Application Chambers

Cybersecurity Defense at Application-Scale

zentera™

"The Corporate Perimeter is Dead…"

The industry is on the verge what may be the most radical overhaul of enterprise network security tools and practices in history. That's because cloud and hybrid computing and remote work have exposed the fact that the traditional network perimeter security business model – delivered as part of the network infrastructure – is fundamentally broken.

Think about it. Firewalls are complex to program and maintain; they are intended to handle all corporate traffic at the network perimeter. Yet a firewall can only guarantee that packets flowing through it are secure. It can't secure packets it never sees.

Growing infrastructure complexity and cloud adoption are making it increasingly difficult to distributed traffic through specific security enforcement points in the network.

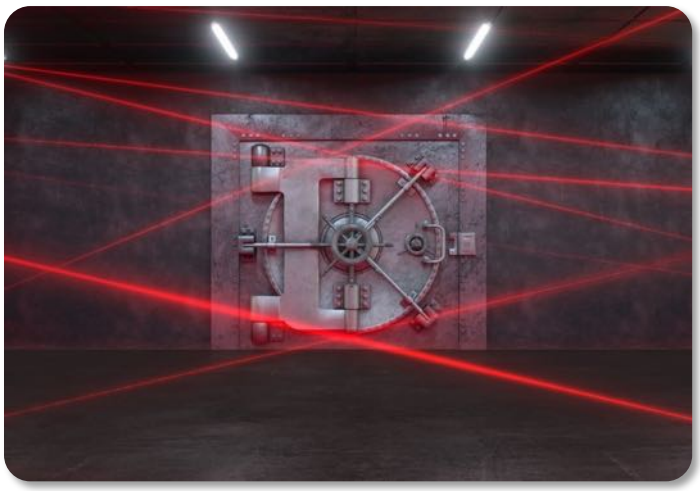
Many public companies have implemented network zones to protect financial data for years, driven by compliance requirements such as Sarbanes-Oxley (SOX). Typically implemented using VLANs with more firewalls, secure zones are reserved for the most sensitive applications and data. Could this model evolve to solve new security challenges?

But you can't just put firewalls everywhere… right? Clearly cost and effort just won't scale with traditional infrastructure, and agility targets won't be met either – today's applications and users are far too dynamic for infrastructure to keep up with. A more flexible solution is required to deploy alongside the applications and data and move elastically with them.

That future is here today, and it's called an *Application Chamber*.

Infrastructure solutions work well when requirements don't change.

They're not a great choice for things that are more dynamic – like next-gen applications and data.



An Application Chamber wraps protections around sensitive applications and data. It is delivered as software, decoupled from underlay infrastructure, and provides multi-layered defenses against malware, insider threats, and ransomware.

