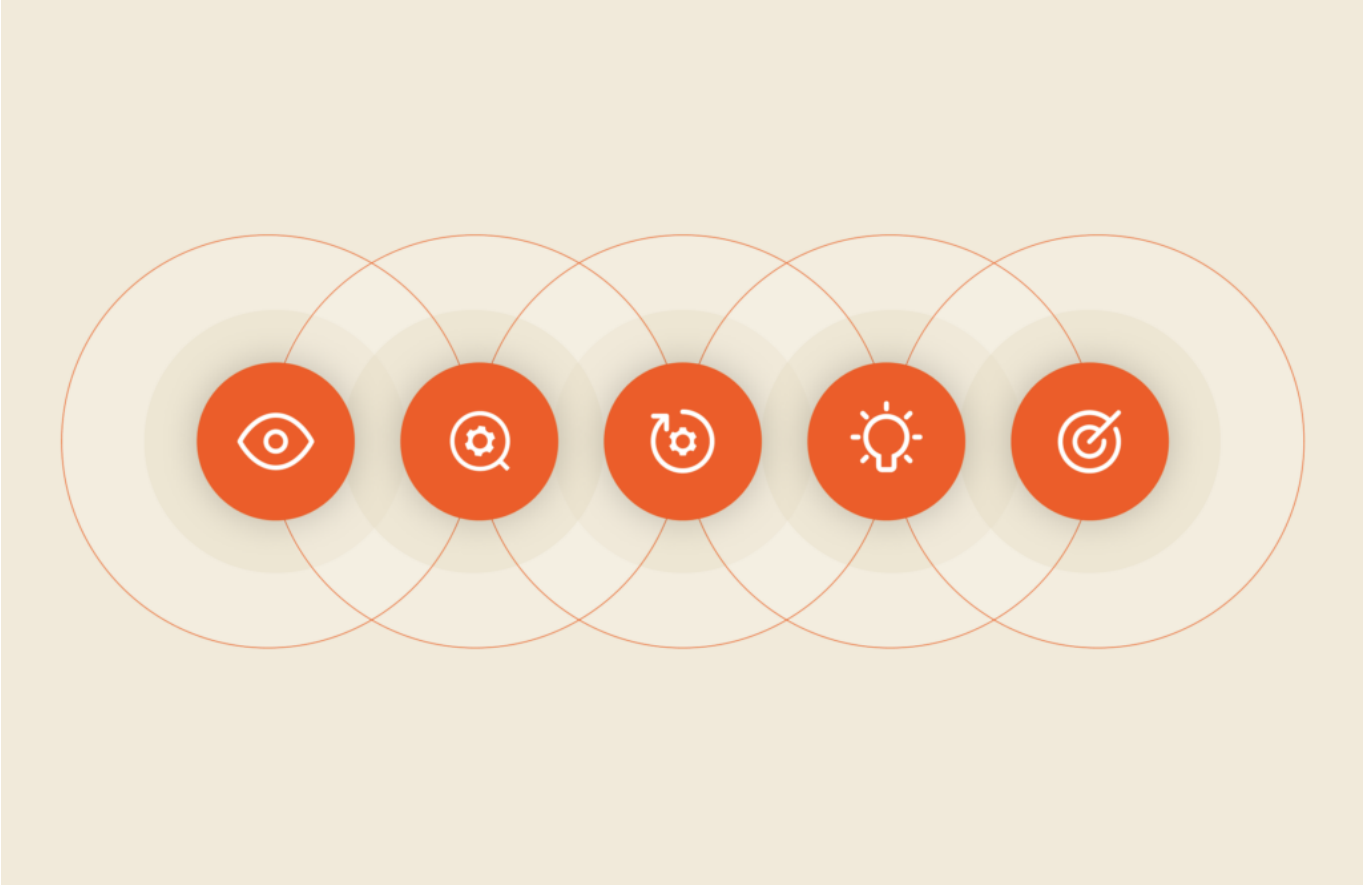
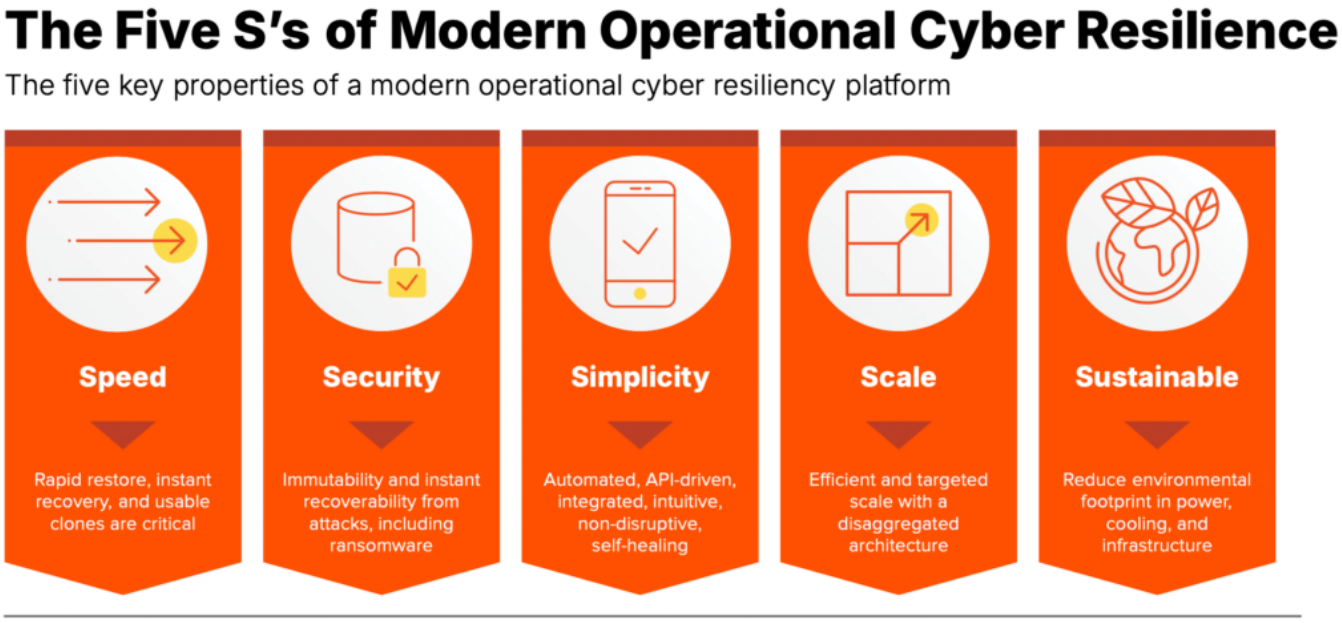
Building Operational Cyber Resilience using the Pure 5//S Principles



