Cloud Storage in a Zero Trust Enterprise

Each month, a new cyberattack makes headlines in terms of scale and financial impact. At the moment, ransomware is the most newsworthy threat, delivered as fake Windows updates[1] and Covid-19 announcements[2]. Hijacked email reply chains[3], fleeceware[4], cryptojacking[5], and IoT attacks[6] plague practically every IT organization, and force IT Ops teams and SecOps teams into an endless firefight, coping with thousands of alerts and hundreds of threats, again and again.

To cope with this never-ending menace, forward-looking organizations deepen their security postures to reduce their attack surface, consider new approaches, and evaluate their technologies for risk. Though there's been no consensus on the best strategy for years, it's become clear that old-school, perimeter security plus eight-character password protection schemes aren't cutting it. Lately, enterprises, cloud providers, analysts, and technology companies are converging around **Zero Trust (ZT)** architectures as the best approach for dealing with the constantly-evolving onslaught of attacks, threats, and risks. Regulators are aligned with this view -- in May 2021, the Biden administration issued an executive order mandating U.S. Federal Agencies adhere to NIST 800-207 as a required step for Zero Trust implementation.

To implement Zero Trust architectures, every component of the infrastructure stack has to be evaluated for risk. As a result, today's administrators are casting a keen eye over their hardware and cloud stacks, trying to identify where they have gaps and weaknesses -- and storage is one of the critical technologies they're evaluating and testing for fit in a Zero Trust architecture.

In this paper, we will explore the state of play for security, dig into Zero Trust, and explore the critical characteristics of storage for Zero Trust. Then, in conclusion, we'll evaluate Wasabi against the principles of Zero Trust and see how it measures up. After reading this paper, you'll better understand how cloud storage fits into Zero Trust, where challenges, gaps, and opportunities arise, and whether or not Wasabi could be the right tool in your search for a more secure enterprise.

The State of Play for Security

We all know that enterprise security is a critical requirement that allows and supports day-to-day IT operations while protecting organizations from data loss, financial risk, reputational risk, and even business collapse. But why is enterprise security so hard to manage today?

Years ago, organizations had a collection of data centers on a Wide Area Network (WAN), managed by internal teams. Their employees used IT-supplied devices with corporate images, a single operating system, and tested firmware. Users could authenticate using a VPN and would have complete access to all systems, applications, and/or databases. More confidential systems would be password protected for administrator access only. IT administrators (we barely had security teams then) felt like they had a nice, pristine castle wall of perimeter defenses (e.g., firewalls, anti-virus software, VPNs, etc.) that kept everyone safe and secure, even though threats and attacks have been around since 1988 when the first threat hit the Internet[7].

Everything and everyone inside the wall was trustworthy and trusted. Today, that's different….

> **Today's difficulty stems from two developments:**
>
> 1. As organizations identified risks and chose tools to block threats like worms and Trojan horses, attack creators evolved. Gone are the days of individual hackers creating a virus. Cyberattacks have become one of the world's fastest-growing illicit businesses. Beginning in the early 2000s, organized crime became the critical creator, sponsor, and facilitator of cyberthreats[8]. Cybercriminals have become more sophisticated, and cybercrime as a business has evolved into cybercrime as an enterprise.
>
> Around 2019, cybercriminals began to create a global ecosystem where they operate 24x7 as managed attack providers that offer a portfolio of threats, including ransomware as a service. They have online points of presence, massive attack infrastructure, and even sales teams and customer service operations that can empower nearly anyone with access to a keyboard to deploy the most powerful and disruptive attacks imaginable. Cybercrime is the fastest growing crime in the U.S.[9]. It's seen by some as an entrepreneurial growth business[10] costing organizations nearly $1.79 million per minute[11].
>
> To make matters worse, cybercriminals aren't the only problem. State actors have gotten into the cyberattack game, and though their motives don't necessarily involve making money, they're capable, sophisticated, and perfectly able to uncover private personal information, steal trade secrets, explore government networks, damage critical infrastructure, and even take down enterprises[12]. China, Russia, North Korea and Iran are the four most dangerous, effective countries sponsoring and sustaining cyberthreats, cyberattacks, and even cyberwarfare capabilities, sometimes in partnership with cybercrime cooperatives, syndicates, and businesses[13].

> 2. To make matters worse, organizations continue to add more attack surfaces because they're making IT more complex. The next wave of IT innovation is emerging because organizations are shifting toward the fourth wave of the industrial revolution (Industry 4.0), which disrupts the way we use data, but shifting, emerging leading-edge industrial IT requirements result in more gaps and weaknesses in overall security.
>
> Today's end-customer services, innovative platforms like Smart Cities and autonomous vehicles, and emerging, AI-powered predictive business analytics all run on data, which needs to be close to the endpoint, easily accessible, moved from place to place with high performance, and kept protected. IT 4.0, distributed infrastructure that includes endpoints, edge nodes, core data centers, and multiple clouds, has evolved to fit those needs. As it becomes more commonly deployed, a natural consequence of the added complexity is that more technologies are exposed to attacks that are difficult to defend. Today, tens of thousands of attack surfaces are all based on different processors, firmware, operating systems, applications, and security capabilities. Initiatives like BYOD make matters worse. It's become impossible to secure the perimeter and make network access safe. There is no longer any "perimeter" - everything is connected to everything, for better or worse.

