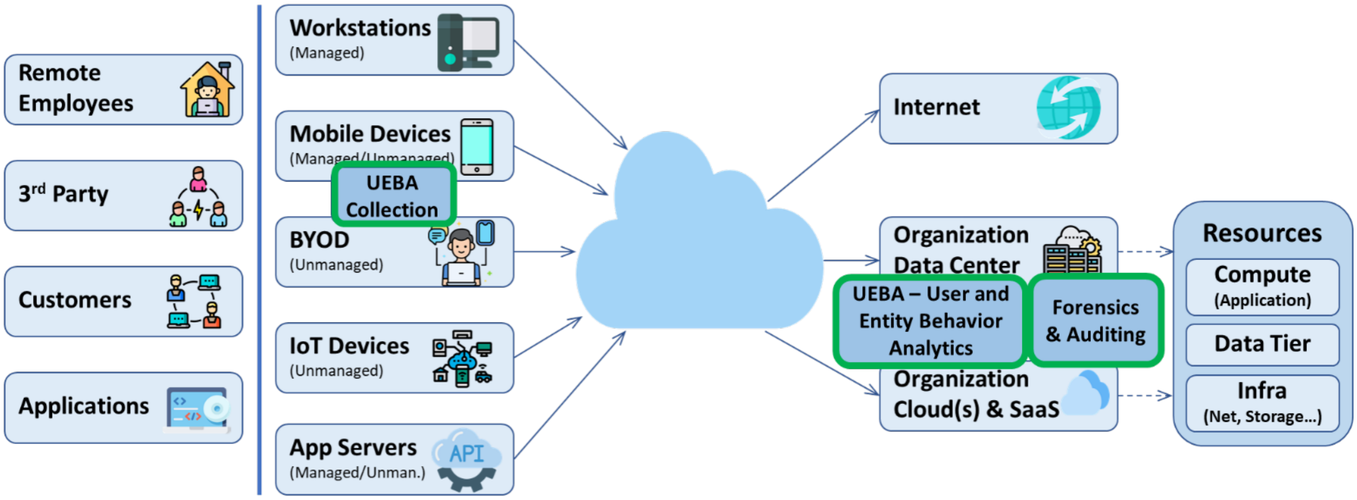


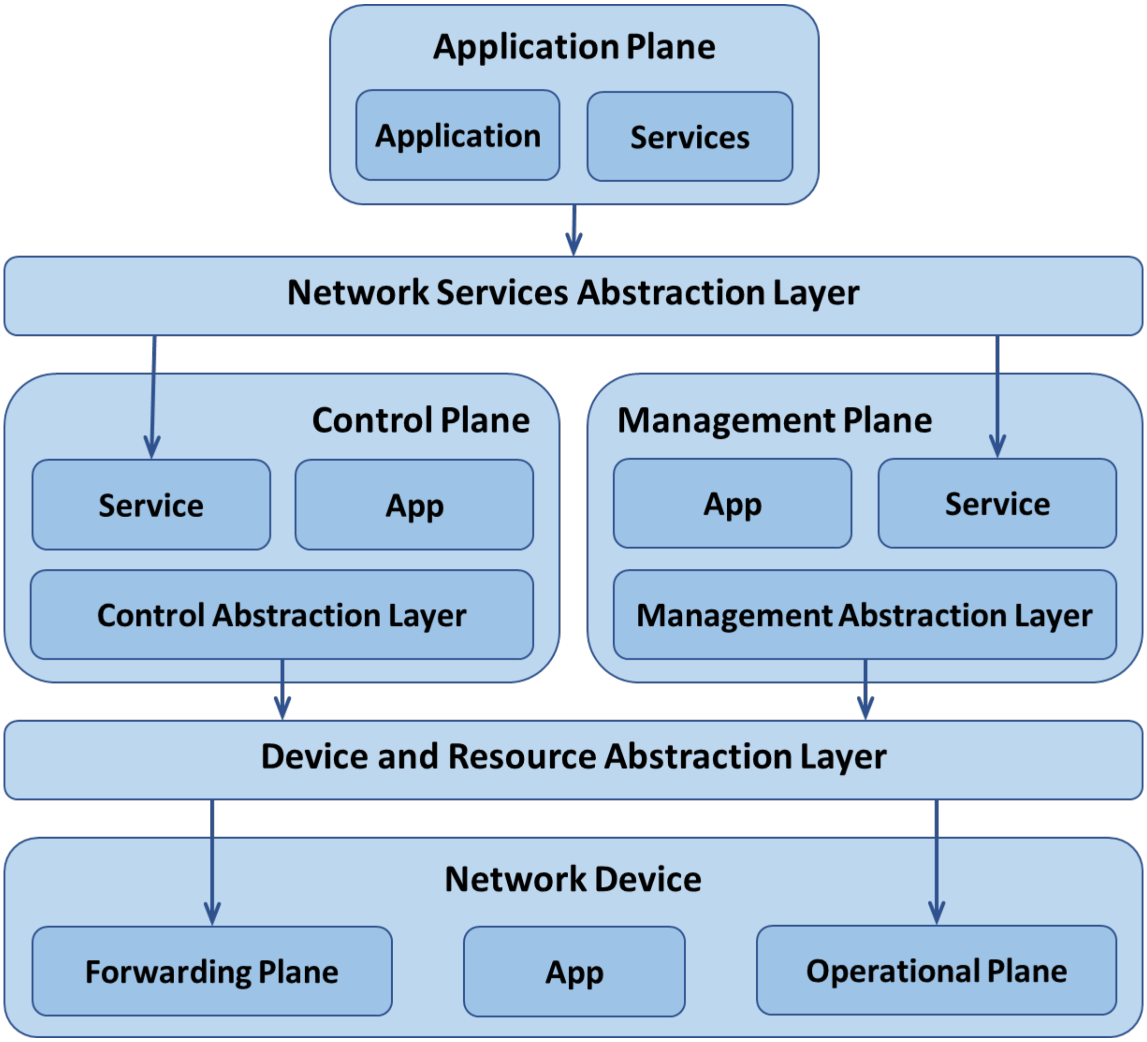
FIGURE 4 **Cloud Access Infrastructure—Analysis**



2. SOFTWARE DEFINED NETWORK (SDN) AND SD-WAN

The modern enterprise is a distributed, global one with remote workers, branch locations, and cloud-based infrastructure dispersed around the globe. As the corporate LAN gives way to the corporate WAN, network traffic optimization between these locations becomes essential for enterprise productivity and performance. Software-defined WAN (SD-WAN) provides a solution for organizations looking to ensure that their corporate WAN meets the needs of their customers, employees, and latency-sensitive cloud-based applications. FIGURE 5 presents the different layers of SDN architecture:

FIGURE 5 SDN Layers Architecture



As SD-WAN continues to be adopted for internet-based WAN architectures, associated security architectures continue to evolve. Security leaders are increasingly moving security out of applications to improve performance and provide standard security solutions to branch offices with direct internet connectivity.

The guidelines and best practices mentioned in this section are based on [1], [2], [3], and [4].