Cyber Resilience, (aka, business continuity or disaster recovery)) has taken a profound turn in the last 5-10 years. Previously, it was focused on natural and operational disasters like hurricanes, tornadoes, or hazardous spills on highways.

Today, ransomware, phishing, rising energy costs, automation with AI, and many additional compounding factors have increased the viability and frequency of attacks, while decreasing the complexity and time to execute them. These malicious attacks require additional steps in the recovery process, which we define as Cyber Recovery. Incident response protocols are there to understand how the attack happened, and ensure that data is free or cleaned from threats and/or vulnerabilities that were exploited.

To help address these ever-evolving threats, organizations need a next generation data platform, based on fast flash and built on five key pillars: Speed, Security, Simplicity, Scale, and Sustainability.



These principles ensure the availability of critical application data so the organization can quickly resume operations from natural or malicious incidents. They provide a secure, resilient data foundation to help you deliver dependable applications and services, , cybersecurity, and even compliance outcomes.

Let's cover how each applies:

Principle 1: Speed

> *"Speed is the essence of war. Take advantage of the enemy's unpreparedness."*
>
> *– Sun Tzu, "The Art of War," Chapter XI*

Are the attackers prepared for how fast and completely you can respond? The Speed principle is all about time to recover an application stack and restore services to your users.

