Privafy™

Securing Data-in-Motion with Cloud-Based Security

A PRIVAFY WHITEPAPER

07.20.2020

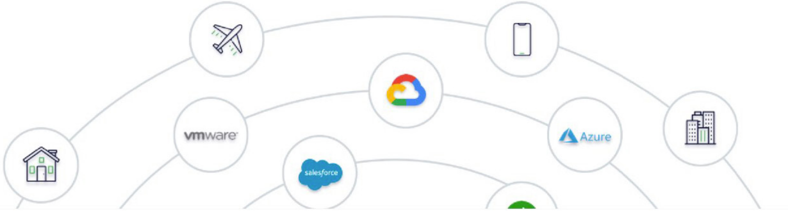
Data-in-motion: A definition

Data is often referred to as both the lifeblood of a business and a mountain of information—two very different images that reveal the duality of data. When data is being stored somewhere, we refer to it as data-at-rest. When data is moving from one point to another through a network, we refer to it as data-in-motion. These two states sum up the daily life of data, though there are some striking differences between the two, particularly when it comes to security. According to analyst firm IDC, eighty percent of all cyberattacks occur while data is in motion.

80%
of all cyberattacks occur while data is in motion

Protecting data-at-rest and protecting data-in-motion involve different processes and technologies. Simply because data is protected at rest doesn't make it secure in motion In a sense, you can think of data as your car. At rest, it's protected in your garage against theft and disasters such as floods. On the road (i.e., in motion), there are other methods that you use to protect against collisions with bad drivers and the possibility of hijacking, not least of which are developing good safety habits.

While we often think of data as static, it's constantly in motion around us. Our computers and mobile devices are continually uploading and downloading data to cloud storage systems. Billions of text messages and emails move back and forth over private and public networks. And the growing list of connected devices that represent the Internet of Things (IoT) are adding even more data traffic to the world's networks.



Data-in-motion

Why do I need to secure data-in-motion?

Data-in-motion is more exposed than you might think. It's exposed to devices which may already be compromised, spoofed websites that pretend to be legitimate, users with weak passwords that can be easily guessed, and networks that may not be secured. This exposure can be effectively mitigated by strong security measures, but your data-in-motion is probably less secure than you realize. Cloud service providers, email providers and Internet service providers will probably tell you that your data is secure, but they're often not telling you the whole story. That security may only apply to data-at-rest, or it may tout strong encryption but default to the lowest common encryption method while data is in motion between endpoints.

Data-in-motion security is fundamentally different than data-at-rest security. While there are many proven security approaches which work well for stored data, they are not as effective for data-in-motion because of the presence of unknown or untrusted endpoints. The reason for different security methods is because data-in-motion is subject to different kinds of attacks than data-at-rest. These attacks, sometimes referred to as "man-in-the-middle" attacks, include:

- Snooping that takes place as data is transmitted over a non-secure, public wi-fi network or, in some cases, on "fake" wi-fi networks that have been staged for the sole purpose of stealing data
- IP spoofing that redirects users to a staged website designed to look just like the intended site and, in some cases, may even redirect the transmission to the real website after the data has been stolen, so users never know their data has been intercepted.

Because of these and other vulnerabilities, securing data-in-motion is a business mandate. It is required for PCI-DSS compliance, HIPAA compliance and other regulatory agencies, both in the federal and private sectors. Not securing data-in-motion can result in heavy fines, lost revenue and, perhaps worst of all, eroded customer trust.

The security requirements for data-in-motion

Protecting data-in-motion is a multi-layered problem that requires a multi-layered solution. In other words, there isn't any one thing that businesses should be doing to secure data-in-motion, but rather a series of security measure that, together, provide a protective shield including:

- End-to-end, asymmetric key encryption with frequent rotation of private keys
- Consistent security policy enforcement across networks, clouds and devices
- Intrusion detection/prevention systems (IDS/IPS)
- Identity & access management (IAM) tools
- A trusted tamper-proof root of security
- Network address topology hiding
- Automated software patches/upgrades
- Up-to-date, continuous threat intelligence
- Good security practices (e.g., using strong passwords, avoiding non-secure networks and using role-based access privileges to data).

