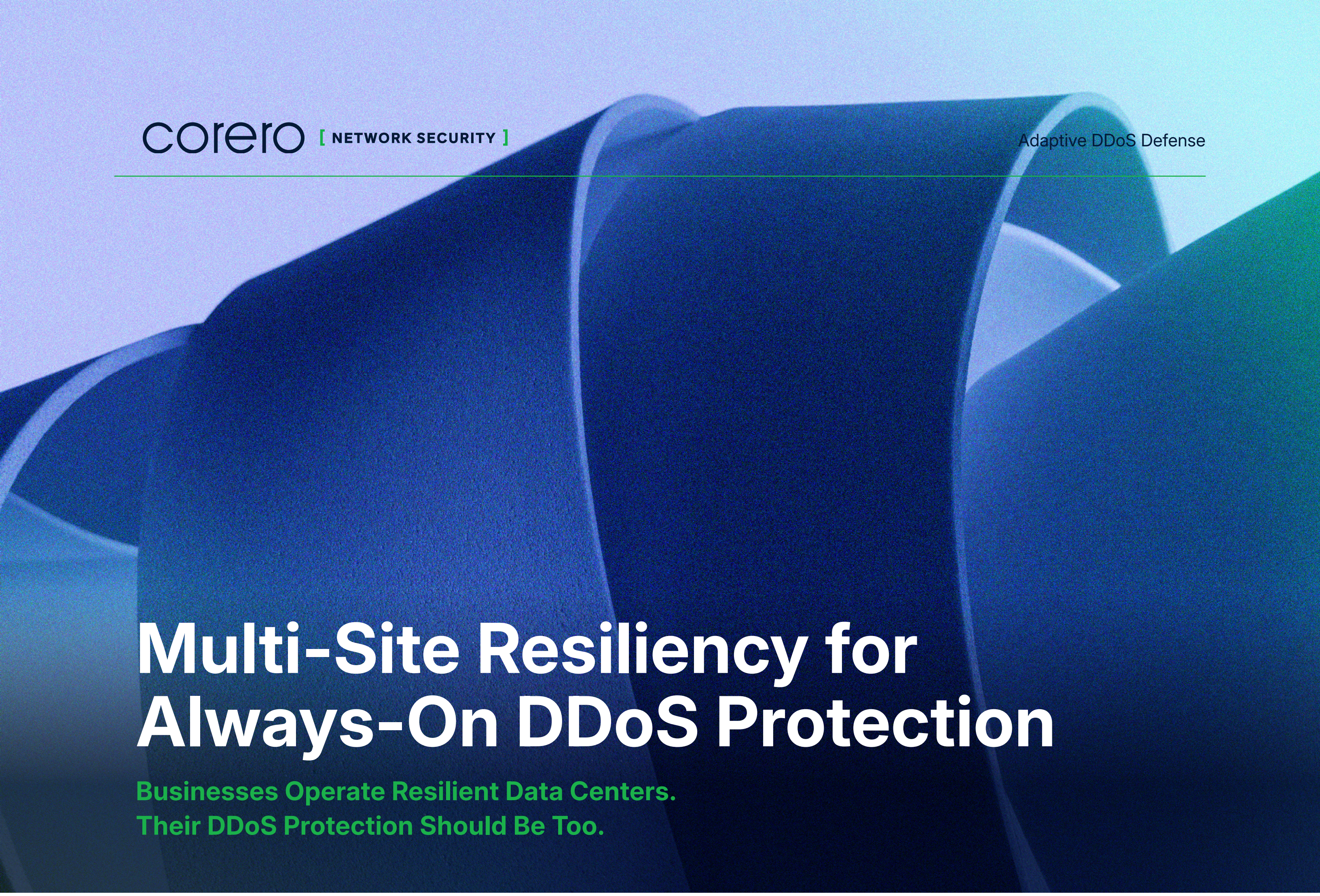


Multi-Site Resiliency for Always-On DDoS Protection

Businesses Operate Resilient Data Centers. Their DDoS Protection Should Be Too.

AI-driven applications, cloud services, and real-time connectivity demands have made multi-data center operations essential. Enterprises and service providers are expanding their footprints to ensure uptime, redundancy, and performance. But co-location alone isn't enough. Best practices for resilient DDoS protection haven't kept pace.

Many organizations still rely on outdated high availability (HA) models that focus on local failover—leaving them exposed to downtime, security gaps, and reactive mitigation.

DDoS attacks don't stop when a data center, or its defenses, fail. Protection must be system-wide and as resilient as the network itself.

