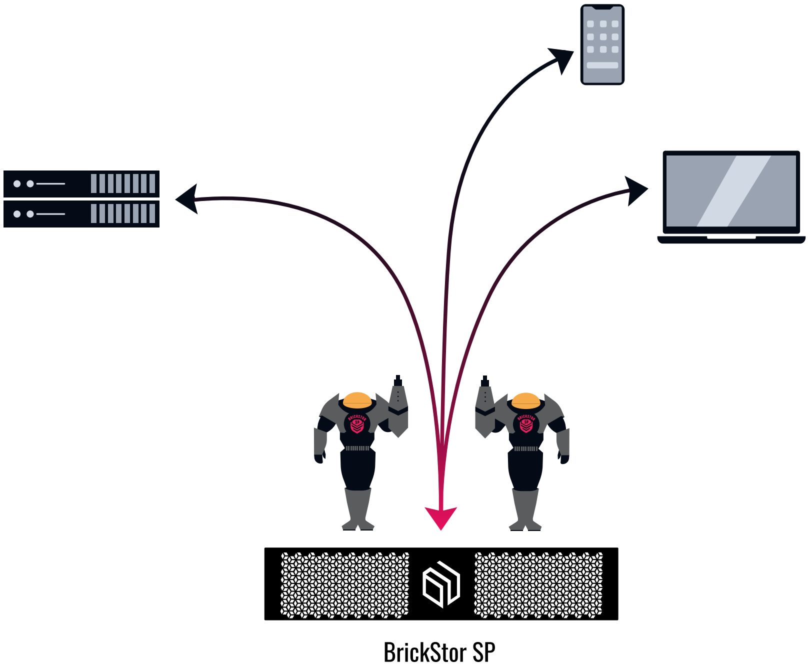
White paper

Zero Trust: Protecting Data at the Source

There are many threats to an organization’s data. High profile breaches like the SolarWinds incident have made the public more aware that state-sponsored cyber operations are occurring against both government and non-government entities for different effects, such as industrial espionage, data manipulation, or data destruction. These operations against data and information systems can be enabled in other domains and don’t solely rely on an attack in cyberspace. Both government and non-government organizations need to understand that threats against their data can come from many modalities, and that the most sophisticated attacks will involve many steps that may enable the success of the cyber operation. For example, of a complex attack could be a turncoat employeeinstalling malware on a computer that enables a backdoor for an external command and control, while a supply chain attack against a new server may enable another device to provide data exfiltration via a 5G network.

Today’s cybersecurity programs place too much emphasis on protecting the network instead of protecting the data. In the case of cyber espionage, the adversary will use any means possible to access and exfiltrate data. Therefore, it is necessary to provide better protection of files and access to files over every file protocol.

Throughout history, chokepoints have been of vital importance to a strategic defense. A chokepoint can allow for clear inspection of everything destined for the other side as well as be used to cut off a supply line or flow of information. Chokepoints are commonly used within the cyber domain by IT architects and security specialists. The most common perimeter chokepoint within recent IT architectures is the firewall. However, over the past two decades, organizations and IT infrastructures have become decentralized and encryption has become mainstream for network traffic. This has weakened the defensive value that perimeter firewalls alone can provide to protect an organization’s data. The world has witnessed that threats can circumvent the firewall through the software supply chain via email phishing and while disguised as an insider threat. Because firewalls aren’t designed to keep data inside the perimeter, adversaries use that to their advantage. The best cybersecurity practices call for a layered defense.



Organizations must create an additional chokepoint to effectively protect their data. In a distributed environment with an exorbitant number of endpoints and applications that can access data via various means and network paths, there is superior chokepoint location. It exists directly in front of the data. And only by creating a chokepoint in front of the data, can we ensure complete visibility and control over every application and user accessing the data

The adoption of a 21st century approach to data security requires moving beyond simply associating cybersecurity with network security. By placing a security chokepoint in front of the data, there is no way to get access to the data without it being audited and without full bi-directional control of who is accessing and manipulating the data. With this in place, the security is now in the data plane to protect the very asset the adversary is after - the data. By making this chokepoint an active enforcer of policy, we can dynamically change who has access to the data based on their location, time of day, current security posture, and threat condition. This approach is a key building block of the NIST zero trust architecture.

A CyberConverged® approach to data security protects the data where it lives; it provides three distinct advantages over legacy bolt-on security approaches:

1. The security controls and user behavior auditing cannot be circumvented because they are embedded in the storage operating system.

2. Organizations gain full visibility into what file is being accessed, file operation type, the size of the operations, client IP, and client ID without sacrificing performance.

3. Governance happens in real time within the data plane and does not require external access by a privileged account that could be hijacked for data exfiltration by an advanced persistent threat.

