FORTRA™

WHITE PAPER (DIGITAL GUARDIAN)

Why SASE is Incomplete Without Endpoint DLP

The Hybrid Office is Here to Stay

The business world changed – perhaps forever – in 2020. The COVID-19 pandemic resulted in a rapid transition to a Work From Anywhere (WFA) environment. According to the 2019 National Compensation Survey (NCS) from the federal Bureau of Labor Statistics, only 7% of civilian workers in the United States had access to a "flexible workplace" benefit, or telework. Post-pandemic, a survey by PWC found that 89% of the respondents believed "Many" or "Most" office employees will be work remotely at least one day a week.

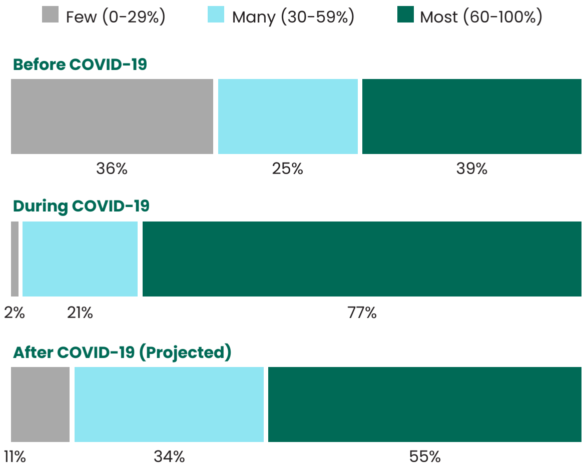
The shift is welcomed by many employees. The average commute time in the US in 2019 was almost 30 minutes each way and could exceed an hour or more in many urban areas. Eliminating the cost and time of commuting allows a better work-life balance. From a security standpoint, many believe that happy workers are more productive, less likely to leak data intentionally, and keep the company interests in mind. Businesses also see benefits in allowing WFA. Fewer on-site employees allow organizations to reduce expensive office space.

10,000 Unmanaged New Remote Offices

There is risk associated with the WFA movement, however. Where before COVID an organization with 10,000+ employees and 30 locations had a manageable number of locations to monitor and protect, it now has 10,000 remote offices, as more people work remotely. This number also includes the multiple locations each employee may use, including public WIFI locations. Each WFA employee represents multiple locations that must be protected from insider and outsider threats, whether that is one day per week or five. For many remote workers, information security controls are not top of mind within the corporate network, and some may feel free to do as they wish outside the office environment. While there is the malicious actor element, often it is unintentional acts where an employee is simply trying to get their job done that can lead to data loss.

WFA workers are not operating within a managed IT infrastructure. Open, unpatched, or poorly protected home routers make an attacker's job simpler. Web-based chat applications like

What percent of your office do you anticipate will work remotely at least one day a week?



> **"From a security perspective, [Remote work is now just work] requires a total reboot of policies and tools and approved machines to better mitigate the risks."**
>
> Gartner Top Security and Risk Trends for 2021

Slack and Teams open avenues for sharing sensitive data with co-workers but can also serve as egress channels for an organization's intellectual property (IP) and data subject to compliance oversight like Protected Health Information (PHI) and Personally Identifiable Information (PII). Likewise, unscrupulous employees may bypass corporate VPNs, upload sensitive data to personal cloud storage services like Google Drive and Dropbox, or use home printers to make copies of product plans, customer lists, and financial records to bring with them to new employers. USB drives are also potential channels for data loss or theft.

> **"Nearly 40% of home routers had not received a security update in over a year; nearly 20% were over 2 years without an update."**
>
> Fraunhofer Home Security Report 2020

Changing Environments Require New Strategies

Organizations that have built security strategies around a perimeter defense – all employees operating within a controlled environment – must adopt new approaches. As organizations contend with a remote workforce, Gartner, a leading research and advisory firm, found that "cybersecurity control failures" were the most critical respondent concern in the first quarter of 2021, topping "new working models", "remote talent management", and "organizational cultural degradation". They cited this as a "High-Impact, High-Velocity Risk", particularly for organizations that "prioritized on-premises security over secure remote work access".