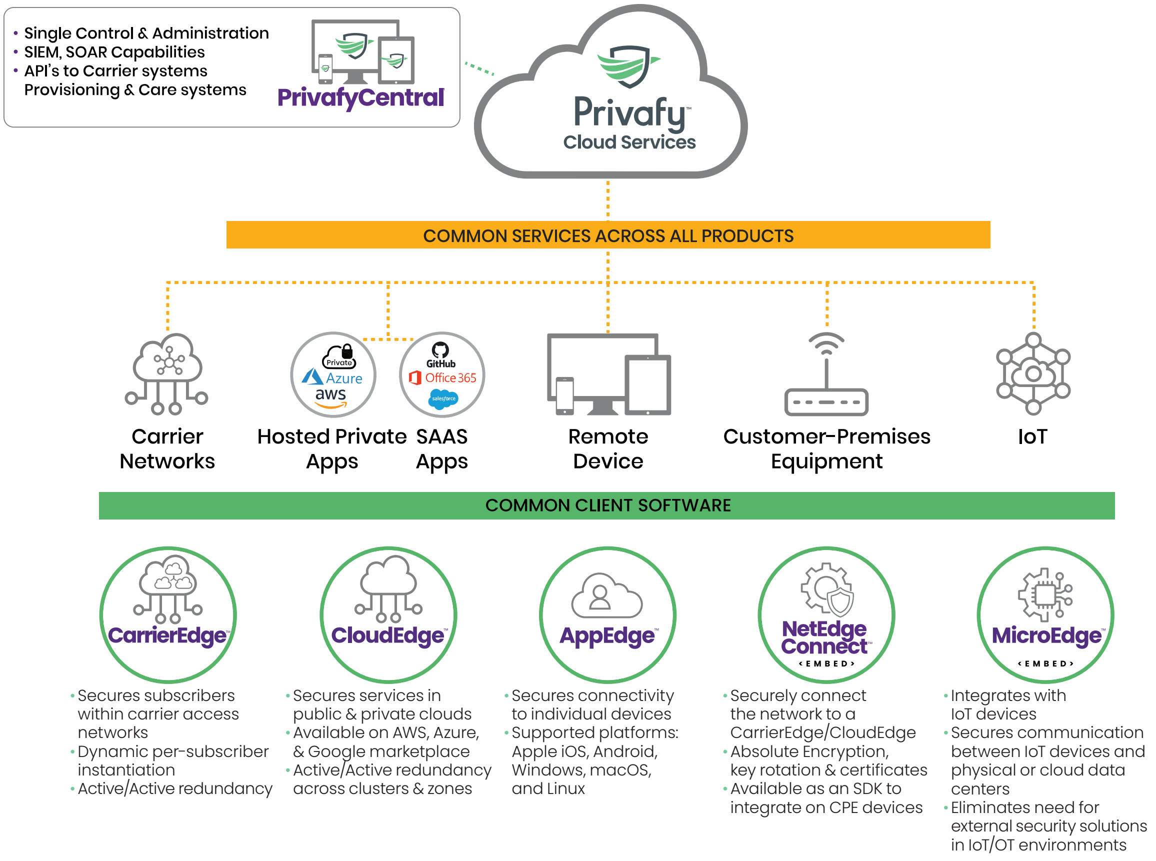
Conversely, there are also things you shouldn't do to protect your data, as these can limit your business productivity and flexibility, as well as unnecessarily drive up the cost of security. They include restricting cloud access, locking employees into using IT-sanctioned devices only, limiting remote access to business applications and assuming that all data should be treated with the same high level of security. The reality is that security is a balancing act that requires businesses to focus on protecting their most sensitive and mission-critical data rather than trying to create an airtight security wall around everything and everyone.

Protecting data-in-motion with cloud-based security

Traditionally, businesses have protected their data using a mix of best-of-breed, multi-vendor hardware and software. This approach has had two significant drawbacks: 1) It's expensive to purchase and maintain, and 2) It creates security gaps between different vendors and tools. As cloud technology evolved, Privafy recognized an opportunity to create a better, comprehensive security solution—one delivered as a service, in the cloud, with only a single piece of hardware (as needed) to protect the network and provide a trusted root of security. Today, the **Privafy solution provides complete, end-to-end security-as-a-service for data-in-motion at a fraction of the cost of a traditional security solution.**

Privafy provides enterprise-class security to businesses of all size with a flexible, affordable and easy-to-implement solution including:

- **CarrierEdge** to protect subscriber data within a carrier network. Dynamic per-subscriber instantiation with active/active redundancy
- **CloudEdge** to protect data as it moves in and out of cloud-platforms, SaaS applications and the network
- **AppEdge** to protect data as it moves to and from devices including laptops, smart phones and tablets
- **NetEdgeConnect** for securely connecting the network to a carrieredge/cloudedge. Available as an SDK to integrate on CPE devices
- **MicroEdge** to protect data as it moves to and from IoT devices including sensors and smart appliances.



