



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

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

Copyright © 2022 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. 28 September 2022. Printed in the United States of America.

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

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated. All other trademarks are the property of the respective trademark owners.

IEEE prohibits discrimination, harassment, and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system, or otherwise, without the prior written permission of the publisher.

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

ABSTRACT	5
1. INTRODUCTION	6
2. SOFTWARE DEFINED NETWORK (SDN) AND SD-WAN	8
3. ENDPOINT SECURITY AND ENDPOINT DETECTION AND RESPONSE (EDR)	10
4. CLOUD ACCESS SECURITY BROKER (CASB)	13
5. USER AND ENTITY BEHAVIORAL ANALYTICS (UEBA)	17
6. ZERO TRUST ARCHITECTURE (ZTA) AND ZERO TRUST NET ACCESS (ZTNA)	18
7. MULTI-FACTOR AUTHENTICATION (MFA)	21
8. IDENTITY AND ACCESS MANAGEMENT (IAM)	23
9. BIOMETRIC AUTHENTICATION	26
10. ZERO KNOWLEDGE PROOF AUTHENTICATION	28
11. CLOUD FORENSICS	28
12. ACADEMIC SURVEY OF CLOUD SECURITY GUIDELINES	32
13. SUMMARY AND NEXT STEPS	32
14. REFERENCES	33