- **General Security**
  - Validate security readiness—Identifying security vulnerabilities during deployment is essential to alleviate them before going live to avoid disrupting service availability.
  - Assess operational security—Proactively monitor operational networks, endpoints, and applications to enhance security by ensuring security functions behave and perform as expected to protect against the ever-changing threat landscape.
  - Certify for security—Security certification must adopt new methodologies that blend network and security testing in the lab and operational networks, using test agents that emulate real-world attacks and proactively identify vulnerabilities.
- **Cloud-based Security**
  - Simplify branch office internet access security by using cloud-based security. The goal should be that traffic destined to an internet site is routed as directly as possible and not routed back to the head office to exit to the internet. Security is often via basic Layer 3/4 security features supported by most SD-WAN products.
  - Consider SD-WAN with an on-site branch firewall only when necessary. An enterprise firewall is typically used to secure branch offices when there are specific needs, e.g., consuming a complicated mix of internet and data center services like collaboration (voice/video), thick client types of applications, etc. Enterprises that need a branch firewall should look toward providers that offer firewall as a service (FWaaS) or allow for hybridization of cloud and branch/datacenter-based appliances by sharing compute workloads or optimizing the network path with already-existing, on-premises equipment. The advantage is avoiding deploying complex functionality in branch offices and using cloud-scalable services located off-network.
  - SD-WANs should offer encrypted tunnels and firewalls. Some SD-WAN vendors provide advanced security, such as a next-generation firewall (NGFW) and anti-malware. These services are usually delivered via the cloud. Depending on the scenario, hybrid environments may provide these services using customer-owned NGFWs.
  - Third-party cloud-delivered security solutions like SWG and CASB should be considered for branch offices where the end-user security requirements primarily focus on securing traffic on the HTTP/HTTPS protocols. The benefit of these cloud-delivered security solutions is that, regardless of the location of the branch and user, their use of globally distributed points of presence can ensure both availability and performance while not sacrificing security efficacy.
  - As enterprises move to use internet connectivity for their branch offices, remote and mobile workers, and various endpoint devices, the task of security becomes a business issue that should be addressed architecturally. Branch office SD-WAN appliances, SD-WAN soft agents, and SD-WAN gateways should be fully integrated with the security functionality.
- **Performance and Reliability**
  - Look for redundancy and failover throughout the SD-WAN. SD-WAN nodes, for example, should be able

to sit out-of-path, and SD-WAN controllers should support redundant and high availability configuration.

- Check support for load balancing schemes (active/active being the most notable), tunnel bonding, and failover times between connections.
- Ask about Quality of Service (QoS) support between the customer premises and the provider edge, type of traffic shaping (interface, tunnel, VLAN, etc.), and rate limiting.
- Limit Use of Public Internet Links—SD-WAN provides improved performance compared to broadband Internet because it optimizes the use of available network links. While SD-WAN chooses the best available link for all traffic, its performance is limited by that link's capabilities. While routing traffic over the public Internet may be cost-effective, the lack of control over routing can cause performance issues. When possible, define SD-WAN policies to route traffic over private links that include service level agreement (SLA) guarantees.
- Perform Regular SD-WAN Testing—SD-WAN is a solution that can help improve the performance and reliability of the corporate WAN. SD-WAN deployments should be tested regularly to ensure that they meet SLAs and provide the network performance and reliability that the organization needs.

3. ENDPOINT SECURITY AND ENDPOINT DETECTION AND RESPONSE (EDR)

Even the most air-gapped, fortified endpoints will likely have some vulnerabilities. According to International Data Corporation (IDC) [5], 70% of successful cyberattacks originate at the endpoint. The risks are many, with interactive endpoints providing direct access to corporate resources and data. Even in highly secured environments, zero-day vulnerabilities in software running on the endpoint, Advanced Persistent Threats, and phishing attempts can create widespread damage to an organization. Attacks may focus on the endpoint itself (denying it of service) or use data gathered from the endpoint and its associated credentials to launch their attack.

Since the scope of this document is to cover secure remote access to corporate applications, user-facing (client) operating systems and devices will be discussed. According to Gartner research [6], security leaders are required to protect endpoints from attacks while allowing access from any device to any application over any network, with minimal impact on user experience. This challenge becomes more complex as companies adopt work-from-home methodologies and allow users to *bring-your-own-device* (BYOD) to connect to corporate resources.

When attempting to secure user-facing endpoints, one should consider the intrusiveness that can be applied to the machine in question and understand the acceptable level of security controls used in a BYOD scenario.

- **Data Security**
  - If users should have access to highly-confidential data or personally identifiable information in or through the organization's data centers, one must consider client-side Data Leakage Prevention (DLP) solutions while thoroughly reviewing the operating parameters and data policies of in-house and third-party software applications that may run on, or otherwise affect the end-user endpoints.

- Such applications may opt to hold extensive offline storage that may or may not be encrypted with strong ciphers. Security administrators must seek to minimize the presence of easily accessible data-at-rest on endpoints with limited client-side security and monitoring measures. This also applies to credentials stored on the operating system or its installed applications (such as web browsers).
- Administrators should consider demanding that unmanaged devices still employ some form of storage encryption to minimize some of the risks attached to this attack vector.

- **Unmanaged, Clientless, or Lightweight Client Device Security**
  - Unmanaged devices are at higher risk of encountering malware through file downloads, being exposed to phishing campaigns over e-mail and other communication channels, and posing a significant risk of leaking corporate data. Ideally, administrators should prefer using managed endpoints to reduce these risks. Nevertheless, administrators may be tasked to support unmanaged and employee-owned devices. In this case, deployment friction and user experience are key in deciding which security software measures to deploy.

When accessing corporate resources

- For unmanaged, roaming devices to be enrolled remotely—administrators may choose to combine a lightweight, non-intrusive device posture scanning agent with a virtual desktop infrastructure (VDI) client while possibly leveraging multi-factor authentication.
- Devices are expected to run up-to-date software with real-time standard endpoint security features (anti-virus, desktop firewall, disk encryption, and default operating system protections).
- Virtual desktops can be used as the conduit through which corporate applications are accessed. Most risks can be detected, prevented, or addressed through security measures on the virtual desktop.
- A refinement to this methodology can be found in clientless SASE/SDP technologies. Products in this segment typically expose corporate resources to the open internet through secure reverse proxies or on-demand application-aware network tunnels. This mode of access is generally provided by leveraging a connectivity software agent, ideally also integrating or implementing device posture security with continuous identity validation as part of the agent's software package.
- Similar to VDI-based remote access, many of the security features in this instance are expected to be deployed in-line or on the server side.
- Ultra-lightweight agents (such as one-off posture checks or self-destructive hardening/environment validation scripts) and browser extensions/native client plug-ins may be leveraged to provide additional coverage for data security, anti-phishing, and malware protection.

When accessing SaaS, the internet, or when using non-corporate applications

- While server-side protections are available when corporate resources are accessed, many of these protections do not apply to SaaS applications and the open web. These unprotected destinations pose risks that can only be effectively mitigated by leveraging a software agent on the endpoints.
- SASE agents typically apply some form of SWG functionality using overriding the OS parameters to utilize

the SASE DNS servers or route internet traffic through the SASE infrastructure.

- Browser extensions and client plug-ins may also be introduced to provide anti-phishing security measures.
- Without leveraging VDI, data leakage prevention risks cannot be considered fully mitigated.

- **Managed Devices**
  - Managed devices give much more freedom to administrators to apply strict security policies with high levels of control. Still, overuse of this privilege can lead to IT support request overload due to exceptions, malfunctions, and the high maintenance required to sustainably manage tightly-hardened endpoints. However, this allows for better security and user experience if applied carefully and with due consideration given to synergies between the “moving parts” of a security stack.
  - Users should be allowed to access applications using their native protocols, running on-device software that communicates with the application directly (or through an application-aware reverse proxy).
  - Administrators should aim to cover the fundamental operating system security control parameters as diligently and thoroughly as possible. At the same time, they may suffer from occasional glitches. Native OS security controls are among the most effective standard risk mitigation tools. They do not necessarily require nor depend on other security solutions to provide most of their value.
  - Native OS security controls (e.g., Microsoft Windows Group Policy Objects, Android / iOS Device Profiles) are typically managed by Enterprise Mobility Management (EMM), Mobile Data Management (MDM), or User Environment Management (UEM) solutions. These leverage as many OS APIs as possible to apply security policies that affect operating system and device behavior and, in most cases, require no agent to deploy. However, they require that the user fully trust the managing organization’s software to run at device administrator privileges.
  - These controls should aim to vet installed applications and block untrusted applications, tighten and monitor the usage of peripheral devices, and prevent the operating system's commonly attacked features or components from running.
  - Once the managed device OS has been successfully hardened by applying a security profile, administrators should consider deployment of Endpoint Protection Platform (EPP), Next-Generation Antivirus (NGAV), or Endpoint Detection and Response (EDR) platforms to combat advanced and basic malware as well as anomalous software-vulnerability-based threat actors.
  - Administrators should review endpoint security platforms’ detection rate and security engine coverage of applicable threat vectors when choosing an endpoint security vendor.
  - Ideally, in addition to core functionality such as real-time antivirus scanning and device encryption management, endpoint security solutions should have some form of behavioral or anomaly-detection-based exploitation prevention, anti-ransomware protections, and functioning integrations with posture scanners and identity agents.
  - Administrators should also take great care to secure credentials or tokens that allow remote administration. Most modern operating systems have facilities that provide single-serving authentication tokens for privileged, locally-defined maintenance.

