Stealth technology for your network.

The race to stay one step ahead of cyber threats costs organisations billions globally. What if you could take yourself out of that race? What if you could reduce your costs, and 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. By cloaking your networks and the applications living inside, Enclave renders 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 cybersecurity target landscape — for good.

Protect vulnerable systems

Attackers are constantly aiming 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, terminate.

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 minutes. Use Enclave for hours, days, or years to exchange sensitive data in private, invisible networks. Then, when your project ends, the network is terminated.

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 allowing you to focus on the task, not the network.

1

Deploy stealth networks

Using outbound 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 and systems get mutual authentication, end-to-end encryption, and perfect forward secrecy for safe connectivity.

Security

4

Deploy, work, terminate.

Enclave provides "on-when-you-need-it" networks that are task, or project specific. 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

No need to change your network, or infrastructure

Enclave works without changes to your underlying network and infrastructure, so you get secure connectivity, without the inconvenience, setup time, or risks of needing to plan, schedule, apply, manage and potentially later undo configuration changes.

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 internal and legacy systems, particularly if they are unpatched, or unpatchable.
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.

Preserving data security and remaining compliant while maintaining legacy systems presents a monetary and reputational risk for organisations, with many choosing to mitigate, rather than upgrade — leaving the boardroom 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 organisational 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 terminated — in a 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 set up 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 that device or system connects to the Internet from, the Enclave address never changes. This gives engineers a constant, and predictable way to address their entire IT estate, no matter where 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 a lifetime-fixed address. Give your infrastructure protection from IP address conflicts, regardless of the underlying network, and future providers you might migrate, move, or expand into.

Enclave also allows you to avoid the complexity and limitations of VPCs and VNETs. Connect 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 avoids Cloud vendor lock-in at the network level and 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.

01

AD-HOC NETWORKS

SHORT-TERM CONNECTIVITY

Rapidly build secure networks for transient or incidental connectivity.

- Quickly handle sensitive file and data transfers.
- Secure administration and remote access to infrastructure.
- Safely isolate special purpose systems and environments.
- Share remote access to internal systems under strict time constraints.
- Enable rapid responder teams to access critical systems and locations.
- Transporting forensic system images for safe off-site analysis.

02

PER-PROJECT NETWORKS

MEDIUM-TERM CONNECTIVITY

Remove the connectivity roadblocks to get projects moving quickly.

- Effortlessly build business continuity and disaster recovery networks.
- Migrate systems and data to, from, or between on-premise and cloud.
- Setup cross-organizational teams for deal rooms, audits, reports etc.
- Safely transport and deploy source code and application secrets.
- Conduct testing, pilots, and innovation without threatening core systems.
- Polling and remote access to IoT sensors deployed on 3rd party networks.

03

LIFETIME NETWORKS

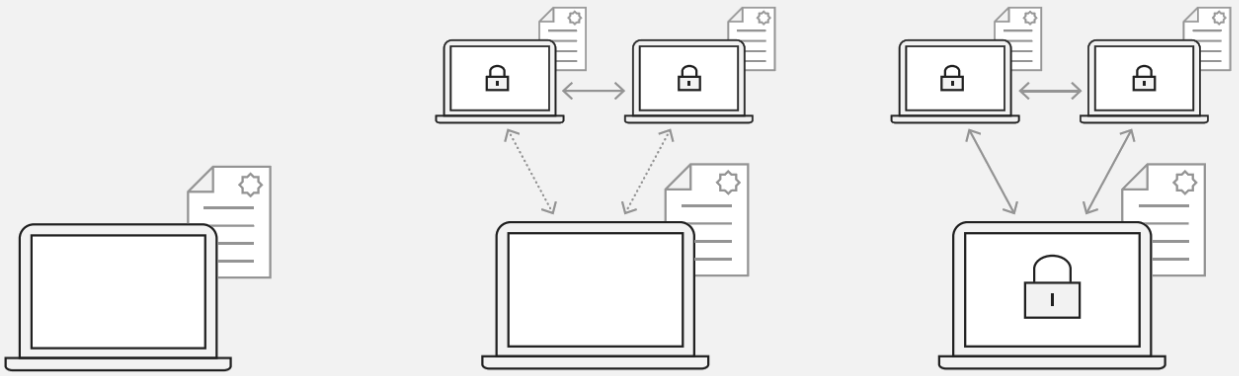
LONG-TERM CONNECTIVITY

Use Enclave improve productivity and reduce your vulnerability to attack.