Downtime is More Than a Technical Issue

Resiliency isn't optional. It's essential.

Even a few minutes of downtime can cost providers and enterprises millions in lost transactions and SLA penalties. Customers expect 24/7 availability, and a single outage—especially one caused by a security event—erodes trust and drives them elsewhere.

Manual reconfiguration wastes resources and creates unnecessary risk. Reactive approaches require significant time and effort to restore mitigation, leaving businesses exposed when they can least afford it.

Multi-Site Resiliency Ensures Always-On DDoS Protection

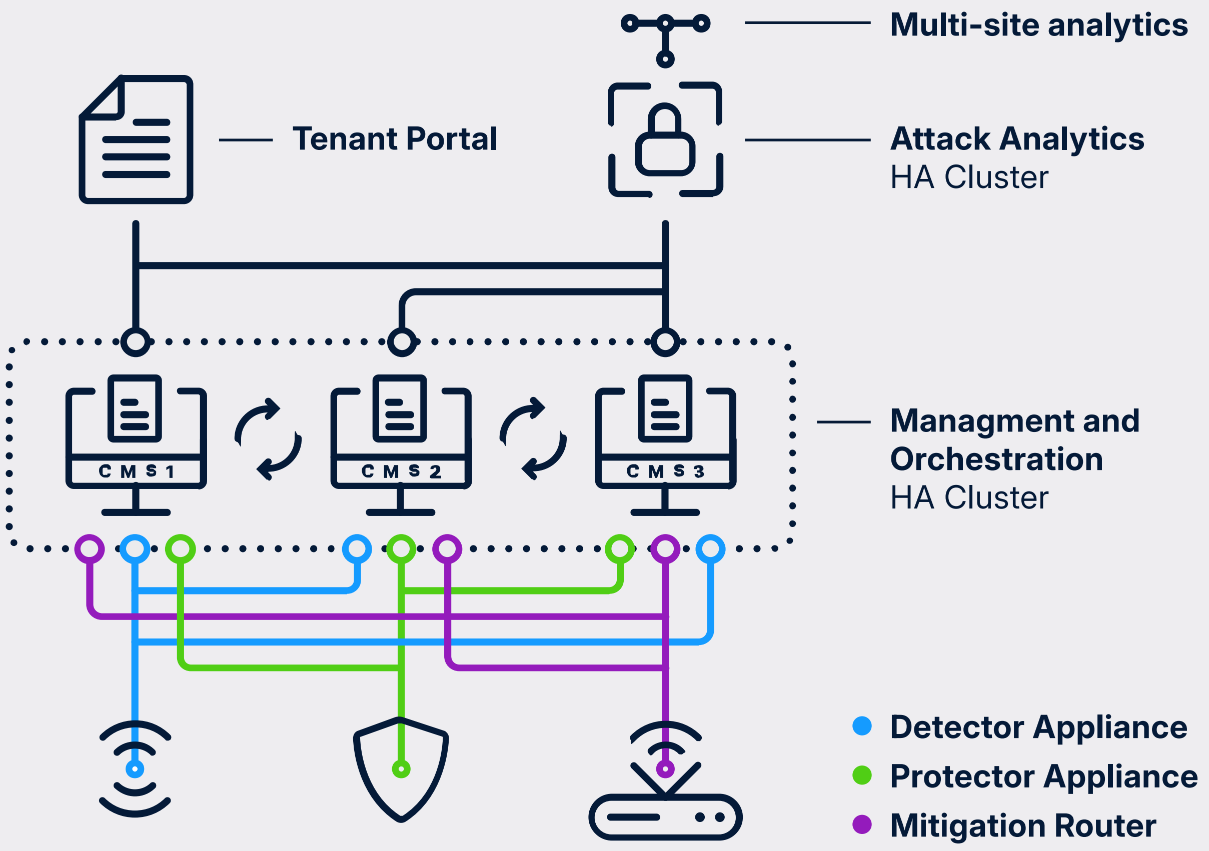
Maintaining full visibility

Traditional high availability (HA) models rely on passive failover, where security only activates after a failure is detected. This reactive approach leaves businesses exposed to downtime, security gaps, and operational delays. Multi-Site Resiliency eliminates these risks by delivering real-time, seamless protection across multiple locations—without disruption.

Corero Management Servers (CMS) act as the enforcement and visibility management plane, distributing security policies and ensuring consistent DDoS mitigation across all active sites. Unlike legacy failover models, our system doesn't miss a beat if there is a failure.

Policies synchronize continuously, so if a data center goes offline, security enforcement and mitigation remain fully operational at other sites—without delays, manual intervention, or reconfiguration.