- In remote access, where auditing and forensics take a significant role in risk management and mitigation, highly integrated security stacks are the key driver in a functional security system and its assumed methodology. Endpoint security solutions for the EDR/XDR (Extended Detection and Response) segment typically include extensive forensic capabilities and auditing features.
- With managed devices, posture scanning is transformed into posture management; administrators should verify that the managed endpoints are running up-to-date software and routinely scan the endpoints for installed applications to detect critical vulnerabilities of outdated software.
- Failure to comply with posture requirements should deauthorize access in all cases.
- Managed devices can manage and deploy their software updates centrally for continuous remediation.
- Additional security measures can include client plug-ins and browser extensions for DLP and anti-phishing.
- As a managed device, more intrusive, context-aware, and system-wide DLP solutions may be deployed to maximize data protection. However, one must only inspect relevant business-related data and avoid personally-identifiable logging or security event creation based on personal data.
- DNS traffic should be made fully visible and available for security inspection. The same privacy guidelines apply.
- Managed devices can introduce a stealthier approach to SASE/SDP by demanding encrypted tunneling of all traffic, including DNS and other plain-text protocols.
- Internet access may be secured using TLS termination, which decrypts the users' HTTPS sessions for inspection. This method should be considered a last resort on high-risk endpoints or high-risk/uncategorized web destinations.
- Remote Web Isolation may also be deployed under the same constraints.
- Browser extensions and client plug-ins should be used extensively if they are well-maintained; they typically provide the most compatible and highest-performing resolution to security issues under their scope.
- Browser extensions and plug-ins can typically be used as "trust agents," authenticators, or DLP, anti-phishing, and malware scanners. They can also be used to enforce the corporate policy on the operating system's native security controls when no primary endpoint security agent is installed.

4. CLOUD ACCESS SECURITY BROKER (CASB)

A Cloud Access Security Broker (CASB) is a gatekeeper that helps organizations monitor and safely use cloud services while ensuring that network traffic complies with the organization's security policies and regulations. With CASB in place to safeguard data, cloud application use across various platforms is visible to consumers. In addition, the actors that pose a threat are identified so that the threat of security violation can be stopped in its tracks.

The guidelines and best practices mentioned in this section are based on [7], [8], and [9].

- **Plan**

  - Gain visibility—When considering a CASB, cloud application discovery is the first place to start. This will let you see which cloud services employees use and the risk posture of each cloud service. However, different CASB vendors have different databases, which may or may not be enriched with adequate risk information. Gain continuous visibility into cloud usage because there will always be new cloud services introduced worldwide, and business units will adopt them, causing changes in the security posture of cloud services in use.

    Select a CASB provider that can provide detailed visibility into:

    - Cloud services usage by category (file sharing, collaboration, payroll, CRM, and so on).
    - Cloud provider security posture assessment against a rich set of attributes.
    - Personal use of sanctioned cloud services. This is also true in infrastructure as a service (IaaS), with cloud services where developers and others create personal accounts.
    - Unknown and risky storage of sensitive data.

  - Plan for adaptive access and identity integration—Integrate your CASB with an existing identity service provider to allow the CASB to enforce adaptive and context-aware access control, such as taking the user's location, the time of day, the time of last access, etc. into consideration. Below are several common adaptive access scenarios that can be implemented using a CASB:

    - Access to sensitive Cloud applications can be blocked entirely if the user is in a hostile geographic region or if a data residency restriction prevents the user from accessing the data from out of the region.
    - Unmanaged devices such as personal home computers or mobile devices are not allowed to access critical enterprise-managed cloud services.
    - Unmanaged devices are allowed to access critical applications, but with reduced functionality—typically "read-only" with no ability to download data locally.
    - When the device, the OS, or the browser represent an additional risk, such as out-of-date versions, they are blocked.

    The CASB project owner should talk to individual application owners and engage in a risk-based conversation with the business owner on how to handle unmanaged devices and mitigate at least some of the risk to a level acceptable to the business unit application owner and security.

  - Closely examine the need to encrypt/tokenize outside of the SaaS provider—Some organizations may be required to encrypt structured data in cloud applications. In such cases, one option is the cloud service provider's native encryption. This approach requires managing each encryption function individually. Using a CASB to encrypt data in cloud applications is recommended because this significantly eases the burden of performing such a critical function for each cloud service. For many organizations, this use case alone justifies using a CASB instead of the cloud service provider for key management.

- Plan to extend the scope to IaaS and PaaS visibility and monitoring—Repeating high-profile vulnerabilities surrounding Object Storage buckets underscores the need to extend the same visibility and control applied to SaaS applications to an organization's IaaS deployment. It is recommended to consider a CASB that extends API support for visibility and control of sensitive data at the IaaS and PaaS layers by integrating with cloud provider APIs to gather and analyze the following:
    - Administrative access and activities
    - Logs of all API-based access
    - Data entering and leaving via APIs to IaaS or PaaS
    - Risky configurations by assessing the security posture of the cloud infrastructure (for example, data stores exposed to the public internet)—Ideally, this would replace the need for cloud infrastructure security posture assessment (CISPA) point products
    - Sensitive data stored in IaaS data stores, file shares, object stores, and databases
    - Malware stored in IaaS data stores, file shares, object stores, and databases

- **Evaluate**
    - Favor multimode CASBs—Some CASBs operate in proxy mode and sit in line between a user and the cloud application. Others take the API approach to securing cloud applications, integrating directly with the cloud application APIs. It is best to choose CASB providers that take a multimode approach, enabling multiple deployment modes:
        - Forward proxies—require some endpoint modification such as the deployment of an agent, VPN client, or proxy auto-configuration (PAC) file. Endpoint agents introduce complexity in deployment and platforms supported, especially for BYOD. Forward proxies also have to deal with how to get visibility into SSL/TLS-protected traffic, typically by some man-in-the-middle approach. However, increased use of certificate pinning breaks this.
        - Reverse proxies—have an advantage in that they do not require an agent to be installed and work well for unmanaged devices where agents cannot be placed. However, reverse proxies do not work with native mobile applications containing hard-coded URLs and certificate pinning. Complex JavaScript applications with embedded URLs can also create issues. Reverse proxy models also require that the enterprise knows what apps to reverse proxy to implement—a problematic proposition when dealing with shadow IT.
        - APIs—provide visibility in ways that proxies alone cannot; for example, visibility into data already located in cloud applications. This also includes access to cloud data by sideloaded applications in the SaaS provider that never touch any network traffic. However, APIs may not provide “inline” blocking and prevention (for example, risky sensitive data exposure is identified only after it has happened).

      An emerging best practice is evaluating a CASB that can extend its security capabilities to in-house custom applications deployed on IaaS platforms using one or more of the aforementioned deployment modes.

    - Look for integration with your Secure Web Gateway (SWG) vendor—Test how CASB will be integrated with SWG via proxy chaining. Another primary use case for integration with an SWG or NGFW is to gain visibility into cloud usage by consuming the logs generated by the solution. It is recommended to use the SWG for cloud malware prevention despite the potential overlap in functionality in that area.