- Safely connect the WAN, eliminating costly MPLS and complex VPNs.
- Enable multicast in cloud to run legacy applications without rebuilding.
- Limit the exposure of critical production assets and reduce maintenance.
- Backplane connectivity for high-availability systems in different regions.
- Compliment OAUTH to enable rapid and secure access to private APIs.
- Connect mobile systems together, without pre-known static IP addresses.

Establishing an Enclave

Users exchange certificate names, and get private, secure networks.



1 Client certificate issued

Westgate Cyber Security has developed a novel twist on standard public key exchange, allowing client certificates to be issued in real-time to end users and systems for an unbelievably simple user experience.

2 Mutual authentication

Cooperating parties exchange the common names of their client certificates. This ensures all parties must mutually authenticate one another before any communication can take place.

3 Secure enclave established

Once authenticated, our peer-to-peer technology establishes direct connections, exchanges ephemeral session keys and stands up instantly available virtual private networks between connecting parties.

Relationships and trust

When two strangers try to connect online, a Certificate Authority can help to establish trust. This is useful if you don't know who you're connecting to; such as entering a domain name for a secure website. But what if Alice has a real-world connection to Bob because they are both senior Lawyers working in different firms, for example?

When Alice knows Bob, she doesn't need the Authority to validate his identity, which just adds time, costs and complexity.

All she needs is a way to find, and connect to him online, and reliably get his public key. The trouble is Bob's IP address changes regularly because he works globally and public keys are long and difficult to share.

This is where Enclave comes in. By elegantly solving these two problems, Enclave delivers encrypted and invisible peer to peer connections. Almost as if a dedicated network cable runs directly between Alice and Bob's devices – without needing old technology like a VPN server in the middle.

Short, sharable certificate names

Public keys are long numbers, which make them difficult to share. But exchanging them online is dangerous without secure connections in place to ensure they're not tampered with by malicious parties.

Example 4096 bit RSA public key

```
30 82 02 0a 02 82 02 01 00 f3 5d fa 80 67
d4 5a a7 a9 0c 2c 90 20 d0 35 08 3c 75 84
cd b7 07 89 9c 89 da de ce c3 60 fa 91 68
5a 9e 94 71 29 18 76 7c c2 e0 c8 25 76 94
0e 58 fa 04 34 36 e6 df af f7 80 ba e9 58
0b 2b 93 e5 9d 05 e3 77 22 91 f7 34 64 3c
22 91 1d 5e e1 09 90 bc 14 fe fc 75 58 19
e1 79 b7 07 92 a3 ae 88 59 08 d8 9f 07 ca
03 58 fc 68 29 6d 32 d7 d2 a8 cb 4b fc e1
```

Public keys form part of a digital certificate, issued by Certificate Authorities. Among other things, a digital certificate also contains a name. The name is normally strongly tied to a recognisable real-world entity, like a domain name.

When a user types in a domain name, if they reach the correct server, they're sent a certificate with a name that matches the typed address, which includes a public key. This combination of matching name, and public key is what enables trust and encryption.

However, Alice and Bob aren't running Internet-facing, public services on their computers, and don't have fixed, or recognisable domain names, so the current certificate system isn't very useful to them.

Enclave is different. In an Enclave network, certificates have names that are not connected to the owner's identity. Instead, certificate names are arbitrary – like telephone numbers, or car registration number plates – but are selected to be short, human friendly, and easy to share, much like a domain name.

Using Enclave, friends, co-workers, system administrators and colleagues from different organisations exchange certificate names, already knowing their partner's identity.

For example, Alice easily shares her Enclave certificate name, GN63 with Bob, and in return, Bob tells Alice that his certificate name is HP8K. This is all they need to do in order to get a secure connection setup between them.

Example Enclave certificate names:

GN63 (Alice)

HP8K (Bob)

When Alice tells Enclave that she wants to talk to Bob and that the name on his certificate is HP8K, Enclave automatically connects to the Westgate cloud service and logs a request to be told if HP8K expresses an interest in communicating back to Alice.

Nothing happens until Bob makes a similar request – that he wants to talk to Alice, and he knows that the name on her certificate is GN63.

Since both Alice and Bob connected to the Westgate cloud service, it knows where they both are on the Internet, and seeing mutual intent between GN63 (Alice) and HP8K (Bob), it makes an introduction before stepping away from the communication.

Now both parties know where to find each other, they initiate outbound only connections to one another using UDP and TCP hole punching, having already undergone mutual authentication before being introduced.