Traffic flows through resilient protectors, detectors, or customer-deployed routers, depending on network architecture. CMS delivers seamless orchestration, ensuring security enforcement remains in place, no matter where traffic flows. Whether an outage is caused by a power failure, fiber cut, or catastrophic event, the security layer stays intact—maintaining full visibility and blocking threats in real time.



How Multi-Site Resiliency Works

Attacks don't pause. Neither should your protection.

Built to protect your resilient infrastructure

You've invested in making your infrastructure resilient. But DDoS attacks threaten that stability. Your DDoS protection should be just as resilient. Our solution delivers adaptive, site-wide protection across your entire environment—ensuring uninterrupted service availability and seamless defense, all within a single system.

Seamless enforcement across locations

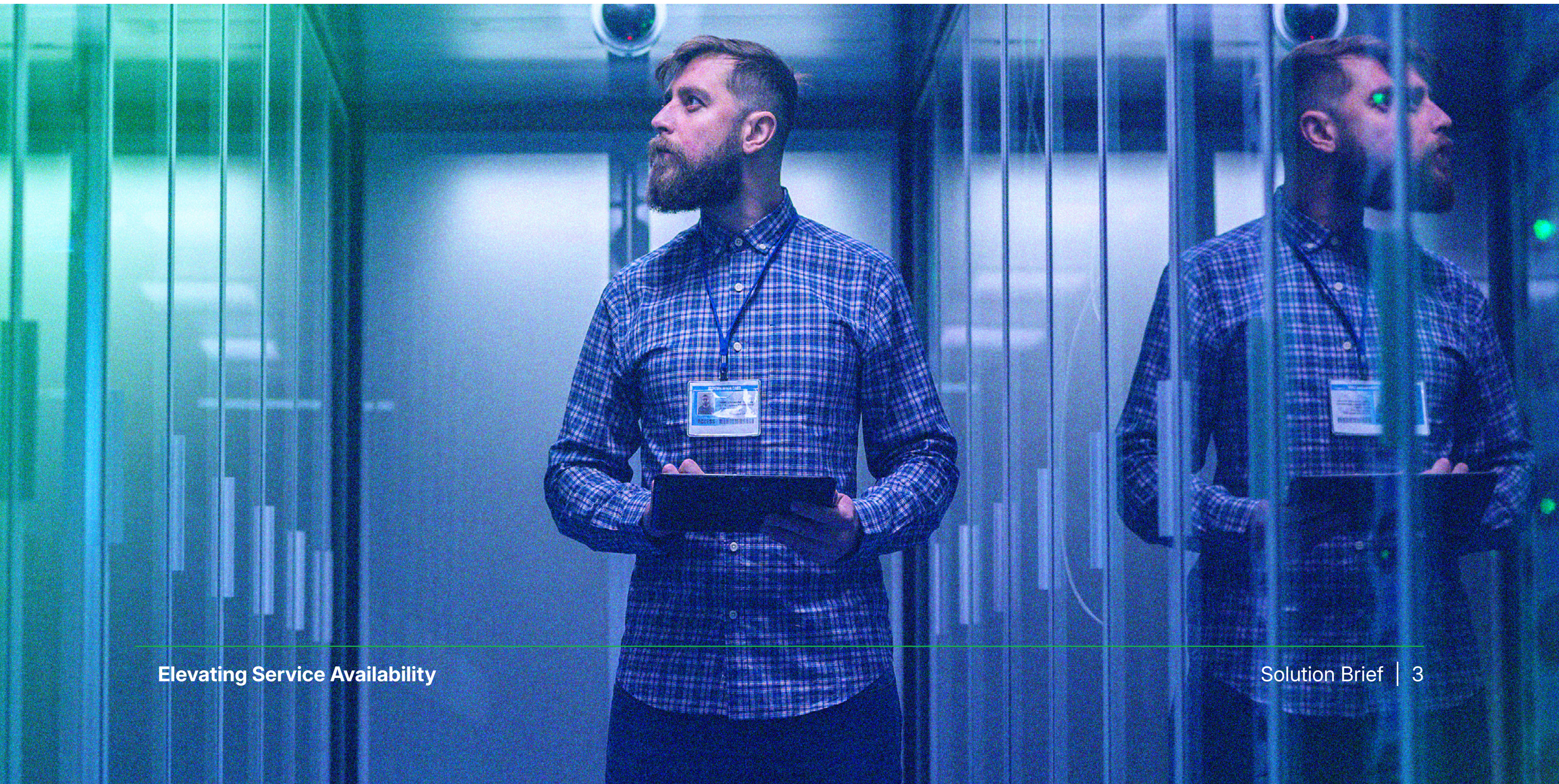
The management and orchestration plane stays operational even during a failure, ensuring that security policies and mitigation actions remain active across sites—without manual intervention.