- Weight-sensitive data classification, discovery, monitoring, analytics, and protection as the most critical use cases—The real long-term value of a CASB is in its ability to accurately identify sensitive information and protect it across enterprise cloud applications. For example, cloud data loss prevention (DLP) is critical to a CASB deployment. Since CASB vendors vary significantly in their DLP capabilities, carefully evaluating the accuracy and feature depth of a CASB's DLP is critical to a successful CASB project. In this regard, the following are a few essential capabilities for CASB evaluation:
    - Detection accuracy and out-of-box detection predefined rules with built-in dictionaries for everyday use cases, such as medical and legal terms.
    - Machine learning against established repositories of sensitive data reduces the time to value so that the DLP engine can be trained for the enterprise's specific needs.
    - The ability to perform user and entity behavior analytics (UEBA) for all devices, users, data, and applications to help discover genuine issues in a large volume of logs.
    - The ability to perform risk-based assessments of the sensitive data and their usage and to act based on the risk. For example, blocking sensitive data from being uploaded or restricting their sharing.
    - Possible integration of policies with existing enterprise on-premises DLP solutions.
    - The ability to protect sensitive data when it is moved out of cloud-based services to a managed or unmanaged endpoint.
- Keep contract short-term and be open to switching—CASB capabilities are evolving rapidly as security providers continue innovating. It is recommended not to sign long-term contracts. Instead, organizations should be open to competitive displacement bids if a superior product is available.

- **Deploy**
    - Integrate with existing security infrastructure and Security Operations Center (SOC) processes—Because CASBs are an integral part of an organization's security technology stack, CASB deployments should include integration with existing security technologies like SIEM, IAM, UEBA, DLP, and SWG. The most critical integration of CASB will be the integration with the enterprise SIEM and SOC processes. For most organizations, the SIEM is the system of record for all security-related events, and CASB events will be part of it. From a process perspective, integrate CASB event handling into standard SOC incident workflow.
    - Phase in the CASB control scope and establish metrics for success—The initial deployment should be in monitor mode to establish a baseline and perform a risk assessment and prioritization. Identify one or two cloud services that host the enterprise's most sensitive information and start the project there, expanding to other cloud services over time. In terms of gauging the success of a CASB project, look at the following:
        - The number of cloud services actively monitored and managed
        - End-user adoption
        - Risky behaviors that are blocked

- Amount of time it takes to detect risky exposure of sensitive information
- DLP incidents that are self-remediated by end users
- Compromised accounts/insider threats identified, and the amount of time it took to detect and respond

5. USER AND ENTITY BEHAVIORAL ANALYTICS (UEBA)

User and Entity Behavior Analytics (UEBA) is a technology for detecting and investigating the suspicious activity of users and entities (non-human units, such as hosts, services, applications, network traffic, etc.). UEBA solutions profile and detect anomalies in users' and entities' behavior using analytical methods like rule engines and machine learning. Employees leave digital footprints during their day-to-day work by accessing files, running applications, visiting websites, etc. Significant deviations in their behavior may be a sign of malicious activity or a compromised account. UEBA may spot potentially risky user activity before an incident happens. UEBA's benefits include automating analytics, preventing data exfiltration, and detecting compromised accounts and malicious insiders.

The guidelines and best practices mentioned in this section are based on [10], [11], and [12].

- Define the use cases to address, e.g., identification of malicious insiders, compromised users, known security threats, or zero-day vulnerabilities. Knowing what risks to identify and what output to expect from the UEBA tool will hint at what data to collect for behavior monitoring.
- Define data sources, e.g., events and logs, business context data, and HR information like performance history, network flows and packets, corporate emails, and social media activity. The more data types a tool will handle, the more precise the baselining will be.
- Integrate data from other monitoring systems, such as advanced threat management and customer relationship management (CRM) systems.
- Enable Active Directory auditing to track who is doing what across your critical systems.
- Enable auditing for all systems that contain sensitive information.
- If you use SaaS applications, enable access and user activity logging.
- Track account creation and logins because such activity can reveal account takeovers and other attacks.
- Define behavioral factors to collect—The effectiveness of UEBA tools highly depends on the variety and amount of data they collect for analysis. UEBA tools can gather and analyze information upon various factors, such as working habits (rhythm, location), user activities (accessing of application, corporate data, and websites), context (psycholinguistic indicators and non-IT data), and biometrics (keystroke and mouse dynamics, eye movement).

- Allocate appropriate time for establishing the baseline, considering the specifics of the business and time of the year (do not select a peak period of employee activity for baseline). Spending too little time monitoring work activities may result in a high rate of false positives.
- Update security policies and conduct awareness training—Ensure to inform employees about the deployment of UEBA tools from the beginning, telling how the technology will be used, and conduct awareness training. Comply with predetermined escalation procedures that include the participation of HR, legal counselors, and team leads when investigating incidents. Analyze alerts with extraordinary care so that dedicated employees do not begin to think they are no longer trusted.
- Consider both internal and external threats when creating new policies and rules.
- Ensure only relevant team members receive UEBA alerts.
- Do not consider non-privileged user accounts as harmless. Attackers commonly gain control of standard accounts and escalate privileges to penetrate sensitive systems. UEBA systems can help detect unauthorized privilege escalation.
- Use other security solutions to double-check for incidents or security violations that may occur during the baselining period.
- Conduct acceptance testing of UEBA tools—Once the baseline is established, conduct acceptance testing of the UEBA tool to see how it works and whether it needs any improvements. First, define the use cases you want to test. Then, run the system for testing purposes and analyze its output. Review the findings and explore the rate of false positives. If the rate of false positives is too high, you may need to enrich information about user activity with additional monitoring data by continuing the baselining period.
- Fine-tune the UEBA system’s rules, alerts, reports, and thresholds to reduce noise and false positive anomalies.
- Rebuild the baseline periodically—User and entity activities may change. Employees can change their tasks and projects, so their behavior will vary from time to time. Most UEBA systems automatically collect data and adjust the baseline periodically, thanks to their machine learning algorithms. However, when the enterprise faces significant structural or personnel changes, establish a new baseline for the continued effective operation of the UEBA system.

6. ZERO TRUST ARCHITECTURE (ZTA) AND ZERO TRUST NET ACCESS (ZTNA)

The adoption of Zero Trust methodologies and solutions is a process. While several turn-key solutions exist, their efficacy is always constrained by incomplete asset coverage and inefficient information systems design. Therefore, one of the most fundamental requirements for a healthy Zero Trust system is to have the broadest possible coverage regarding good, real-time visibility of all participating nodes in the network (this includes BYOD and external endpoints that can access the organization remotely).

The guidelines and best practices mentioned in this section are based on [13] and [14].

- Validate the security posture of participating nodes, and mitigate risks using standard APIs where applicable. In this context, the first steps to be applied are:
  - Asset visibility and control. Multiple solutions in the market are available to discover and map all networks, endpoints, and their configuration parameters. Cyber Asset Attack Surface Management (CAASM), Unified Endpoint Management (UEM), Network Access Control (NAC), and Network Traffic Analysis (NTA) solutions are all relevant utilities when attempting to fully map the organization's digital assets and entry points. They exercise control over their functionality to varying degrees.
  - Grading the assets on their potential risk to the organization when compromised (based on the actions that can be carried out on them and their exposure to other assets).
  - Applying a context and risk-based security policy to user access. This policy (and the security controls that enforce it) should be used to govern cybersecurity solutions and their operating parameters for a given session, based on:
    - The degree of risk that applies to interactions with the application in question.
    - The continuous validation of the identified user being the actual source of application activities and interactions
    - The continuous validation of the accessing device's security posture.
- Even a fully-mapped organization will fail to deliver strong security without various highly-serviceable Policy Enforcement Points (PEPs). PEPs range from network-based security gateways and core in-line equipment to host-level security controls, SDK/API-based integrations, application plug-ins, hooks, and wrappers, or full endpoint agents that can control running applications directly, either on the client side or server-side.
  - In contrast to network-based security controls, active security controls—those that integrate with application controls available in running programs—can be highly effective at surgically mitigating risks in real-time. Integrated security controls provide a higher level of visibility into application usage for auditing and behavior-based continuous authorization.
  - In an ideal system, one could potentially manage not only the entire network path leading to and from the application on a per-user, per-session basis but also engage in multi-way handshakes and communication between all security controls and PEPs that apply to any given session, allowing for load sharing and high-resolution collaborative enforcement between the PEPs. Such a "software-defined enforcement" environment can highly synergize and optimize the use of network-based, agent-based, and application-integrated PEPs, as mandated by the PDP's governance over offloading parameters and orchestration of the security controls applied to the session.
- An additional layer can introduce varying levels of confidence and compliance in user identity and device posture metadata, lowering friction caused by authentication prompts or software deployment requirements based on an inherent understanding of the underlying application's API, business logic, or available front-end actions. This is highly relevant for administrators deploying applications in a "clientless," web-based manner, typically to provide access to unmanaged endpoints.

