The Perimeter at the Data Object: Zero Trust and Data Protection

As many struggle with the latest bring your own device, multi-cloud environments, and data audits within complex organizational and supply chain structures, any discussion of a fixed perimeter with known entry and exit points is a relic of a bygone era. Today's new frontier reflects an ever-expanding attack surface and vulnerabilities that extend well beyond their own control. While there is broad acceptance that the perimeter is dead, what comes next remains hotly debated.

Within this expansion of the attack surface and growing access points, a Zero-Trust approach is gaining traction. First coined by Forrester Research almost a decade ago, Zero Trust essentially introduces a deny by default mentality, limiting access to prevent lateral movement within systems. Largely centered on network segmentation, gaining greater visibility and eliminating network trust, Zero Trust continues to evolve to include devices, users, applications, endpoints and data. Across each of these, data remains the common factor. Whether on a device, accessed by specific users or stored in select applications, data is the lowest common denominator and therefore is the most effective focal point for any Zero-Trust strategy.

With a Zero-Trust approach to data, access privileges can be customized based on specified parameters - including devices, users, locations, bots or segments within the data itself. This moves Zero Trust beyond the network, and data becomes the new perimeter. In this paper, we detail the benefits of a Zero-Trust strategy focused on the data itself, with customizable access privileges and portability to allow secure data sharing even within untrusted environments. Guiding principles of usability and integration within existing systems are equally important to ensure the data protection becomes a force multiplier and not a hindrance. A data-centric approach embraces the broader tenets of Zero Trust, but simplifies it to avoid reliance and trust on any third-party provider or service, while introducing data control wherever it travels.

The Quest to Regain Control

Zero Trust emerged out of this desire to regain a level of control, better defend against a growing attack surface, and meet the needs of changing business processes and technology while supporting a more mobile and connected workforce. It also has helped spark new approaches for identity management, behavioral analytics applications, and device management. While these are certainly welcome shifts in approaches to security, they generally do not fully eliminate reliance on a third-party service or provider. For instance, even if a cloud provider offers end-to-end encryption, who maintains the keys and who has access

to them? If it is the provider, it still requires a level of external trust. This is most clearly evident in Google's BeyondCorp approach to Zero Trust, which focuses on device and user access privileges. However, since that approach was created, there is a growing concern about cloud providers accessing data, and protections persisting only within an organization's ecosystem and not outside their network. Greater attention is required to protect the data itself, wherever it goes, and not simply focusing on devices and users.

In addition, organizations simply cannot stay apace of the devices and applications connected to their networks. The statistics vary depending on the survey, as one finds 40% of organizations lack full visibility into their connected endpoints and networks, while another identified two-thirds of organizations without IoT visibility. This limits organizations from fully realizing significant control from a Zero-Trust approach, which often relies on identifying all resources across all environments. It also introduces workflow and usability challenges, inefficiencies, decreased collaboration and frustrations within the workforce if essential tools are blocked.

These limitations are evident when looking at the growing challenges of data sharing and collaboration. Despite a growing awareness and adoption of a Zero-Trust strategy, organizations don't have full data control and so limit data sharing and collaboration to minimize their risk posture. From health care research to cybersecurity indicators and warnings intelligence, organizations actually lack access to relevant and impactful data due to security and privacy concerns of the data.

Sharing and exchanging data is a prerequisite of the digital economy. With data flowing at unprecedented rates, there has not been a good way to protect data and maintain a level of control, auditability and transparency once it is shared. To date, most Zero-Trust approaches fail to apply the key tenets of Zero Trust to the data itself. In the next section, we'll discuss how the same Zero Trust requirements can be applied to the data and open up organizations to secure data sharing and collaboration.

Zero Trust Tenets at the Data Level

Despite some distinctions in approaches to Zero Trust, whether focused on users, devices or applications, several core consistencies have emerged across the Zero-Trust literature. These same requirements are all the more impactful when explored through a lens focused on the data itself.

Least Privilege Approach

Central to any Zero-Trust strategy is deny by default, wherein access is only granted to those with specific privileges. A Zero Trust data strategy therefore requires object-level data protection with customizable and granular access privileges, ideally based on attributes. These privileges must evolve over time, including eliminating or expanding access as attributes, roles and partnerships change. With encryption-based data protection, key management also becomes essential with least privilege access applied to the keys as well. More often than not, attackers access encrypted data through key access, not by breaking the encryption, and so key management is of paramount importance.

Portability

A least privilege approach only combines increased security with business success if those secure access privileges persist regardless of location. For data-centricity, that means that the protections must persist across devices, environments and applications, as well as physical locations, and apply to any data type.

