Stealth technology for your network.

The race to stay one step ahead of cyber threats is a billion dollar industry. What if you could take yourself out of that race? What if you could make your computer systems and critical assets invisible to attackers?

Enclave lets you securely connect with others on the Internet without creating a footprint that attackers can discover, profile or target. Enclave cloaks your networks and the applications living inside, rendering your systems invisible to attackers. Our innovative authenticate-then-connect (AtC) technology prevents discovery, data interception and attack, allowing you to remove yourself from the cyber security target landscape — for good.

Protect vulnerable systems

Attackers are pointing cyber-weapons at your organisation's digital footprint. Enclave allows you to safely connect your internal systems, critical infrastructure and supply chain together, without creating a footprint.

Be invisible, stay secure.

Enclave is pioneering authenticate-then-connect (AtC) technology. A paradigm shift from conventional "connect first, then authenticate" systems. Enclave places powerful discovery-resistant "cloaks" around your critical endpoints and applications rendering them undiscoverable, protected from electronic observation and targeted cyber-attacks.

Deploy, work, destroy.

Establishing secure connectivity is hard. You need specialists to first plan, design, security test, and make risky changes to your network. Enclave is different. It works without changes, which means you can deploy in seconds. Use Enclave to work for minutes, days, or even years, exchanging sensitive data in private, invisible networks. Then, when your project ends, the network is destroyed.

Automatic security

Enclave uses elliptic curve cryptography, AES256, digital certificates and perfect forward secrecy to automatically provide mutual authentication and guarantee end-to-end encryption — without you needing to set it up.

Security meets convenience.

Computer networks are either secure, or convenient — but not both.
Enclave changes this. Focus on the task, not the network.

1

Deploy stealth networks

Using out-bound only traffic and client-client connections, Enclave builds stealth networks that cannot be discovered, targeted, or attacked. Forget about ACLs, keep your firewall closed and "cloak" your systems from sophisticated adversaries.

2

Authenticate-then-connect

Security today revolves around the broken concept of connect first, and then authenticate. Enclave is different. We are pioneering authenticate-then-connect technology, to prevent attacks before they even start.

3

Automatic encryption

Enclave handles security automatically, and you don't need a specialist to set it up. All users get mutual authentication, end-to-end encryption, and perfect forward secrecy for safe connectivity.

Security

4

Deploy, work, destroy.

Enclave provides "on-when-you-need-it" task, purpose, or project specific networks. Deployable in seconds, an Enclave network can last for years, or just a few minutes depending on your requirements. When your project ends, the network is destroyed.

5

Don't change your network

Enclave works without changes to your underlying network infrastructure, so you get secure connectivity, without the inconvenience, setup time, or risks of needing to make configuration changes to your network.

6

Auto-expiring connections

Enclave networks are based on public-key infrastructure, where all members hold a digital certificate. When a member's certificate expires, so does their connection to the network, leaving no legacy configuration to maintain, manage, or secure.

Convenience

Use-cases

There are five main reasons why customers choose Enclave:

1. To protect unpatched, or unpatchable legacy systems.
2. To protect the assets and infrastructure that gives their organisation value.
3. To work, or collaborate with someone they don't fully trust.
4. To connect different cloud providers together, with a network that works the same everywhere.
5. To migrate Multicast-based applications to the cloud, without having to re-design them first.

1. Unpatched/Legacy Systems

Legacy systems exist in all large organisations, often running highly specialised applications, or software written by third parties.

The problem with legacy systems is that at some point in their lifetime, the support cycle ends and they become unpatchable, and difficult to maintain. The cost of upgrading legacy computers, or rebuilding specialised applications, can mean keeping legacy systems online is both a necessity, and an organisational liability.

For example, many police forces in the UK rely on specialised applications, built for outdated operating systems which no longer receive security updates.

Preserving data security while remaining compliant and maintaining legacy systems presents increasing monetary and reputational risk for organisations, leading many to apply mitigating controls, rather than upgrade — with the board room asking what compensating controls are in place.

Teams tasked with management and maintenance of legacy systems suffer too. It's not just the time management, and cost factor of setting up separate networks, but keeping them interconnected, fielding support calls, and the challenge of hiring and motivating teams to work with old technologies.

We can help. When you protect vulnerable, or legacy systems with Enclave, you are:

1. Deploying a powerful cloaking technology to hide vulnerable systems from sophisticated adversaries.
2. Removing the risks of making network changes to work around legacy systems.
3. Using authenticate-then-connect technology to guarantee that only the correct parties are granted access, at the correct times.

Enclave buys you time. Bolstering your network security, lowering the risks of maintaining legacy systems, and reducing your team's workload.

2. Protecting organisation value

Organisations build virtual castles to defend themselves online because the Internet can be hostile. But what happens when you have to work with people who don't live inside your castle?

Secure connections between employees and partners are vital for safely sharing data, and when your team is starting a new project, working with suppliers, on-boarding new employees, reviewing contracts, finalising deals, or planning new acquisitions, they do it online.

Usually the tools your employees want to use live in the cloud; fast and modern, but outside of your control and on shared platforms. Hacks, legal requests, data-breaches and vendor mistakes can, and do, regularly expose these communications. Regulatory compliance, reputation damage, downtime, and monetary losses are all major concerns that we can help to mitigate.

Our customers use Enclave to work together safely in transient, secure networks. Purpose built for each task or project, and then destroyed — in way that preserves CISO sanity.

3. Sharing data, without full trust

Organisations regularly need to work outside of their established castle walls. When our customers need remote access for people, or systems, they tend to be most concerned by three main risks:

1. Distrust of the other organisation's IT security. For example, lawyers who have to work with other lawyers, or banks who have to work with other financial institutions. Enclave provides a convenient way to quickly, directly and securely connect with organisations that you don't fully trust, without putting either side at risk.