- Continuously manage risks and audit the session activity; once anomalous behavior, a cybersecurity risk signal, or a device anomaly is surfaced, the security controls should apply a stricter policy, which could, for example, require additional authentication, enable full session recording, or shut down access to resources due to low confidence in the end-user's identity establishment and unsatisfactory device posture compliance.

- Multi-factor, multi-dimensional authentication solutions (e.g., across multiple devices or by baselining authenticated device environmental signals) should ideally be adopted to reduce friction in a practical Zero Trust system while increasing confidence levels for sustainable user identity establishment. Solutions that leverage as many signals and authentication factors as possible, ideally without engaging the user for manual interaction for authentication, would be ideal in ZTA.

- Behavioral Biometrics and device signal analytics, withdrawn from the accessing device and the way the user interacts with it and with the application, can be used to create an initial baseline for identity establishment and can be continuously sampled without direct user interaction. Various confidence levels can be established with other authentication factors, such as hardware tokens, biometric credentials, or other software-based OTPs. Risk mitigation can be done by leveraging additional authentication factors and increasing confidence when necessary. Different Identity Governance and Administration (IGA) solutions can help facilitate this.

- Organizations adopting a ZTA will benefit from good IT hygiene. ZTA will optimize the organization's general security posture by utilizing common, shared services, reducing information system infrastructure complexity, and eliminating/consolidating unnecessary systems, system components, and services—employing the least functionality principle. This should be reflected in the network topology and access control lists, managed by network security gateways or on-device controls, adhering to micro-segmentation concepts that segregate nodes and limit their network access to white-listed destinations and sources.

- Leverage typical configuration and deployment templates to reduce the attack surface while increasing the manageability of all underlying assets in the ZTA ecosystem.

- Eliminate as many permanent or ambiguous authorizations defined on their systems. This includes eliminating redundant, temporary, hard-coded, or globally non-provisional roles, permissions, tokens, or keys of users, machines, or services.

- Consider leveraging Key Management Service (KMS) and Privileged Access Management (PAM) solutions to avoid key and credential reuse or exposure. This applies to both cloud and CI/CD workloads and nodes as well as end-user nodes in the context of remote access.

- Consolidate log and signal ingestion to unified systems (such as SIEMs) that apply correlated analytics to their inputs. In the context of ZTA and ZTNA, this is primarily relevant when attempting to establish a Cybersecurity Mesh Architecture by leveraging a central Policy Decision Point (PDP) with integrated Policy Enforcement Points (PEPs) and a Security Orchestration, Automation and Response (SOAR) system. These should ideally be integrated into a singular mechanism.

7. MULTI-FACTOR AUTHENTICATION (MFA)

Multifactor authentication (MFA) is a security process that requires more than one method of authentication from independent sources to verify the user’s identity. A typical example is to log in using a username and password; a one-time code is generated and sent to the user's phone or email as a second factor. MFA can be used to add a layer of security when accessing sensitive information or whenever enhanced security is required, e.g., accessing primary email, financial accounts, and health records. Some organizations require using MFA; others provide it as an option. As users, if you have the option to enable MFA, you should do it to enhance your security.

The guidelines and best practices mentioned in this section are based on [15], [16], [17], [18], and [19].

Principles of an exemplary MFA implementation include the independence of authentication mechanisms, protection of authentication factors, and ensuring that no knowledge of the success or failure of a factor is provided to the individual until all factors have been submitted. When and how MFA should be implemented depends on several factors, including the threat model, the users' technical level, and the administrative control over the users. The following recommendations are generally appropriate for most cases and provide an initial starting point.

- **General**
  - Provide the option for users to enable MFA on their accounts using TOTP (Time-based One Time Password).
  - Require MFA for administrative or other highly privileged users.
  - Consider allowing corporate IP ranges so that MFA is not required when logging in from these IPs.
  - Allow the option for browsers to remember the use of MFA, so users are not prompted every time they log in.
  - Implement a secure process to allow users to reset their authentication methods.

- **Account Recovery Flow**
  - Independence of primary and secondary factors—Separate the recovery of the first and second factors. Should an attacker gain access to the primary authentication factor (e.g., password), the second factor becomes irrelevant if it can be reset with possession of just the password. Further, the recovery flow for the second factor should be completely separate from the recovery flow for the primary authentication. For example, if an email message is a method for recovering a password, make sure to recover the second factor through an altogether separate channel.
  - Involve an administrator—An administrator can, in many scenarios, implement a sophisticated high assurance authentication method
  - Provide a backup second factor—Many scenarios require an automated method for recovering the second factor. Enrolling the user in more than one-second factor at the time of registration allows the user to

recover a second factor by completing authentication through a third factor. One notable, simple, and low-cost example is to provide users with a card (either physical or printable) with a set of codes that can be used only once and that can be used as a backup for the second factor.

- **Protection Against Attacks**
  - Login flow sequence—Place the challenge for the second factor on a different page than the login page. This has two benefits: first, it protects users from an attack aimed at locking them out of their accounts once a failed login attempts limit is reached (with rate limits applied to the primary factor); second, obscuring the second factor provides an attacker with less visibility into the other layer of security.
  - Rate limits and account locking—Implement a rate limit and lock policy on the second factor. The probability that users enter their tokens incorrectly multiple times is low. Therefore, the suspicion of attack should grow with each failed attempt. Response times should increase with each subsequent attempt to decrease the total number of attempts per time unit, with a complete account lockout (where feasible) upon several consecutive failed attempts. For time-based second factors, manage rate limits according to the token's life.
  - Logs and alerts—Collect and analyze unsuccessful MFA attempts. In the event of several failed MFA challenges, alert the administrator of this suspicious behavior, and prompt the user to enroll a new token.
  - Use an out-of-band token—A second factor verified through a separate channel than the primary factor adds extra protection against brute-force (and phishing) attacks. For example, a popular new factor sends the user a push notification on a mobile phone with details about the authentication request and a prompt to accept or deny the request. This channel is inaccessible to a traditional brute-force guessing approach.

- **Design to Manage Risk, Usability, and Cost**
  - Offer a spectrum of MFA options—Different user populations present different levels of risk and require different levels of authentication. For example, an administrator can have a larger scope of access than an individual user. Therefore, you may want to provide stronger second factors for administrators while offering more convenient options for users. In consumer scenarios, different users have different preferences, and a low assurance, more convenient alternative may provide more security than a high assurance option that lacks adoption.
  - Support federated authentication—In enterprise scenarios, many companies implement MFA locally for identities they manage. This approach allows product vendors to outsource the administration of policy and security processes to customers. Enabling customers to implement MFA independently allows them to optimize the process according to their specific circumstances and constraints. For example, customers can design administration of account recovery to suit their particular IT function. This outsourced approach allows users to access all resources using one token.