Today, we see the consequences of these changes in the scope and scale of the problem.

- 49% of U.S companies have experienced a data breach[14].
- A typical endpoint is attacked every 39 seconds[15].
- 7 out of 10 organizations that use the cloud experienced a security incident in the past year[16].
- A breach can directly cost an organization as much as $392 million[17].
- Increased indirect costs, including insurance premiums, increased costs to raise debt, lost value of customer relationships and contracts, afflict organizations for years[18].
- Publicly traded companies that experience a damaging attack end up underperforming the market for years[19].

In short, security is becoming a substantial challenge for organizations of all sizes, driven by the growth of sophisticated bad actors and increasingly complicated IT infrastructures. So how can an organization cope with literally hundreds of criminal enterprises and state agents attacking every single piece of technology that's accessible?

Today's answer for many enterprises is **Zero Trust.**

Becoming a Zero Trust Enterprise

Zero Trust isn't a new idea. Devised in 2009, the concept simply stems from the idea that, instead of trusting devices on a network, it's best to NOT TRUST devices and users in today's distributed world.

Zero Trust rethinks two fundamental principles of IT Operations:

1. Authentication

2. Authorization

In authentication, identifying a user (or application) typically begins with a username and password, or, more recently, a PIN or a Token. It also considers context, like behavior, device address, location, biometrics, etc. Authorization is the process of determining which applications, files, and data a user can access, view,or change. In both cases, users are tied to an account record in a database and can't be modified by the user, unless they're a root user or administrator.

Traditionally, authentication and authorization were governed at the perimeter,through network access. Once a user, device or application had access to the network, they had access to many resources. In the past, that wasn't entirely problematic, though, once in a while, you'd hear about a user accessing some files on a share they probably shouldn't have accessed. The reality was that many resources didn't have the right permissions set and people's permissions from old roles might have been accidentally kept.

The world changed once bad actors started breaching the perimeter with sophisticated authentication and authorization attacks.

Whether the breaches are conducted by a hacker sniffing around internal networks, a bit of code surreptitiously accessing a cloud storage volume, or a tailored attack crashing the simple security of an IoT device, access to the network is dangerous -- unless the organization operates under the principle of Zero Trust.

"Zero Trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources." -- NIST[20]

Zero Trust aims to prevent authorized access to data and services by making access as granular as possible, not location-network (i.e., not dependent on network permissions), resulting in a fine-grained set of security controls for every user, every app, every API, and every asset. The underlying premise is that every access is hostile unless proven otherwise.

The idea behind Zero Trust is that network access doesn't automatically provide access to resources. The Principle of Least Privilege applies. Any new user has NO access to anything and slowly gets approved or qualified for access to only the resources necessary for them to do their job at that moment. Accesses are automatically monitored and can be turned on and off as needed

In a Zero Trust world, just because a bad actor gets into the network, they don't automatically have access to resources.

So in a Zero Trust architecture:

1. **Access is contextual:** Users who authenticate with username, passwords, and virtual token/SMS PIN, are further authenticated with a machine learning algorithm that conducts a real-time security audit based on GPS location, MAC address, keystroke profile, and other unique identifiers.
2. **Access is examined:** Every bit of network traffic is authenticated and inspected, even encrypted traffic, in real-time, to stop inappropriate access requests from reaching their destinations.
3. **Access is restricted:** Applications and associated data sets are restricted. Only the users who must have access to do their work, get access to do their work. Everyone else is blocked.
4. **Access is segmented:** Networks, servers, applications, and devices are micro-segmented, reducing the blast radius in case of an infection or breach.
5. **Access is defended:** Successful defense isn't a function of the network. It's a function of the network, the applications, data storage devices, IoT devices, endpoints, and everything else on the network. As a result, protections are much more robust and harder to crack.

Organizations that adopt Zero Trust enjoy a collection of advantages, including:

1. Reducing business and organization risk, including damage due to cyberattacks
2. Better ways to control cloud and container environments
3. Better support for compliance initiatives
4. A better foundation to ensure security as infrastructure evolves.

Expanding on that last point, infrastructure always evolves. As a result, every IT organization has a mix of legacy, contemporary, and even emerging technologies that they're obligated to protect. And to be honest, not every technology is a good fit for Zero Trust architectures.

That's especially true of storage.