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

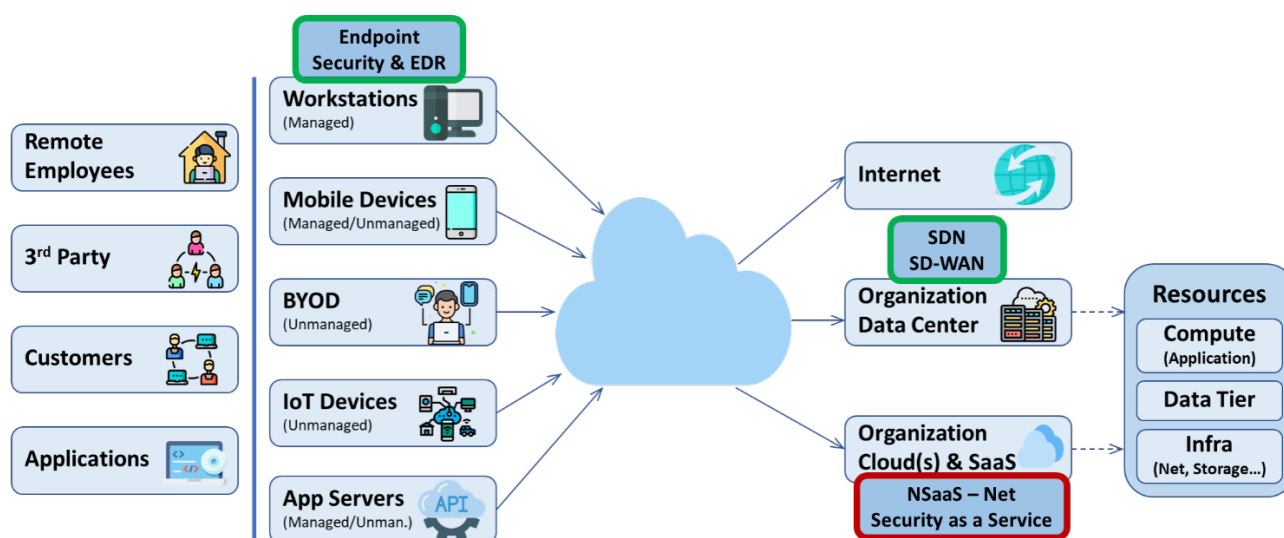


FIGURE 2 Cloud Access Infrastructure—Access Control

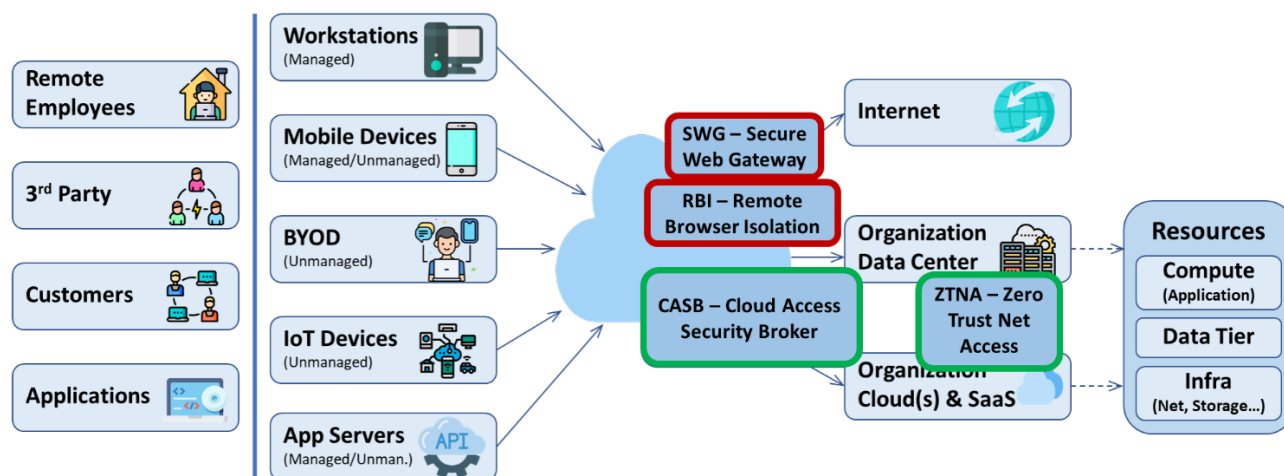


FIGURE 3 Cloud Access Infrastructure—Identity and Authentication

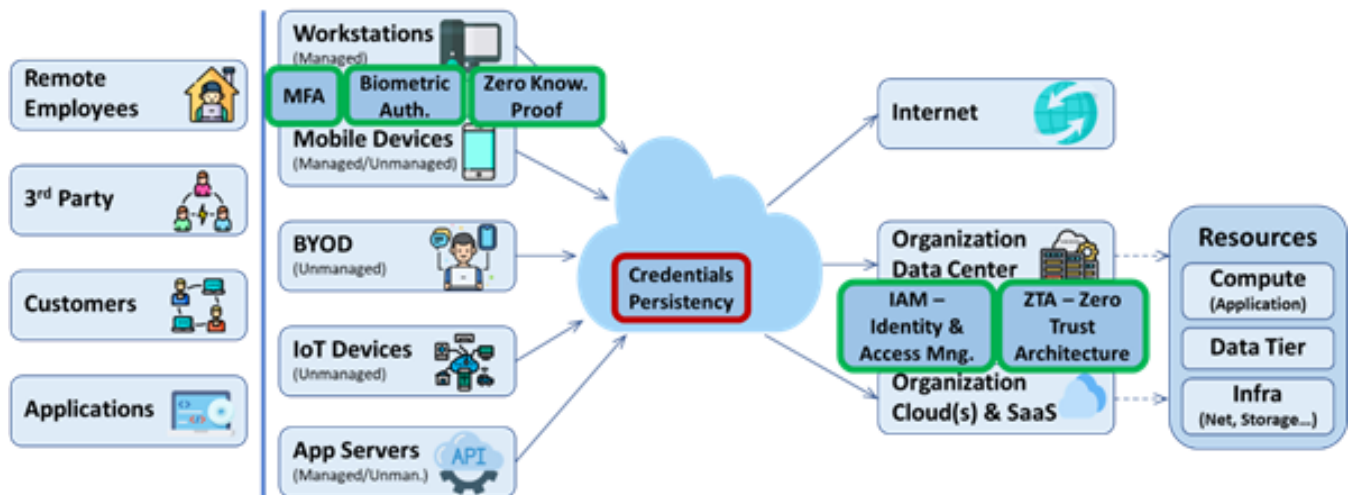
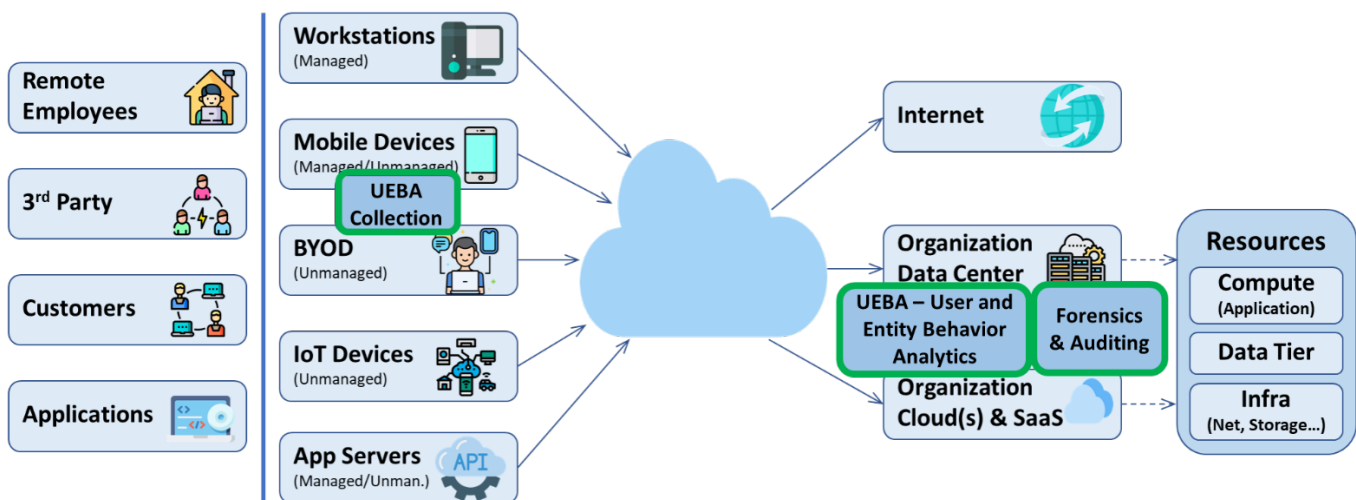