8. IDENTITY AND ACCESS MANAGEMENT (IAM)

The first step of IAM, identity proofing, is described in NIST SP 800-63A [3] for three identity assurance levels. An applicant provides identity evidence and attributes, is uniquely resolved to a single identity, then validated and verified. The purpose of Identity proofing is to ensure the applicant is who they claim to be to a stated level of certainty by presentation, validation, and verification of the minimum necessary attributes. The authentication process is described in NIST SP 800-63B [4], while federation and assertion are covered in NIST SP 800-63C [5].

The guidelines and best practices mentioned in this section are based on [20], [21], [22], [23], [24], [25], [26] and [27].

- **Identity Management**
  - Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. Validate that all active accounts are authorized on a recurring schedule at a minimum quarterly or more frequently.
  - All activities performed with an ID (including root) must be associated with an individual user. Users must be held individually accountable for all actions they perform with any ID they are approved to use.
  - Chang or remove access rights to promptly reflect changes in or termination of employee or contractor job function or third-party agreements.
  - Disable inactive user accounts after no more than 60 days of inactivity. Disabled user accounts should be deleted within one year.
  - Centralize account management through a directory or identity service.
- **Passwords**
  - Implement password-less login where possible.
  - The system must require a minimum password length of eight characters, which includes three of the following: one upper case letter, one lower case letter, one number, and one special character.
  - Users should be advised of the parameters and security benefits of strong passwords and encouraged to create strong passwords.
  - Users must not create passwords that constitute common keyboard combinations (e.g., QWERTY), common dictionary terms, or easily obtained personal information.
  - Systems must require users to create their own passwords the first time they log in with a temporary password.
  - For privileged IDs, the system should require two-factor authentication and passwords of at least twelve characters with all of the following: one upper case letter, one lower case letter, two numbers, and one special character.
  - The system should maintain password history and prevent using the same password within seven

iterations of a password change cycle.

- Passwords for IDs with control of an enterprise credential repository (e.g., Active Directory) must not be fully known to a single person, but knowledge should be split. These passwords should be renewed annually.
- All passwords created as part of the development process must be changed by production support staff immediately upon promotion to production.
- Passwords must not be included in any automated login process (e.g., stored in a macro or function key), including Remember Password functions.
- Passwords that are compromised or suspected of being compromised must immediately be changed, or the ID must be disabled or suspended.
- All authentication credentials (such as passwords/phrases) must be cryptographically protected during transmission and storage.

▪ **Access Management**

- Implement zero-trust security: presume that no one is trustworthy unless proved otherwise. The zero-trust model is focused on continuously authenticating consumers—activities are tracked, and risk levels are evaluated during each session.
- Access to the organization's resources should be denied by default unless expressly permitted by the resource owners, i.e., deny all access that is not explicitly granted and remove all system access not explicitly required.
- Access to the organization's resources must require a login process that includes a unique ID and authentication through a reliable and secure means.
- Using access control procedures, ensure access and privilege (read, write, delete, execute, etc.) to the organization's resources are restricted based on the principles of least privilege, need to know, and segregation of duties.
- Define and maintain role-based access control (RBAC) through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties and restricting non-essential access to sensitive information.
- Implement an access management life cycle process: how additions, deletions, and modifications to access privileges and IDs are managed, authorized, and tracked.
- Any prompts for ID and password should be generic and must not identify the version or build number of the operating system or platform accessed. Any response must not reveal if the user name or password was wrong.
- Lock terminals after fifteen minutes of inactivity and require re-authentication to regain access.
- Restrict user access to applications based on the time-of-day requirements defined by the organization.
- Do not allow generic and shared user IDs for system administration and other critical functions.

- Restrict all access to any database containing data with a protection categorization of High (including access by applications, administrators, and all other users).
- If presenting services to untrusted networks, such as the Internet, isolate the external-facing access management components from the rest of the systems.

Privileged Access

- Limit the assignment and use of privileged IDs to a minimal number of persons responsible for operational system support or administration.
- Manage privileged accounts by the enterprise privileged account management tool.
- Privileged accounts should only be used when performing authorized administrative tasks.
- Issue separate user accounts to users who should perform both privileged and typical day-to-day functions.
- Avoid users performing privileged actions from untrusted devices.
- When working across network boundaries or zones, prefer access from the more trusted environment to the less trusted environment.
- Monitor privileged user actions by defining rules that could detect suspicious activity.

Remote and Non-person Access

- Device, service, and application accounts should be assigned to an account owner and must not be used by individuals to access the system. These accounts should be managed by the enterprise privileged account management tool.
- Authenticate all remote access with multi-factor authentication, e.g., password and logical security token, and utilize encrypted connections.
- For all remote access, the system should validate that all computers and devices that require access to a network or system are securely configured and meet the following security requirements: up-to-date system patches, current anti-virus software, and functionality that provides the capability for automatic execution of code disabled.
- Permit remote administrative access only for compelling operational needs; strictly control and monitor them.
- Accounts used by vendors to access, support, or maintain system components via remote access should be enabled only during the time needed, disabled when not in use, and monitored when in use.

OT Access Management

- OT should not be administered from an enterprise IT domain.
- OT systems should not rely solely on systems in a lower trust domain for authentication and authorization.
- When data needs to be transferred between IT and OT systems, ‘push’ data from the OT domain to the IT domain and avoid allowing systems in the IT domain to reach into OT systems.

    - Where system-to-system communications are needed across IT to OT boundaries, ensure they are in an inspectable format and are monitored and validated at the boundary.

- **SecaaS (Security as a Service) IAM**
    - To avoid vendor lock-in, cloud environments and services should be portable. Using standard protocols and interfaces for integrating cloud-based IAM services can simplify technical aspects of portability.
    - SecaaS IAM providers should be able to dynamically scale up and down based on the requirements of the service consumer.
    - SecaaS IAM services should provide two-factor authentication.

9. BIOMETRIC AUTHENTICATION

Utilized alone or integrated with other technologies such as smart cards, encryption keys, and digital signatures, biometrics is set to pervade nearly all aspects of life. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as passwords or PINs). As e-government applications accelerate globally, the use of biometrics will accelerate to enhance citizen trust in e-gov services.

The guidelines and best practices mentioned in this section are based on [21], [28], [29], and [30].

- **Organizational**
    - Make sure you are not using biometrics for technology’s sake but rather to solve the organization's problem.
    - Try getting senior management's full support and involvement to have successful implementations.
    - Plan for a lengthy biometric enrollment process. A biometric system may require more processing time than traditional authentication methods such as passwords or smart cards.
    - Plan for post-implementation support. Biometric systems require a lot of back-end support, without which their implementation would not be successful.
    - Plan initially on implementing biometrics on a small scale.
- **End Users**
    - Employees may mistrust technology and see it as more of an impediment to their job rather than an enabler. Plan for an education process that can explain to employees why the biometric system is needed and how it could benefit their jobs.
    - Make extensive efforts to inform employees so they understand how their biometric data would be collected, what the data would be used for, if any health problems may arise, and whether enrollment is voluntary or involuntary.
    - Biometric systems should allow users who may be unable to present the specific biometric used by the system.

- Plan for user training in biometric enrollment and subsequent use.

- **Technology**
  - Biometrics should be used only as part of multi-factor authentication. Adding a biometric as an additional step in the authentication process may improve overall security.
  - The biometric system should allow no more than five consecutive failed authentication attempts.
  - Biometric devices in the field should be capable of operating in stand-alone mode. This becomes critical when there are network breakdowns or power outages. On the other hand, organizations should reduce the amount of sensitive information about employees stored at any time in biometric devices operational in the field.
  - Find the right balance of processing speed and accuracy trade-offs when selecting a biometric for an application.
  - Achieving the accuracy and quality of biometric samples recorded on a system is critical to obtaining reliable results from the system use.
  - Searching and processing biometric data can be computationally intensive. Use the right solution to fit the relevant use case. Cloud services may help in dealing with requirements for flexibility and growth.
  - Try to avoid vendor lock-in by selecting vendors that comply with standards.
  - Prefer a system that collects “signals”—information that helps reassure the person is acting within norms post-log-in, provides real-time alerts, and offers machine learning to add strategies for identifying fraudsters in the system.
  - Prefer a system that enables authentication when users log in using multiple devices.
  - Compliance with relevant standards has significant advantages—interoperability of data and systems; faster and cheaper development of solutions; lower lifetime cost (initially and when upgrading the solution); interchangeability of components; easier and better testing.