2. Running vulnerable applications that can be abused, leading to a data breach. Consider an EHR (Electronic Health Records) provider with an end-user application for doctors and nurses accessed over the Internet. Restricting access with VLANs and ACLs isn't good enough. IP addresses tell you where, but not who, or what something is, leaving you to defend applications from stolen credentials, brute force attacks, denial of service flooding, information disclosure, zero-day exploits, SQL injection and so on.

Enclave can safely provide a mobile workforce with secure access to sensitive systems without the complexity and exposure of a VPN, or the headache maintaining ACLs.

3. Complex security procedures preventing a transaction from taking place. For example, many law firms still rely on air-gapped systems for security - turning employees into human couriers to move sensitive data between offices and across borders, rather than setting up complicated virtual private networks online, where configuration mistakes can be catastrophic.

Enclave makes it safe to work with organisations that you don't fully trust. Once you've setup an Enclave, any resources you put inside it are only accessible to other members of the same Enclave, and you control who has access, when, and for how long.

Suppose you need secure video collaboration. Add a video server to an Enclave network and invite your cross-organisational team. Now everyone has access to run secure, directly connected video conferences that are invisible to the outside world, hidden from attackers, and segregated from your primary network. When the project is finished, destroy the network in a matter of seconds.

4. Multi-cloud environments

Enclave provides a networking layer that works the same way everywhere. It delivers the capabilities of VPN, SDN, and SD-WAN allowing you to manage all of your connected resources across local, cloud, wide-area and mobile networks, as if the whole planet was your own private network.

Devices get an additional IP address when participating in an Enclave network, and no matter where the device or system connects to the Internet, the Enclave address never changes. This gives engineers a constant, and predictable way to address their entire IT estate, no matter where the systems are located, without ever needing to make a firewall change, or expose servers to the public internet.

Predictable IP addressing gives you truly seamless connectivity. Deploy with the certainty that your resources have lifetime-fixed addressing, to give your infrastructure protection from IP address conflicts, regardless of the underlying network, and future providers you might migrate, move, or expand into.

Avoid the complexity and limitations of VPCs and VNETs. Connect all of your devices, systems and cloud compute-resources together easily. With Enclave your engineers can spend more time on activities that differentiate you from your competitors, and less time on tasks that don't — deploying VLANs and NAT, re-configuring firewalls, adjusting ACLs and debugging VPNs.

Put simply, whether you deploy Enclave on a short-term transient basis, a medium-term per-project basis, or as a long-term network fabric, Enclave turns your network into a competitive advantage.

5. Enable Multicast in cloud

Many of our customers have applications built on a one-to-many messaging technology called Multicast. Almost all cloud providers have disabled multicast traffic on their networks because it's considered too "chatty", which presents a challenge to organisations adopting cloud services.

For clustering, or messaging functions like those commonly used in the financial services industry, Enclave provides an overlay network which sits on top of the cloud vendor's network, bringing the capability to send and receive multicast support to cloud vendor networks.

Customers use Enclave to gain the benefits, and competitive advantage of deploying to cloud, without having to re-design their applications first.

On when you need it.

With high flexibility, convenience and security, there are few limitations on how, or where Enclave can be applied. Many scenarios and use-cases benefit from Enclave's convenience, minimal setup time and security capabilities, and what follows is a growing list of customer use-cases.

1. Ad-hoc (short-term connectivity)

- Quickly handle sensitive file transfers.
- Secure remote administration and access.
- Secure remote support and assistance.
- Transporting forensic images for safe analysis.
- Secure transfer of PII data.
- Transient, short term or incidental connectivity.
- Safely expose internal systems to the outside world under strict time constraints (technical pre-sales team needs access to internal system to run a demo from a hotel network).

2. Per-project (medium-term)

- Quickly provision disaster recovery networks.
- On-premise migration to, or from cloud.
- Safely connect partner and supplier networks.
- Isolated / special purpose environments.
- Cross-organizational teams, deal rooms, troubleshooting, audits, reports.
- Secure offshore delivery services, transport source code and application secrets.
- Environments for testing, pilots, sandbox activities which don't threaten core systems.

3. Lifetime (long-term)

- Enable Multicast support in cloud networks.
- Additional security between WAN locations.
- Reducing the organisation's attack surface area.
- Limiting exposure of critical production assets.
- Cloud vendor, location and provider agility.
- Ship transaction logs offsite (or on-site).
- Data backup, restore and archiving.
- Application specific N-Tier networks.
- Distributed microservice service connectivity.
- Trust bootstrapping and secret distribution.
- Cross-site secure message bus.
- Remote access & administration to IoT sensors.
- Rapid access & transport level security for APIs.
- Safely exposing non-public web applications.
- Networks with no static locations (i.e. start-ups).
- Building access and control networks (BACnet).
- High availability backplane networks for distributed systems, or clustered services.

Westgate

CYBER SECURITY

Connect with us

Whether you're a lawyer that has to work with other lawyers, a financial institution that has to work with other financial institutions or a law enforcement agency that has to work with other law enforcement agencies, if you found this paper interesting and would like to learn more, or arrange a technology demonstration please contact us.

Email: founders@westgatecyber.com

Telephone: +44 (0)1633 215 545

Website: https://westgatecyber.com

Company: Registered in England & Wales — No. 08181759

Address: Westgate Cyber Security Ltd
Springboard Business Innovation Centre
Llantarnum Industrial Park
Cwmbran
NP44 3AW
UK