

Enforcing End-to-End Trust in Business Services

Enterprises and government agencies are facing increasingly borderless computing environments with mobile, cloud and now the Industrial Internet of Things. Delivering secure and trusted digital business services has never been more difficult with constant cyber-attacks on their infrastructures.

Traditional security approaches focused on detecting breaches simply cannot keep pace with the continuous change in today's environments. A new, adaptive approach to cyber defense is needed to support today's rapidly evolving technological and operational environments.

An adaptive cyber defense model must enforce end-to-end trust across the business, supporting any enterprise, cloud and hybrid environments. Why this so important? Simply, systems that are exposed to unauthorized or unidentified network connections are vulnerable to attack, and erode the trust in a company's ability to protect critical services. An adaptive cyber defense model ensures that only identified and authorized users or devices can see and access sensitive systems and data by dynamically establishing and enforcing endpoint trust models.



An adaptive cyber defense model must dynamically segment both networks and complete data centers, and be able to enforce consistent segmentation policies across enterprise and cloud environments. Micro-segmentation using identity can effectively block any identity from seeing and accessing unauthorized systems or network segments. This enables full access control of which identities can access the network, effectively cloaking systems from all unauthorized traffic without requiring any change to the network.

The Keys to Adaptive Cyber Defense

To effectively meet these new challenges and prevent cyber breaches, an adaptive cyber defense model must address three key needs.

An adaptive cyber defense model must proactively isolate applications and cloud systems to prevent attacks, rather than simply react to attacks after a breach has already occurred. Isolation can block or redirect unauthorized or unidentified access to cloud services, providing real-time protection of critical business services at the network layer.

A New Adaptive Trust Model

BlackRidge provides a new approach to cyber defense through the BlackRidge Adaptive Trust Model. BlackRidge operates across network boundaries, effectively cloaking networks and systems from unauthorized access. This enables companies to explicitly trust who is accessing and traversing their network to better protect key business services, and reduce the risk of insider threats, DDOS and replay attacks.

The BlackRidge Adaptive Trust Model is based on the following three technical pillars, which together enable the most comprehensive solution to preventing cyber loss.

End-to-End Enforcement of Trust

BlackRidge authenticates identity and enforces policy across network boundaries, without impacting network compatibility. Custom end-to-end trust models and security configurations are managed for each endpoint application, device and host, which can be dynamically changed in response to attacks.

Identity extends across any network boundary and policy is enforced at multiple points. This end-to-end security architecture reduces risks from remote and branch office access into any application or business service over the cloud or a corporate network.



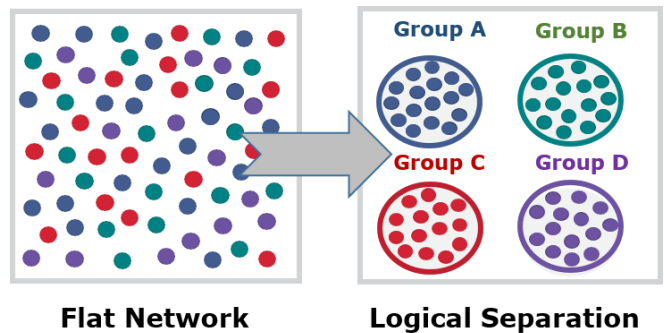
Software- and Identity-based Network Segmentation

Segmentation is increasingly impractical to maintain in today's IT environments. Traditional approaches of maintaining ACLs and firewall rules has high administrative overhead and network topology dependencies. Using firewalls for network segmentation is costly and can impact application performance.

BlackRidge provides a software-based approach to segmentation with identity-based access

controls to block or allow network connections. This provides granular and topology independent security zones on shared networks without creating separate physical or logical networks.

Identity-based segmentation offers a practical way to describe and monitor access policies, handle exceptions, and provide proof to auditors and regulators of your controls, including actions taken by individual users.



Isolation of Cloud Services and Management Control Networks

Applications and cloud services are dynamically isolated in real-time, at the first packet of a network session. The solution blocks or redirects unidentified or unauthorized traffic, including port scanning and network reconnaissance, isolating and protecting these services at the earliest time.

BlackRidge isolates and protects IT management networks, control planes and management systems across the cloud from unauthorized users and devices. This additional layer of protection lowers risks of IT management systems being attacked.

About BlackRidge Technology

BlackRidge Technology provides an adaptive cyber defense solution that enables our customers to deliver more secure and resilient business services in today's rapidly evolving computing and cyber threat environments. The BlackRidge Adaptive Trust Platform provides an end-to-end security solution that proactively isolates cloud services, protects servers and segments networks.