- **Security and Privacy**
  - Security is essential for protecting the correct functioning of the system and avoiding corruption or loss of data or processing capability of the system itself.
  - Take all appropriate technical and organizational security measures to protect personal biometric data during storage, biometric template extraction, and transmission to central servers for authentication.
  - A biometric system inherently stores personal data, which therefore needs protection from attack and improper processing, such as disclosure to anyone not entitled to receive it.
  - Enrolment data packets (individual electronic files containing resident demographics and biometrics) should be strongly encrypted by the Enrolment Client software at the time of enrolment, even before saving any data to any hard disk.
  - User protections are critical, such as clear opt-in, opt-out, the right to review data, and the right to delete data; such protections are enshrined in the GDPR.

- The system should detect attempts to deceive (or 'spoof') the system by presenting a false biometric sample or image (Presentation Attack Detection).
- Client software should run in a secure environment, such as a Virtual Machine, to prevent malware infection and modification to the client software.
- Before any implementation, perform a Privacy Impact Assessment (PIA) exercise conducted by accredited agencies or specialized law firms to guarantee that this program is in complete adherence with the GDPR and/or the national legislation at stake in the country of deployment.
- For defense organizations, the system should set up a device certification process to ensure all biometric capture devices are certified for use.

10. ZERO KNOWLEDGE PROOF AUTHENTICATION

As this is a sub-technology used in the authentication process, it is covered in previous sections.

11. CLOUD FORENSICS

Digital forensics is a branch of forensics handling the recovery, investigation, and analysis of material found in digital devices. Cyber forensics deals with techniques used to track the footprints left by a cyberattack. Cyber forensics is intensely employed in incident response, malware analysis, data leak protection, and any cybercrime investigation. Cloud forensics is cyber forensics when the examined artifacts reside in the cloud.

The guidelines and best practices mentioned in this section are based on [31], [32], and [33].

- **Policy and SLA**
  - Have a well-documented digital forensic process. This can be part of the incident response policy and procedures, but it should cover the complete forensic investigation/evidence lifecycle. The required training and expertise of forensic examiners should also be covered under the same policy.
  - Predefine a set of corporate-approved tools to be installed as part of any instance deployment in the cloud platform, which includes forensic-enablement tools.
  - Establish logging requirements for cloud platforms (compute/server, network, or storage) and set the severity level, timestamp format, and retention and rotation periods. Define where else logs should be sent (e.g., event correlation tools—SIEM).
  - Build a forensic playbook that describes procedures to be followed as part of the corporate incident-response (IR) procedures and policies.
  - Enable logging and auditing in the cloud environment (all pipelines, compute, network, and storage instances) by corporate policy.

- Enable consistent time synchronization among all systems within the private cloud zone or region.
- Establish training requirements for staff members handling security incident response and digital forensics. Make sure staff has active and valid certificates about their specialty.
- Ready forensic server image (forensic acquisition and analysis tools, cloud API command-line tools) and version it for all deployed CSPs. This includes processes on how the IR team obtains the required access to carry out all of their mandatory investigations' tasks.
- Acquire and document from the chosen CSP a clear process guiding how law enforcement agencies can approach the CSP for information requests.
- Ensure that the SLA clearly defines the timeframes and mechanisms for the CSP to notify consumers about data breaches or security incidents to the consumer platform or the cloud underlay infrastructure.
- Define with the CSP which logs from the underlay infrastructure can be exposed during forensics examinations, if requested, what the request process will be, and how long the log retention periods.
- Describe the types of logs to be maintained regarding the deployed IaaS cloud and the retention periods for each type of log. Specify recoverability after deletion options for every kind of log.
- Define ownership of the data residing in the corporate cloud instances and any derivatives of it.
- Define data storing location(s) by agreeing with the CSP on the corporate authority to decide where all the data is stored for the deployed environment (country, state, and jurisdiction).
- Clarify the process of retrieving encryption keys from the CSP (if required or lost) and capture any limitations to data decryption.
- Define data-volatility recovery options (elastic autoscaling groups and resources): what type of data can be recovered for every kind of ephemeral resource, and what are the associated time constraints.

▪ **Identification**

- Evaluate organizational configuration or development platform models: private, community, public or hybrid cloud. Evaluate the service model supplied by the provider being analyzed: SaaS (Software as a Service), PaaS (Platform as a Service), or IaaS (Infrastructure as a Service).
- The detection of an incident in a cloud environment may differ according to the model adopted for the services. The adoption of the cloud in intrusion detection systems can be implemented by the user in the IaaS or even by the CSP in cases involving SaaS or PaaS.
- Interact with the provider's professionals to map the incident and damage extent.
- Identify if the provider performs regular snapshots, object auditing, and multiple backups.
- Identify the particular data sought, relevant time periods, the involved cloud service providers, and the utilized services.
- If using an acquisition option requiring the service provider's involvement, identify a legal point of contact for the provider and consider the provider's policies regarding user notification of the legal process.

- **Preservation**
  - Implementing preservation techniques may require isolating cloud resources, which can cause performance degradation for other clients. Providers should isolate the physical disk connected to an incident, considering that data from other customers sharing resources could also be copied.
  - The chain of custody must start when the researcher has access to physical media. Implement contracts that allow the investigator access to the evidence, sometimes physically, not just with network access, or even a chain of custody that begins with the provider and then is transferred to the client.

- **Collection**
  - Consider using the Cyber Forensic Field Triage Process Model (CFFTPM), which proposes an onsite or field approach for providing the identification, analysis, and interpretation of digital evidence in a short time frame, without the requirement of having to take the system(s)/media back to the lab for an in-depth examination or acquiring a complete forensic image(s).
  - The memory capture and other states might be limited to an interface available to the customer, and it may be virtually impossible to shut down a machine to remove the disc or boot via live CD. Therefore, establish remote collection strategies.
  - The expert would be performing the imaging of a disc through duplication bitstream equipment. In the cloud, an interface apparently on a single disk is divided into multiple physical disks. The expert's challenge is knowing each segment that composes the target and is interesting for the investigation, cloning the devices (defining the start and end clusters), and then having the capability to concatenate them in an investigation environment. Thus, the expert will have to deal with the concept of distributed multi-tenant, such as Google GFS.
  - The provider should be responsible for extracting the forensic image of a physical disk or partition, or at least a virtual machine created for the client by handling the hypervisor. They should be cautious when handling the hypervisor. It will be usual for cloud providers to provide snapshots of the disk and client memory. This generation should be documented and assisted by an expert for the customer so it can be used as digital evidence in court. This approach will help ensure that the hypervisor was reliable.
  - In the live collection, consider all endpoints; the generation of the timeline of events should consider time synchronization, which is difficult and demands specific tools.
  - Assess whether the system already has a solution to generate hash files from the cloud and provides support for a remote binary copy.
  - Evaluate if the examined system offers versioning of erased or overwritten files/objects and how these mirrors can be accessed.
  - Keep notes during the acquisition process to document information regarding system information, methods used, or how the data is received. Photographs and screen capture may also be used instead of or in addition to, written notes to document data with evidentiary value. This step is crucial to help ensure the integrity of the process.
  - Note that some systems may utilize local storage in addition to cloud storage. With proper legal authority,

any local data should be acquired.