There are three phases of a cyber-attack: before, during, and after. Before an attack, a CyberConverged approach with the use of chokepoints in front of the data makes it is easier to improve cyber hygiene and establish normal behavior. During an attack, it is possible to automatically detect the attack and automatically respond based on the organization's desired response, which could include stopping the attack, slowing down the attacker, and/or alerting the IT and security teams. After an attack, organizations can quickly report on what data was compromised. The sooner the organization understands what has been accessed and compromised, the sooner it can report and remediate. Most organizations don't have this visibility, which is why it can take them months to report on the damage and compromise of an attack.

RackTop's BrickStor Security Platform (SP) with Seagate's TAA/FIPS drives utilizes and ensures a secure supply chain for software and hardware and provides a data centric zero trust architecture to protect unstructured data. RackTop's mission is to provide organizations of any size the ability to protect their data like a national secret. BrickStor is the first CyberConverged network-attached storage solution to provide unprecedented data security against nation state sponsored threats. Organizations can get full visibility into who is accessing their most valuable asset, the data. Built-in active defense capabilities can stop ransomware, doxware, insider threats, and cyberattacks before it is too late. BrickStor SP becomes an additional high-fidelity sensor for security and IT organizations to understand what is happening within their infrastructure. This information can be fused in a SIEM with other information to reduce the time to detect suspicious or malicious behavior. BrickStor SP eliminates security blind spots within the IT infrastructure.

Unfortunately, most organizations cannot answer the question of who accessed what files and when with their current infrastructure. But with BrickStor SP, if an organization suspects a breach or nefarious activity they can go back as far back as necessary to review the details about which accounts accessed specific files and from what machines and locations. This is critical in detecting abnormal behavior as well as being able to instantly report on what has been compromised after a cyberattack.

BrickStor SP's modern architecture scales to offer full security features while maintaining performance by adding a minimal amount of compute resources. A CyberConverged architecture requires 50% or less total resources than bolt-on security and compliance solutions to legacy network-attached storage and file shares. BrickStor SP's security and compliance features happen inline while the data is being read and written to the storage and processed in RAM to eliminate latency. Bolt-on architectures require double the IO to facilitate compliance and security scans, which can create additional bottlenecks and latency.

If an organization had BrickStor SP in their architecture while updating to the infected SolarWinds, they would have received at least two key benefits: real-time alerts and user behavior auditing. If a compromised system or account was used to access data anytime between March and when the malware became publicized, they would have been alerted to the suspicious behavior. For example, it would stand out if a system account or user account was accessing network file shares that they do not normally access, or if an account was accessing data from a server that users do not log into to access user files.

Once the SolarWinds malware became public, organizations had a hard time determining if they were breached. The recommendation from SANS was to look at DNS logs to see if any systems tried to connect to the malware command and control systems. Unfortunately, many organizations do not have those logs or do not have logs that go back that far, so they had to assume they had been breached. If they had BrickStor SP in their architecture, they would have had better visibility into what those systems or accounts accessed internally and what file access behaviors changed after the SolarWinds update was applied. This second benefit, user behavior auditing, is critical in helping organizations recover from an attack; without this, it becomes nearly impossible to understand if there was a breach, what was compromised, and what actions are necessary to remediate the situation.

By shifting the way we think about cybersecurity from a network approach to a data centric approach, we can simplify the problem and improve the chances of success in defending against an attack. Banks take this approach in the physical domain with alarms, multiple security layers, and holding valuable assets inside a vault. By taking a zero trust approach to the core of the infrastructure, and keeping the data inside a vault, we can drastically improve our defensive posture. This will scale with an organization as it changes shape and size and will improve our ability to defend against and respond to the most sophisticated threats.

About RackTop

RackTop Systems is the pioneer of CyberConverged™ data security, a new market that fuses data storage with advanced security and compliance into a single platform. Engineered by U.S. Intelligence Community veterans RackTop's BrickStor Security Platform is architected following a Zero Trust security model that protects data from ransomware, detects insider threats, and facilitates meeting complex data privacy and regulatory compliance requirements. BrickStor SP is a zero-impact, drop-in replacement for existing network attached storage (NAS) systems, which eliminates the cost, complexity, and added vulnerabilities of bolting on disparate security suites to legacy storage. The security platform also features an embedded transparent data mover, which can leverage third party cloud systems to tier archive data without sacrificing security or impacting customer experience. Headquartered in Fulton, Md., RackTop was founded in 2010 by cyber experts who have been solving the most complex data and security problems for more than two decades. RackTop's technology has been deployed at numerous organizations in a variety of industries worldwide, including government/DoD/public sector, media/advertising and entertainment, financial services, health care, higher education and life sciences.