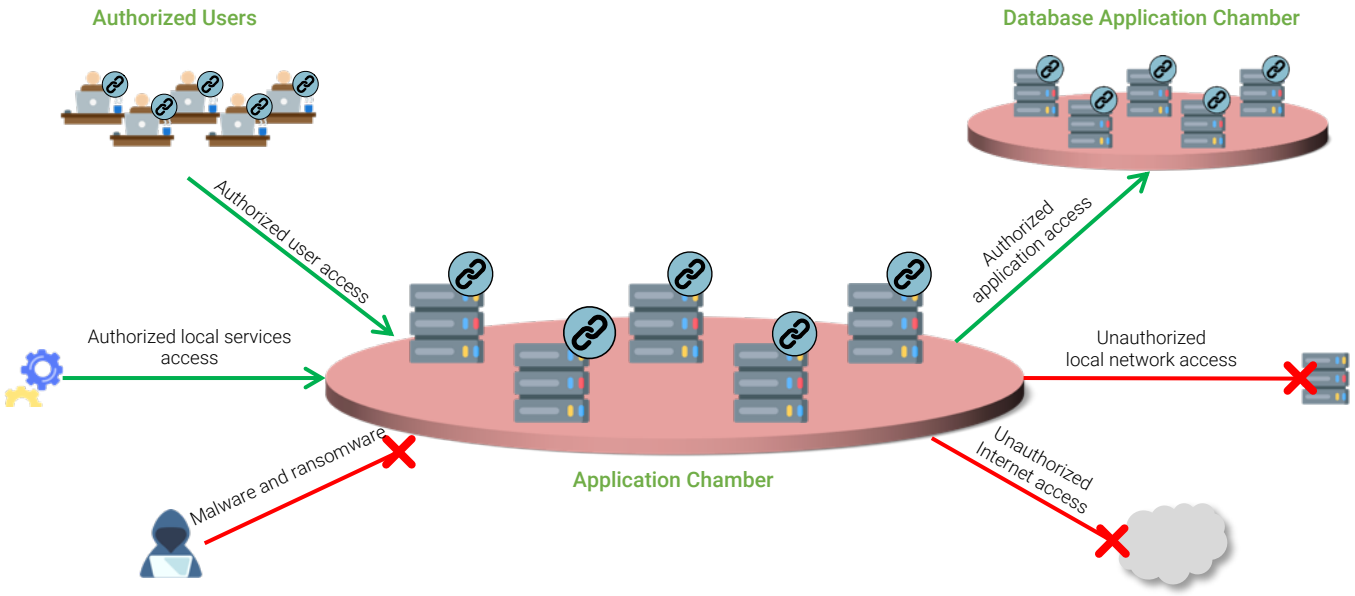
"Long Live the Application Chamber (Perimeter)!"

An Application Chamber is a new "application-scale" perimeter that protects applications and data, right at the application edge, by ensuring that all network traffic, both inbound and outbound, undergoes a full security inspection. It deploys as software, enhancing the security of existing application servers without disrupting them or setting up new infrastructure.

Zentera's CoIP® Access Platform allows you to quickly configure Application Chambers to manage groups of servers by their role or function. Application Chambers support access policies that allow you to model tiered or interconnected applications, while automatic learning and easy policy templates allows you to rapidly secure existing applications.

Fully integrated with CoIP Access Platform's Zero Trust Network Access (ZTNA), you can provide on-prem or remote users instant, least-privilege access to specific chambered applications.

And best of all, Application Chambers work everywhere you need them, to protect bare metal and virtualized apps in any environment – on-prem, cloud, or even 3rd party-owned infrastructure.



Application Chamber Features

Application Cloaking

Application-scale secure zone, inaccessible on the shared network

Ransomware Defense

Blocks ransomware from accessing vulnerable application servers

Data Leak Prevention

Blocks unapproved access methods, so data stays locked in the Chamber

Zero Trust

Natively integrated with ZTNA to authenticate and authorize each access

Template-Based Policies

Static policies that are enforced dynamically to react to changing workloads

Use Cases for Application Chambers

CoIP Access Platform's Application Chambers are incredibly powerful due to their tight integration with ZTNA. Together, they enable CoIP Access Platform to solve a variety of enterprise security and compliance challenges:

- **Cloaking sensitive applications (ERP, AI/Big Data, etc) to protect them from lateral attacks inside the enterprise**
- **Safeguarding critical data against exfiltration and insider threats**
- **Blocking ransomware and worm activity from reaching protected servers**
- **Enabling remote employees and 3rd parties to applications without exploring the network**
- **Maintaining a single consistent and auditable set of corporate policies across all hybrid environments**

How an Application Chamber Benefits Your Business

CoIP Access Platform enables enterprise to easily implement next-generation Zero Trust Security for application access security and control. The business benefits include:

- **Lower cyber-risk through dramatically reduced attack surface**
- **Promotes adoption of next-generation Zero Trust security, while avoiding "rip and replace" of the existing infrastructure**
- **Reduces employee stress by shifting the burden of maintaining cybersecurity to tools and processes**
- **Dramatically lower TCO and improved ROI compared to traditional infrastructure security, due to agility and consolidation of tools and methods across all hybrid environments**

More Resources

On the web: www.zentera.net

Email: sales@zentera.net

Phone: +1 (408) 436-4811