When you can rapidly restore applications and environments back online, from a

known good point in time, in times measured in minutes or even hours, why would you ever need to pay a ransom? This need is not just financial, but more often regulatory as well, with requirements like DORA driving these timelines. Two hours for operational payment systems is aggressive but doable with the right choices of technology and orchestration.

Case in point, a Pure Storage customer customer's applications and data were encrypted by ransomware and restore from backup was the only option available; at this point, they had not deployed any of Pure's resilience capabilities. They began restoring the data from a widely deployed disk-based purpose-built backup appliance (PBBA), hoping the mechanical components didn't break or burn out. After 10 days, about 10% of the environment was recovered—and no critical applications. For them, rebuilding from scratch was faster than actually continuing with the restoration.

The customer implemented an architecture built on the 5S's with two key innovations enabled by Pure Storage: a layered approach to application recovery using SafeMode™ Snapshots and rapid recovery with one of our data protection partners. This allows them to test and validate a full data center recovery, quarterly, *in about three hours*. When they were attacked a second time, they were able to bring their Tier-0 applications back online in about 15 minutes—*15 minutes* to recover to a "good copy" of the data, delivered by Pure Storage.

Principle 2: Security

> *"…offensive operations, often times, is the surest, if not the only…means of defense."*
>
> – *George Washington*

A good defense helps place you in the best position to successfully respond to an attack. You want the attacker to lose the incentive to attack by increasing the cost of an attack, thereby exponentially reducing any monetary, political, or social gain from the effort. You want them to give up and move on early in the attack.

We can accelerate and take action in collaboration with security applications and

XDR/EDR systems. Importantly, one of our core objectives is the security and recoverability of your data and the applications that allow it to be purposefully used. A defensive security footprint must engage in three key areas:

1. **Perimeter detection:** The first defensive barrier that occurs at the network edge. Firewalls, intrusion detection, VPN, and access controls such as multi-factor authentication are all best practices to employ. This helps reduce the blast radius of an attack by isolating applications on a network and a protocol level, increasing the difficulty of getting further into your network and applications.
2. **Processing detection:** This second layer of defense enables you to assess the behavior of application consumers as it's occurring. "Is this process behaving correctly?" "Has this user behavior or interaction profile changed?" These questions are asked by SIEM class systems to determine if an attack is in progress.
3. **Persistence detection:** This introduces capabilities to assess data in storage systems for active or latent threats, as well as providing the ability to restore known copies of your data, nearly instantly.

At the persistence layer, infrastructure systems must meet two functional definitions: indelibility and immutability. These properties ensure a privileged attacker is not able to change the security posture of the system, nor eradicate data in the system, without predefined retention periods completing and manual out-of-band authorization processes. At Pure Storage, we call this indelibility enforcement layer SafeMode, which builds upon our immutability layer, volume snapshots, providing an unchangeable point-in-time representation of your data.

Principle 3: Simplicity

> *"We tried to make something much more holistic and simple. When you first start off trying to solve a problem, the first solutions you come up with are very complex, and most people stop there. But if you keep going…you can often*

times arrive at some very elegant and simple solutions. Most people just don't put in the time or energy to get there."

– Steve Jobs, Interview in "Newsweek," October 14, 2006

This mantra is what made Apple's "iDevices" so successful. Unfortunately, simplicity is very hard to do. Simplicity at its core allows teams to focus on what's innovative and important to a business. Teams overwhelmed by alerts and false positives, struggling to secure disparate systems and apply modern security tools, the technical debt of legacy architectures, or the mundane and repetitive tasks of poorly built systems all distract from what the business is truly trying to achieve.

What if a system was simple to deploy? Simple to operate? Self-healing? Didn't require low-level management of LUNs? Could identify known good copies of data, or better yet, what data has been compromised? Would trigger automation workflows to protect applications and services when an attack is detected?

Surely, this would result in more available applications and fewer critical incidents. Imagine what you can build with this change in mindset and technology.