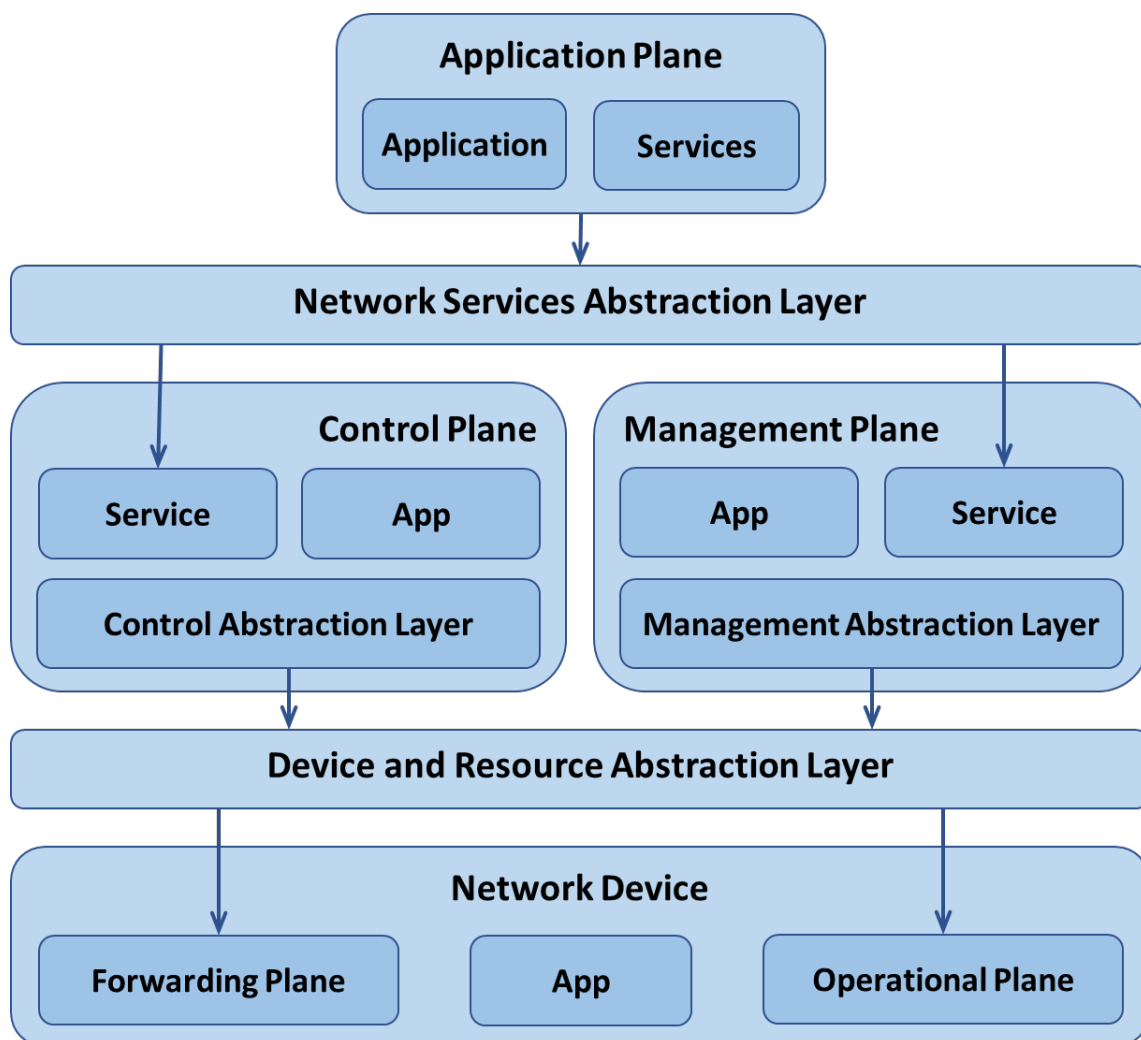
FIGURE 4 Cloud Access Infrastructure—Analysis



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 control