Active-aware protection, not passive failover

Rather waiting for a failure to trigger a manual failover, our system allows DDoS defenses to operate across multiple locations simultaneously, eliminating gaps and delays in mitigation.

No reconfiguration or security gaps

If a data center goes offline due to power failure, fire, or network outage, DDoS protection across the remaining infrastructure stays active. Security policies are automatically enforced at another site—no manual adjustments needed.



Get Resilient DDoS Protection Now

Resiliency is the next evolution

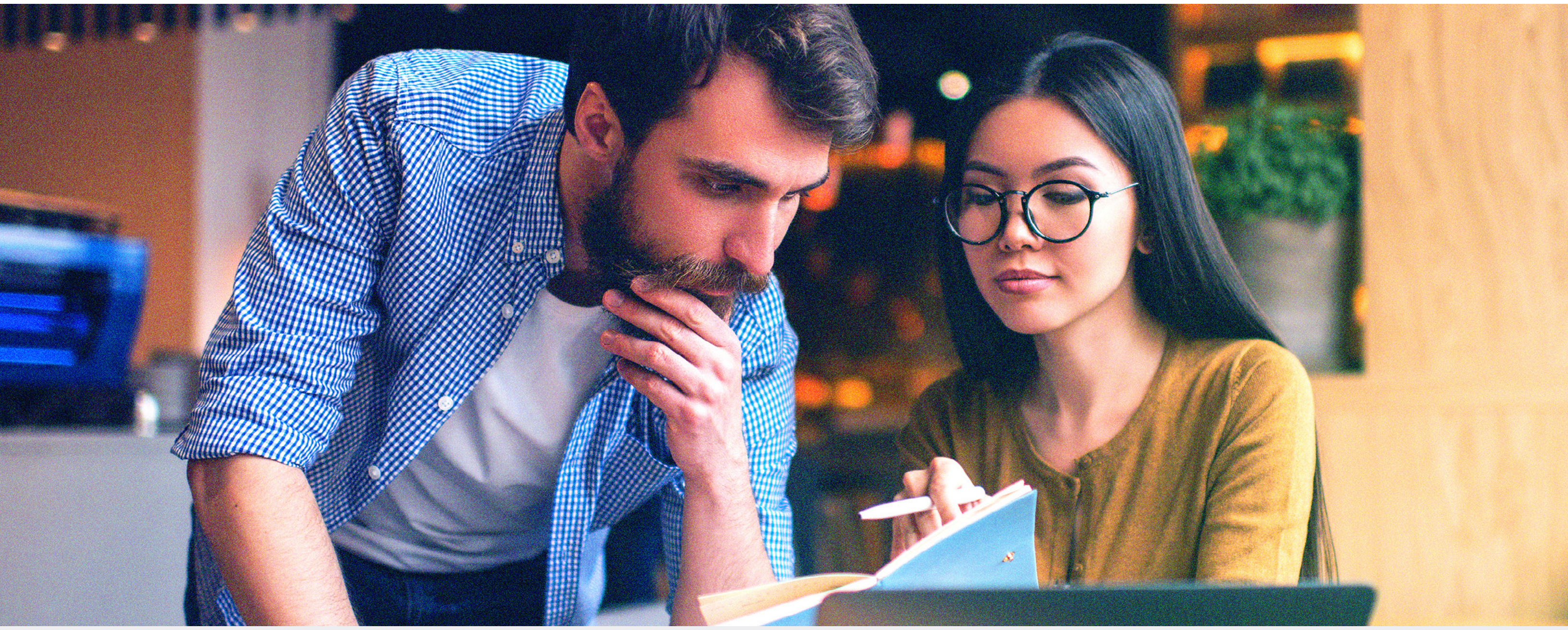
Traditional HA solutions weren't built for today's hyper-connected world. Multi-Site Resiliency is the next evolution—delivering adaptive, always-on protection that keeps your business online, no matter what.

Minimize downtime and prevent costly service disruptions.

Eliminate manual intervention with automated, intelligent enforcement.

Protect your reputation with 24/7 service availability.

Reduce complexity with seamless, real-time protection.



Local Redundancy vs Solution-Wide Resiliency

Talk to a specialist today to see how Multi-Site Resiliency ensures continuous protection and service availability—even in the face of failure.

SPEAK WITH A SPECIALIST