Principle 4: Scale

"Engineering is the closest thing to magic that exists in the world."

– Elon Musk

One of the most difficult engineering challenges to address is scale. When an environment is constrained to a fixed quanta of resources, optimizing it is relatively straightforward. Workloads, consumption, and utilization could be bound thereby ensuring service levels. Today's internet-scale systems have created a new paradigm. We must learn new techniques, grow beyond old answers, and innovate in ways we hadn't previously considered.

Effecting scale of applications and data is a combination of innovating at the protocol layer, network layer, metadata layer, and storage persistence layer. I use

"storage persistence layer" because the traditional "filesystem" term and concepts are no longer how scalable and performant systems are being built. New innovations in this area abstract such concepts from the protocol layer and use newer techniques such as key-value stores to ensure scale and durability.

Network scale is a substantial problem for the data center. Each port provisioned brings with it requisite capital, operational, and raw data center costs such as power, cooling, and rack space. One way to improve this is to ensure that data storage and network ports scale independently. Disaggregating these components ensures that storage growth can focus on increased capacity, transactions, and throughput—not increased infrastructure costs.

A large bank in the US was not meeting its SLA for restoration from backup. The current system consumed 700+ 10Gb network ports and was not able to deliver on timely recovery throughput. Pure Storage, with one of our cyber resilience partners, delivered a solution that dropped network port count to under 100 10Gb network ports and substantially exceeded recovery SLAs. The bank saved floorspace, infrastructure costs, and data center costs and has since expanded the system multiple times.

Today's network bandwidth can enable new capabilities—for platforms that can handle it. It requires an architecture model that takes into account arbitrary scale of the system: storage, compute, and network resources.

Protocols and APIs are also important in this disaggregated architecture. Resilient applications should simply connect to an endpoint (e.g., a URL for S3 protocol cloud storage consumers), and the service *automatically* balances connections across every compute, network, and storage resource available. No special configuration or techniques—it's Evergreen because it just works, and you never have to migrate data or take an outage again, raising the limits of scale and service availability.

Principle 5: Sustainability

> *"The key to understanding the future is one word: sustainability"*
>
> *– Patrick Dixon, "Futurewise"*

Sustainability collectively refers to the sum of resources required to run and maintain a system: power and cooling costs, operational effort, or the components required for a given task. Reducing resources directly improves the sustainability of systems and solutions. As energy costs rise, resilience will mean staying ahead of resource limitations with next-gen efficiency.

In this article, "How Modern Storage Can Offset Power Utilization in the Data Center," we learn how our purpose-built DirectFlash® Modules save tremendous energy, floor space, and associated cooling costs. It's not just storage costs and performance that are impacted; it's every operational cost associated with infrastructure.

I have seen customers use this to make the data center economics of new critical projects viable. One consolidated 34 racks into 4 racks, an 88% reduction in racks, infrastructure, and all associated utilities! One multiexabyte-scale video provider anticipates saving so much power, it may amount to megawatts across all data centers, while dropping network port requirements and infrastructure down by an order of magnitude. These free up costs and resources to provide a better customer experience while ensuring resources are available for critical next-generation innovation.

The Pure Storage platform also impacts *employee sustainability.* After deploying a cyber resilient architecture built on the 5S's, the employees of the company mentioned earlier in Principle 1 stated that *they won't work anywhere without this level of ability to recover applications*. With Evergreen, the risk introduced by forklift upgrades and data migrations is a task of the past, as are change control meetings, migration planning, scheduled application outages, parts replacement, and other operational efforts.

Conclusion

> *"There is a great satisfaction in building good tools for other people to use."*
>
> *– Freeman Dyson, "Disturbing the Universe"*

The 5S's are key properties that when applied to cyber resilience architectures,

allow you to provide a better service and experience to your customers. It substantially improves SLAs, reduces cost and complexity, and frees up resources to tackle the next big project.

Reach out to your Pure Storage team and ask to speak to a cyber resilience specialist to learn how the 5S principles will help you.