- **IaaS-Related**
  - When possible, preserve evidence source and isolate the server to a secure location where the only permitted access is from the forensic examiner workstation; to minimize additional changes and lessen the impact on the investigated server, the server must be isolated to a secure location.
  - Expect collection cycles because case-relevant data may be located in many places in the cloud environment. While the collected data may be analyzed on the forensic server, additional data might be required to construct a timeline or uncover a relevant event.
  - If data transfer is required, transfer the data using the appropriate transfer mode for the file type (binary/ASCII). This makes sure the data is transferred bit by bit without losing information. The file transfer should be encrypted or local between the forensic workstation and the examined server/destination storage.
  - Use tools compiled from the source before being used, capturing the calculated executable hashes via the continuous auditing mechanism or tools that are well known and trusted within the community (preferably certified under NIST CFTT) or natively provided by the provider authenticated interface. The tools' authenticity must be validated and captured via a continuous integrity mechanism.
  - Check all collected evidence with analysis tools to validate the hash value, the completeness of the acquired data, and the possibility of gathering the needed information from the collected data. This is important because collected data can be corrupted, inoperable, or irrelevant to the ongoing investigation (for the purpose it was generated).
  - Once files have been transferred to the forensic server, check the hashes for all collected files against the original values. If confirmed, then the forensic examiner can carry on the forensic analysis.
  - Save all artifacts generated from the acquisition process directly on write-once read-many storage. This requirement helps ensure the integrity of all artifacts and evidentiary data throughout the forensic lifecycle.
  - Store evidence near where the data was collected and perform as much as possible of the forensic examination in an isolated network on the investigated public cloud. Since the incident occurred in the public cloud and data acquisition took place in the public cloud, it makes sense to isolate the evidence to avoid mishandling. This measure also greatly helps reduce the amount of data that must traverse between the customer network and the cloud services provider network. This also helps reduce the chain of custody.

- **Examination and Analysis**
  - The timestamping should be considered in the collection phase and also in the analysis phase.
  - A knowledge process involving all jurisdictions should be adopted and timestamps applied to services.
  - Regarding the logs, it is the experts' task to be familiar with the most used platforms, knowing how they are generated, so they can use a parser efficiently, detailing their report effectively.

- **Presentation**
  - When applying a determined known technique, the Court should consider the potential rate of error and the existence and maintenance of standards and controls on their operation.
  - It is highly recommended that cloud Provider's technicians sign along the client's expert report, ensuring uniformity of opinions and avoiding exploitation thesis as self-defense on the argument that the provider was unaware or did not recognize what was performed by investigators.

12. ACADEMIC SURVEY OF CLOUD SECURITY GUIDELINES

We could not find any academic paper regarding cloud security guidelines.

13. SUMMARY AND NEXT STEPS

Guidelines and best practices regarding the selected cloud security technologies were presented.

In the subsequent phases, the standards gap regarding cloud security technologies will be evaluated, and ways for raising awareness of Cloud Security with the presented best practices, e.g., workshops and conferences, will be examined.

14. REFERENCES

The following sources have either been referenced within this paper or may be helpful for additional reading:

[1] Gartner, Best Security Practices for SD-WAN, https://www.gartner.com/doc/reprints?id=1-279UF3IS&ct=210823

[2] Mushroom Networks, Best Practices for SD-WAN Deployment, https://www.mushroomnetworks.com/blog/best-practices-for-sd-wan/

[3] Check Point, Top 4 SD-WAN Best Practices, https://www.checkpoint.com/cyber-hub/network-security/what-is-sd-wan/top-4-sd-wan-best-practices/

[4] Spirent, How to Tame SD-WAN Complexity, https://www.spirent.com/blogs/how-to-tame-sd-wan-complexity

[5] International Data Corporation (IDC), https://www.idc.com/

[6] Gartner, https://www.gartner.com/en

[7] Gartner's 10 Best Practices for Successful CASB Projects, https://www.mcafee.com/blogs/enterprise/cloud-security/gartners-10-best-practices-for-successful-casb-projects/

[8] A Comprehensive Guide to Cloud Security in 2022 (Risks, Best Practices, Certifications), https://kinsta.com/blog/cloud-security/#what-is-a-cloud-access-security-broker-casb

[9] Oracle CASB for Oracle Cloud Infrastructure, https://www.oracle.com/us/solutions/cloud/platform-as-a-service/oracle-casb-oci-5043476.pdf

[10] Ekran, 7 Best Practices for Building a Baseline of User Behavior in Organizations, https://www.ekransystem.com/en/blog/best-practices-building-baseline-user-behavior

[11] Netwrix, User Behavior Analytics: Best Practices You Should Start Now, https://blog.netwrix.com/2016/10/18/user-behavior-analytics-best-practices-you-should-start-now/

[12] Imperva EUBA, https://www.imperva.com/learn/data-security/ueba-user-and-entity-behavior-analytics/

[13] NIST SP800-39 2.6.2 Trustworthiness of Information Systems, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[14] NIST SP800-37 Revision 2, Risk Management Framework for Information Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[15] PCI Security Standards Council—Guidance for Multi-Factor Authentication

https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf

[16] PCI Security Standards Council —Understanding new PCI guidance on MFA https://blog.pcisecuritystandards.org/understanding-new-pci-guidance-on-mfa

[17] NICCS—A how-to-guide to MFA

https://niccs.cisa.gov/sites/default/files/documents/pdf/ncsam_howtoguidemfa_508.pdf?trackDocs=ncsam_howtoguidemfa_508.pdf

[18] OKTA—Building Secure Multi-Factor Authentication—Three best practices for engineering and product leaders

https://www.okta.com/sites/default/files/pdf/Okta-Whitepaper-building-mfa-FINAL.pdf

[19] OWASP—MFA Cheat Sheet https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html

[20] NIST SP 800-63A, Digital Identity Guidelines, Enrollment and Identity Proofing, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

[21] NIST SP 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[22] NIST SP 800-63C, Digital Identity Guidelines, Federation and Assertions, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf

[23] University of Toronto, Identity and Access Management Standard, https://isea.utoronto.ca/developing-standards/identity-access-management-new

[24] Minnesota IT Services, Identity and Access Management Standard, https://mn.gov/mnit/government/policies/security/?id=38-323904

[25] UK National Cyber Security Center, Introduction to identity and access management, https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management

[26] Cloud Security Alliance, SecaaS Implementation Guidance, Category 1 Identity and Access Management, https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_G

uidance.pdf

[27] Center for Internet Security (CIS) Critical Security Controls (CSC), https://www.cisecurity.org/controls/cis-controls-list/

[28] Biometrics in identity: Building inclusive futures and protecting civil liberties - A best practices and recommendations guide, https://secureidentityalliance.org/publications-docman/public/156-biometrics-in-identity-building-inclusive-futures-and-protecting-civil-liberties/file

[29] Babita Gupta, School of Business, California State University, Monterey Bay, Biometrics: Enhancing Security in Organizations, https://www.businessofgovernment.org/sites/default/files/GuptaReport.pdf

[30] Security Guidelines for use of Biometric Technology in e-Governance Projects, Government of India Ministry of Electronics & Information Technology New Delhi, http://egovstandards.gov.in/sites/default/files/Security%20Guidelines%20for%20use%20of%20Biometric%20Technology%20in%20e-Governance%20Projects.pdf

[31] Cloud Forensics - Best Practice and Challenges for Process Efficiency of Investigations and Digital Forensics, José Antonio Maurilio Milagre de Oliveira and Marcelo Beltrão Caiado, http://icofcs.org/2013/ICoFCS-2013-003.pdf

[32] IPCFA: A Methodology for Acquiring Forensically-Sound Digital Evidence in the Realm of IAAS Public Cloud Deployments, Hosam Badreldin, Dakota State University, https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1367&context=theses

[33] Scientific Working Group on Digital Evidence, Best Practices for Digital Evidence Acquisition from Cloud Service Providers, https://www.swgde.org/documents/published

RAISING THE WORLD'S STANDARDS

3 Park Avenue, New York, NY 10016-5997 USA http://standards.ieee.org

Tel.+1732-981-0060 Fax+1732-562-1571