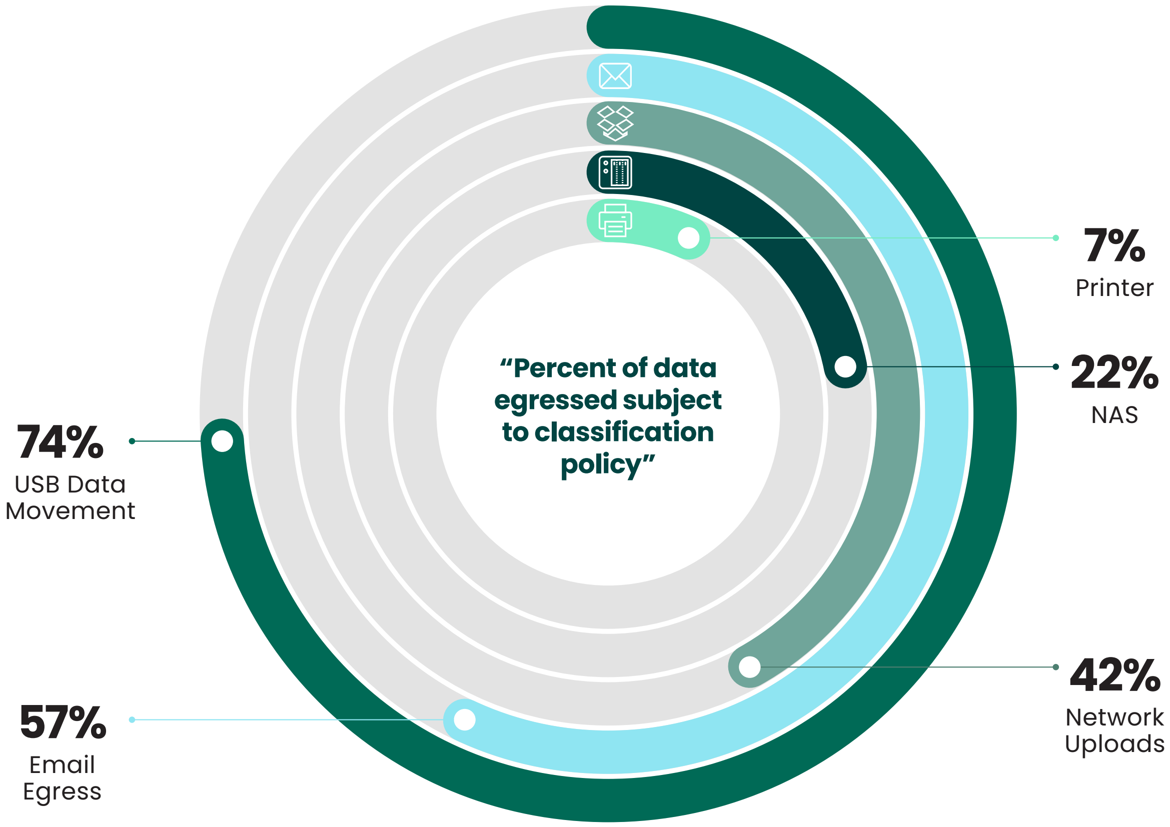
Focus on the Endpoints

In the WFA environment on-premises defenses are a poor match. Organizations working to control the loss of intellectual property, trade secrets, and other sensitive data need visibility and control over data wherever it resides, while also enabling an increasingly distributed and agile workforce. That means protecting data on the endpoints, where egress typically originates and can be a blind spot to network based security tools focused on the office based worker.

> **"The real challenge in cybersecurity is preventing breaches on the endpoint. Breaching the endpoint is the goal of almost all cyber-attacks because that's where the sensitive data actually sits."**
>
> George Kurtz
> Crowdstrike CEO

The 2021 Digital Guardian Data Trends Report found a large increase in data egress in the months following the World Health Organization's pandemic declaration. This included:

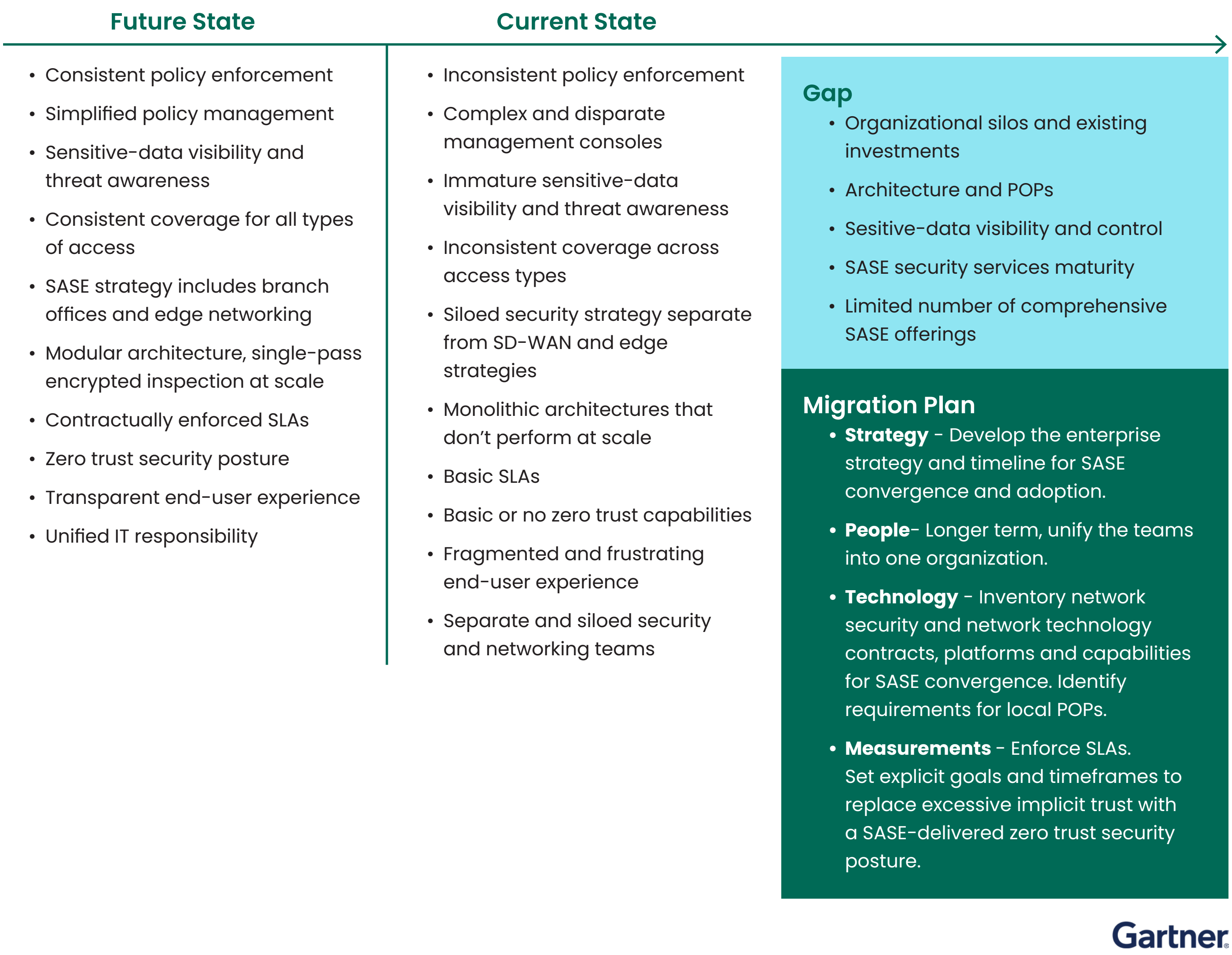
- An 80% Increase in volume of data egressed across all channels
- A 123% increase in volume of data employees copied to USB devices, 74% of those was
- "classified" data
- A 72% increase in volume of data uploaded to unsanctioned Cloud Storage Services, 42% of which was "classified" data
- A 49% increase in data emailed as attachments, 57% of which was "classified" data



SASE Gaps

Many organizations have turned to cloud-based Secure Access Service Edge (SASE) solutions to address security in a distributed workforce. SASE combines network security functions like Secure Web Gateways (SWG), Cloud Access Security Brokers (CASB), and Zero Trust Network Access (ZTNA) with Software-defined Networking (SD-WAN) capabilities to provide organizations with better control and visibility to users and data on an organization's network. Briefly, SASE pushes security monitoring to the "service edge" where users and systems interact with data. Rather than maintaining security functionality on each device, endpoints redirect traffic to the service edge for authentication, authorization, monitoring, and control.

Strategic Roadmap Overview for SASE Convergence



Future State

- Consistent policy enforcement
- Simplified policy management
- Sensitive-data visibility and threat awareness
- Consistent coverage for all types of access
- SASE strategy includes branch offices and edge networking
- Modular architecture, single-pass encrypted inspection at scale
- Contractually enforced SLAs
- Zero trust security posture
- Transparent end-user experience
- Unified IT responsibility

Current State

- Inconsistent policy enforcement
- Complex and disparate management consoles
- Immature sensitive-data visibility and threat awareness
- Inconsistent coverage across access types
- Siloed security strategy separate from SD-WAN and edge strategies
- Monolithic architectures that don't perform at scale
- Basic SLAs
- Basic or no zero trust capabilities
- Fragmented and frustrating end-user experience
- Separate and siloed security and networking teams

Gap

- Organizational silos and existing investments
- Architecture and POPs
- Sesitive-data visibility and control
- SASE security services maturity
- Limited number of comprehensive SASE offerings

Migration Plan

- **Strategy** - Develop the enterprise strategy and timeline for SASE convergence and adoption.
- **People**- Longer term, unify the teams into one organization.
- **Technology** - Inventory network security and network technology contracts, platforms and capabilities for SASE convergence. Identify requirements for local POPs.
- **Measurements** - Enforce SLAs. Set explicit goals and timeframes to replace excessive implicit trust with a SASE-delivered zero trust security posture.