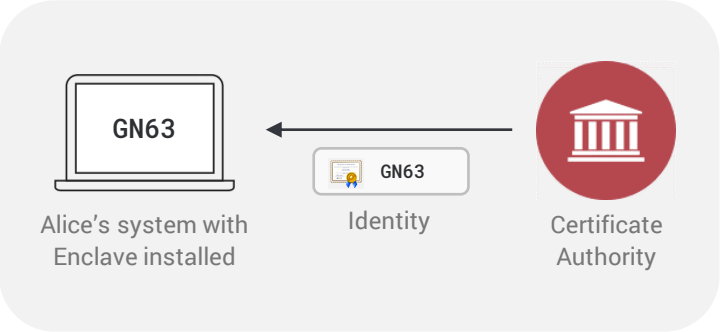
Once directly connected, Bob and Alice exchange certificates to verify the connection, and generate encryption keys for that session. When the session is terminated or expires, so are the encryption keys.

Three-step setup

Issue certificates — Exchange names — Connect directly.

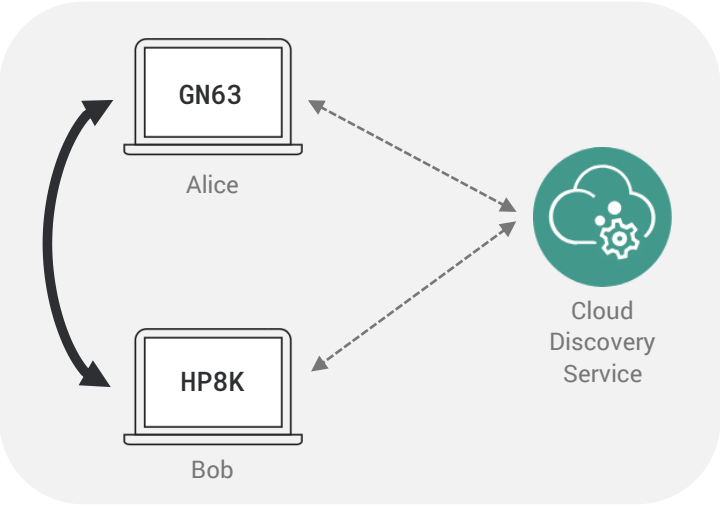
1. An system running Enclave generates a private key locally and sends a certificate signing request (CSR) to the Westgate Cyber Security Certificate Authority.

   The Authority issues a certificate back to that system with a name of its choosing. Enclave now has an identity (a private key, and a certificate).



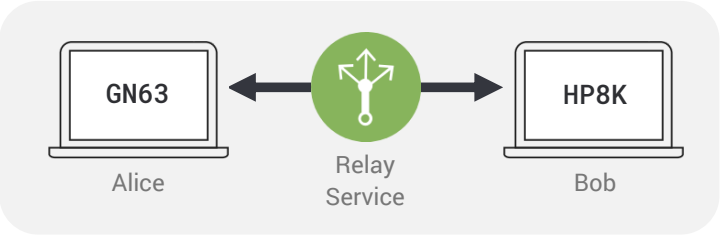
2. On Alice's computer, Enclave makes a connection to the Westgate cloud discovery service and requests a connection to Bob, supplying his certificate name, HP8K. The request is accepted, but no connection is made.

   Bob's computer also makes a connection to the Westgate cloud discovery service, requesting a connection to Alice by providing her certificate name, GN63. Now the discovery service can see mutual intent to communicate between Alice and Bob, it introduces them to each other so they can try and establish a direct, invisible and encrypted connection. Once Alice and Bob are connected, they exchange certificates and perform a key exchange to secure the session. *



* As each party's public key is digitally signed into their certificate, the certificate exchange shares public keys, which are then used to perform a key exchange, and agree a shared secret used to encrypt any data they exchange

3. If a direct connection between Alice and Bob was not possible, the discovery service selects a relay service, and builds an alternative pathway that both parties can use to reach to one another. Relay services only ever see encrypted traffic, and never have access to, or knowledge of encryption keys.



Westgate

CYBER SECURITY

Connect with us

Enclave makes secure communication easy and turns your network into a competitive advantage. It can reduce the time, cost and inertia of building secure networks whilst increasing your organisation's agility, productivity, and capacity to innovate.

At the moment, complex and insecure networks are often a major barrier to getting things done — and it doesn't have to be like that. 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