Zero Trust and Storage: Features and Functions

As organizations have, for years, coped with exponential data growth, many of them have invested in expensive data storage platforms that house many terabytes or petabytes of data. However, whether using conventional on-premise or cloud storage, concerns around data gravity (the cost, complexity, and risks of migration) tend to mean that once data is written to storage, it stays on storage.

Data gravity also means that data storage tends to be one of the older technologies in an IT infrastructure simply because it's hard to replace. Storage that doesn't support Zero Trust can be one of the most dangerous platforms if it's attacked, simply because it contains more data than every other device.

This is especially true of online backup and archival storage. Typically, backup and archive are seen as afterthoughts, not particularly important unless there's a problem. However, that makes backup and archive storage a sitting duck for cybercriminals, state agents, and other bad actors seeking a relatively soft target to breach, steal data from, lockdown for ransomware, and otherwise attack. Unfortunately, they're also often the single most dangerous device in your environment, because they contain data from many users, applications, services, and primary storage platforms.

It's hard to know how often data storage devices, arrays, and cloud storage volumes are breached, and it's also hard to understand how unprotected they are. But it's relatively easy to assess whether your platform is good enough to fit into a Zero Trust architecture.

Some principles of safe storage include:

- Does the platform support end-to-end encryption?
- Does the root account utilize two-factor authentication?
- Does the platform support IAM policies to manage user capabilities?
- Are key pairs quickly deprecated and/or replaced?
- Does the platform support versioning and bucket logging?
- Can the storage be tied into your security AI engine for activity monitoring and patterning?
- Can your system be logically air-gapped for micro-segmentation?
- Does it support immutable buckets/objects that protect data from malicious alteration, encryption, or deletion?

Not many platforms support all these features, **but Wasabi does.**

Exploring the Wasabi Difference

Wasabi is a leading cloud object storage provider and a compelling alternative for organizations seeking the right integration of cloud storage into Zero Trust architectures. It fits Zero Trust because it offers ten features that align with Zero Trust principles and architectures. End-to-end encryption.

- Two-factor authentication
- Application-specific IAM for micromanagement of user capabilities
- Easy key management, even across multiple volumes
- Versioning and bucket logging
- API connections to security AI engines
- Logical air-gapping
- Immutable objects that simply cannot be changed, even with root access
- Re-encryption blocking that protects against crypto-ransomware
- Validation with the leading backup vendors, including Veeam and Commvault.

And unlike other vendors, it's enterprise-class, tier-free, and instantly available, with options for backup, file storage, and many other use cases. As a result, it's an ideal fit for SecOps teams who want to minimize threats.

To learn more about Wasabi and why it helps organizations build a Zero Trust architecture, visit us at www.wasabi.com/ransomware

ABOUT WASABI

Wasabi provides simple, predictable and affordable hot cloud storage for businesses all over the world. It enables organizations to store and instantly access an unlimited amount of data at 1/5th the price of the competition with no complex tiers or unpredictable egress fees. Trusted by tens of thousands of customers worldwide, Wasabi has been recognized as one of technology's fastest-growing and most visionary companies. Created by Carbonite co-founders and cloud storage pioneers David Friend and Jeff Flowers, Wasabi is a privately held company based in Boston.

wasabi
hot cloud storage
www.wasabi.com

End Notes

1 https://blogs.blackberry.com/en/2022/03/lokilocker-ransomware

2 https://www.ociso.ucla.edu/resources/covid-19-cybersecurity/covid-19-scams-phishing-malware-ransom-ware

3 https://thehackernews.com/2022/03/hackers-hijack-email-reply-chains-on.html

4 https://www.wired.com/story/what-is-fleeceware-protect-yourself/

5 https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking#:~:text=Cryptojacking%20is%20a%20type%20of,computing%20power%20to%20generate%20cryptocurrency.

6 https://securityintelligence.com/articles/iot-security-internet-forgotten-thing/

7 https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

8 https://www.jstor.org/stable/j.ctv1fxh0d.8?seq=1

9 https://www.natlawreview.com/article/c-suites-cybercrime-damages-expected-to-reach-6-trillion-2021

10 https://www.wired.com/insights/2014/10/cybercrime-growth-business/

11 https://www.infosecurity-magazine.com/news/cybercrime-costs-orgs-per-minute/

12 https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/

13 https://nationalpost.com/news/politics/canada-the-target-of-thousands-of-cyber-attacks-every-day-csis-reveals

14 https://cpl.thalesgroup.com/en-gb/euro-data-threat-report#download-popup

15 https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

16 https://www.sophos.com/en-us/content/state-of-cloud-security

17 https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542

18 https://www2.deloitte.com/us/en/pages/finance/articles/cfo-insights-seven-hidden-costs-cyberattack.html

19 https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

20 https://csrc.nist.gov/publications/detail/sp/800-207/final