However, the current state of SASE leaves organizations with several security gaps, particularly around Data Loss Prevention.

- **Visibility to Sensitive Data** – The Gartner 2021 Strategic Roadmap for SASE Convergence report cites "Sensitive-data visibility and control" as one of the top five gaps in SASE solutions. SASE have visibility to data stored in the Cloud but typically not to on-premises data stores and sensitive data on endpoints.mEndpoints are the primary attack vector for malicious insiders, a simpler target for attackers, and more challenging for infosec teams to control in the WFA environment.
- **Inconsistent Policy Enforcement** – Cloud-based SASE solutions rely on multiple Points of Presence (POP) to which traffic is redirected for inspection and policy enforcement and, according to Gartner, none yet support distributed cloud architectures or platforms such as AWS Outposts, Google Anthos or Microsoft Azure Stack. This can lead to a requirement for additional solutions at remote offices with low-latency requirements. In an organization with hundreds or thousands of WFA employees, "additional solutions at remote offices" and consistent policy enforcement using SASE is extremely unlikely, or at best extremely difficult and expensive.

- **Poorly Secured WFA Environment** – The remote office is an attractive target for adversaries. Employees can bypass corporate VPN and outdated, unpatched devices can include routers, printers, and Internet of Things (IoT) devices like monitors and IP cameras. Any of these can provide attackers with an initial foothold from which to launch attacks on endpoints and the corporate network. Public WIFI hotspots are an even greater risk. In short, all the usual challenges exist, but there is less oversight or control over them. Many end users are unlikely to spot a compromised device until the damage has been done.
- **Local Device Egress** – As noted, an employee's endpoint need not be connected to the enterprise network to operate. This allows an insider to download sensitive data to a remote storage device like a USB stick or simply print sensitive documents.

Closing the SASE Gap

While SASE are useful for ensuring authorized access to systems and data for employees operating within the corporate network, they are poorly suited for protecting sensitive data in a WFA environment. InfoSec leaders need to take steps to address this challenge and address the new work environment expected to last for the foreseeable future.

Fortra™'s Digital Guardian® complements SASE adoption to extend visibility and control to endpoints inside and outside the corporate network. Digital Guardian provides information on where your data is, how it is used, and how it flows throughout organization, and when it is at risk:

- **Visibility to data wherever it resides** – Digital Guardian works on Windows, Mac, and Linux endpoints on and off the network, on-premises devices, and cloud applications to discover sensitive data, making it easier to see and protect data.
- **Visibility to Risky Activity** – Not all data loss is the result of malicious attacks. Employees may inadvertently move large files to cloud drives to bypass email size limitations and "print to PDF" or "print screen" to save information for later use. Others may copy data from a "password.txt" file to a web login page. The former examples can be attempts to perform legitimate tasks. The latter may indicate that passwords are stored in cleartext on the user's device. Digital Guardian maintains classification tags when sensitive information is copied to the new files, even when the file extension is changed. It can also provide alerts to educate users about the risk involved in risky behaviors.
- **Flexible classification and granular, contextual control** - Protecting data requires more than simply access control or encryption (though both are obviously important). To protect data while allowing full – legitimate – use, Digital Guardian provides a contextual understanding of three factors: what actions may be taken with the data; by whom; and, under what circumstances. Privileged users need to configure devices but prohibited from viewing specific, sensitive files on those devices.
- **Control desktop applications for Cloud services** – While SASEs can provide control over native web applications, they are unable to monitor and control the desktop applications used to access those services. Digital Guardian extends to both corporate and personal collaboration application accounts like Microsoft Teams, Skype, Slack, and Zoom to block users from sharing sensitive files – or warn them, require a justification, or just log the attempts to do so.
- **Block and protect removeable media** – Copying sensitive files to removeable storage devices is a common attack vector for malicious insiders. Digital Guardian monitors and controls sensitive information transfer through Bluetooth, USB, CD/DVD, and Media Transfer Protocol (MTP) and Picture Transfer Protocol (PTP) devices.
- **Controlled printing** – Digital Guardian can block printing of sensitive information, even on the user's home network. Since Digital Guardian understands data classification, user, and action, it can block or warn the user, as well as maintain an evidentiary quality log file of all attempted and completed actions. Alternatively, Digital Guardian could allow printing, but restrict that action to a named network printer to allow administrative review prior to releasing the printed documents.

SASE and DLP Together

Secure Access Service Edge solutions can simplify network security by combining multiple solutions. The missing piece – Data Loss Prevention – is particularly acute in a Work From Anywhere environment where employees have access to poorly secured networks and devices. Digital Guardian works on the broadest collection of endpoints to provide visibility and control to all sensitive data, educating users of unsafe behavior, blocking malicious actions, and providing the detailed reporting security leaders need.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.