- Single Control & Administration
- SIEM, SOAR Capabilities
- API's to Carrier systems Provisioning & Care systems

CarrierEdge
- Secures subscribers within carrier access networks
- Dynamic per-subscriber instantiation
- Active/Active redundancy

CloudEdge
- Secures services in public & private clouds
- Available on AWS, Azure, & Google marketplace
- Active/Active redundancy across clusters & zones

AppEdge
- Secures connectivity to individual devices
- Supported platforms: Apple iOS, Android, Windows, macOS, and Linux

NetEdge Connect
- Securely connect the network to a CarrierEdge/CloudEdge
- Absolute Encryption, key rotation & certificates
- Available as an SDK to integrate on CPE devices

MicroEdge
- Integrates with IoT devices
- Secures communication between IoT devices and physical or cloud data centers
- Eliminates need for external security solutions in IoT/OT environments

Because it’s cloud-based security-as-a-service, Privafy has a much lower cost of entry than comparable, best-of-breed security solutions. And where most solutions require days or weeks to install and integrate, Privafy’s service can be deployed and fully operational in a data center or office branch location in minutes with no on-site technical expertise required. While speed and cost are important factors, it’s in the security delivery where Privafy distinguishes itself. Developed by a global team of security experts and featuring patented technology, Privafy provides complete, end-to-end protection for data-in-motion in a single, seamless solution.

It protects data-in-motion as it moves between your network, the cloud and connected devices.
Privafy features asymmetric key encryption with patented key rotation technology to ensure that data-in-motion is ultra-secure. This technology creates a secure connection between networks, endpoints/users and cloud platforms that is stronger than the industry’s leading VPN solutions.

It stops known attacks and spots suspicious activity.
Privafy NetEdge blocks network attacks at every network entry point where a NetEdge device is deployed. Privafy leverages the latest virus definitions and threat intelligence from around the world to ensure that businesses are protected against new attacks including zero-day viruses. When malicious or suspicious activities are detected, the Privafy dashboard (PrivafyCentral) creates an alert along with recommended actions.

It enforces strong security policies consistently across devices and networks.
Security systems are only as strong as their weakest link. Inconsistent security policies across networks or endpoints create vulnerabilities that can be exploited by cybercriminals. As a cloud-based service, Privafy ensures that every protected network and endpoint is using the “latest and greatest” security policies.

It prevents bad things from getting into your network—and bad agents from taking things out of your network.
Privafy NetEdge establishes a trusted, tamper-proof security sentinel at the network’s edge that blocks unauthorized users, compromised devices and suspicious packets from entering the network, and blocks confidential data from leaving your network through a data breach.

Why do I need to secure data-in-motion?

While most businesses recognize the need to protect their stored data, secure data-at-rest doesn’t mean your data is secure once it leaves your network. In mawny ways, these are different security initiatives that require a different solution. There are dozens of security vendors that offer partial solutions, from antivirus software and malware detection to firewalls and IDS/IPS appliances. Only Privafy offers comprehensive protection for data-in-motion in a single, seamless solution as a service.

It’s simple to get started with Privafy. You don’t need security expertise to integrate and maintain a complex security system. You don’t need to spend thousands of dollars on hardware and software licenses. And you don’t need to wait months to see ROI on your security investment, because Privafy shows you exactly what it’s doing and how many attacks it’s stopping through real-time alerts and logs. You just switch on Privafy through the click of a button, and you can switch off that part of your brain that worries about cybersecurity at 1:00 AM in the morning.

To learn more about Privafy’s cloud-based security solutions, visit us at **www.privafy.com**.

Privafy™

WORK ASSURED

US HEADQUARTERS
2 Burlington Woods Drive
Burlington, MA 01803

SALES
phone: 781.342.1077
email: sales@privafy.com

WEBSITE
Learn more about Privafy
privafy.com

PRIVAFYCENTRAL
Purchase, monitor and manage
your Privafy service
https://dashboard.privafy.com/login

About Privafy

Privafy's vision and mission are to harness emerging cloud technologies to bring enterprise-grade data security within reach of businesses of all sizes. The company currently holds 25 technology patents and has offices in Boston, Massachusetts, and Bangalore, India.

The content set forth in this presentation or document is for informational purposes only and does not constitute a binding commitment or obligation on the part of Privafy. Please visit www.privafy.com for the most current pricing, technical information and features. In the event of a conflict between this content and the information provided on Privafy's website, the website will prevail.