As organizations modernize their environments and increase visibility into data silos or mislabeled and mishandled data, this modernization provides a unique opportunity to apply data protections to enable sharing and generate value from the data an organization already has.

Auditability

Zero Trust not only focuses on access control, but on persistent monitoring as well. This is a core reason visibility - and the absence of it - is so important. A Zero-Trust approach focused on the data requires logs and insights on data access attempts as well as key access. This does not mean additional tools for the operator to manage, but the logs and insights should be integrated into existing monitoring platforms to help provide context and clarity.

Each of these central tenets of Zero Trust served as baseline requirements in the design of the open standard Trusted Data Format (TDF). The next section describes the core features of TDF and how organizations can begin implementing a Zero-Trust strategy within their existing architecture.

Zero Trust with the Trusted Data Format

TDF provides a protective wrapper that cryptographically binds protections to the data at the attribute level. Instead of focusing on role-based access controls, TDF leverages Attribute Based Access Control (ABAC) to enable customized and granular data access privileges that fulfill the least privileged access approach of a Zero-Trust strategy. TDF is agentless and allows file locking, content expiration and access revocation for both structured and unstructured data of any size. Organizations and data owners can tag, encrypt, revoke, expire and audit access to data, even after content has been accessed. From micro-segments found in messaging apps to real-time streaming data, TDF provides least privileged access which can evolve over time.

These attribute-level protections travel with the data, tackling another core tenet of Zero Trust. Portable protections persist with the data, regardless of cloud environment, system, device or application. This core functionality eliminates vendor lock-in while providing greater confidence to share and collaborate while maintaining access control. It also is central to eliminating trust in third-party providers and services. Because the attribute-level data protection travels with the data, it can only be accessed by authorized recipients while remaining protected from the networks, applications, and devices through which the data flows and is stored.

Finally, TDF protocol and infrastructure enables logging every key request for reliable auditing and tracking of access requests. Audit logs identify when the data has been accessed, by whom, where and from which devices. Because the key is on a key server, it provides a cryptographic guarantee that only those with granted access can see the data. If data is removed and placed on an unauthorized system, all access attempts are logged while defending against unauthorized access. This provides an unprecedented ability to track who accesses what data, at what time, and where. Importantly, data owners determine the key management, either opting for Virtru key management services or storing their own keys for complete control.

Zero Trust Made Easy

Despite being introduced almost a decade ago, Zero Trust has yet to see widespread adoption. One of the biggest hurdles is the belief that Zero Trust does not work with legacy systems - including older architectures, workflows or transactional processes. Another challenge is confusion or fear about where to start. Regardless

of the current state of the environment, increasing visibility of users, devices and especially data and then prioritizing based on risk and sensitivity will drive the fastest results. This can be done in alignment with broader IT modernization efforts in order to align operational improvements and security benefits and allow users to share data more securely which should improve efficiency and effectiveness.

TDF eliminates these obstacles to Zero-Trust implementation while realizing the full aspirations of a Zero-Trust strategy. TDF enables data to be both protected and shared without disrupting existing investments and workflows. In fact, because usability is so essential to TDF, organizations can get started with a Zero Trust strategy today.

- **Zero Trust within existing systems:** Because TDF is platform and data agnostic, organizations can start deploying TDF today, within their existing environments.
- **Security through Obscurity No More!:** Zero Trust does not have to introduce greater complexity, but can actually simplify data protection.TDF audit features provide granular-level visibility into access attempts.
- **Software Developer Kit to streamline implementation:** The Virtru Developer Hub consists of an SDK, and key and policy management services to quickly deploy TDFs. Learn more at: https://developer.virtru.com.

For many organizations, Zero Trust seems like a desirable yet unattainable strategy. This is largely due to misperceptions surrounding the complexity of a Zero Trust strategy and confusion on where to start. By applying Zero Trust tenets to the data, it becomes simplified and achievable within existing infrastructures.

Attack surfaces are only going to continue to expand, and the combination of a proliferation of attackers, insecure third-party data practices and new regulatory requirements reinforce the growing necessity for a Zero-Trust strategy. With TDF, organizations can begin implementing a Zero-Trust strategy today. Instead of added complexity, TDF can help organizations regain data control and the confidence to securely share and collaborate anywhere without entrusting data protection to any third-party service or provider.

About Virtru

At Virtru, we understand that data is an organization's most valuable asset and sharing it is critical for business success. But sharing data creates significant risk. We believe no one should have to choose between protecting data and sharing it. We help more than 5,000 organizations, large and small, across almost every industry, protect data wherever it's created or shared so they can collaborate with confidence. Virtru provides the power to get the job done.
For more information, visit www.virtru.com or follow us on Twitter at @virtruprivacy.