SECURING THE CONNECTED FIN-TECH

INTRODUCTION

Today's Fin-tech operations face increasing risk as they become more connected. Yet, connectivity is essential to improving productivity, customer satisfaction, efficiency, and ultimately, profitability.

Typical operations are comprised of disparate, siloed environments including building automation systems, internal and external applications, and ATMs. These are often designed with multiple vendors utilizing both cutting edge and legacy technology. In addition, Fin-tech operations have enterprise management systems for many sensitive areas of business including, personnel, finance, market analysis, pricing, and customer data,.

Increasingly, Fin-tech operations are being targeted by nation states, competition, hacktivists, organized crime, and opportunistic malicious software.

CRITICAL THREATS

- **Down-time** - System, equipment, or communications failure can cause significant losses while the operations must wait for vendors to arrive, assess the problem and provide a solution.
- **Intellectual Property** - The loss of market analysis, financial records, pricing, and sensitive financial methods can lead to losses in customers and ultimately profits.
- **Security** - Building automation, ATM (often older) systems and partner applications can pose significant risk to other financial systems and valuable property if hacked.
- **Market / Brand** - Modern supply chains have little room for error, thus placing signifiant pressure on Fin-tech operations to keep the data secure, operations efficient, and brand clean.

SOLUTION

Blacksands offers dramatic improvement to data accessibility, security, efficiency, policy, governance, management of critical operations devices, systems, and applications. Blacksands' utilizes existing protocols to connect both current and legacy systems in physical and cloud environments. Blacksands patent-pending Separation of Powers connectivity architecture can provide a significant advantage to modern mining operations.

Dynamically Brokered Encrypted Point-to-Point Connections:

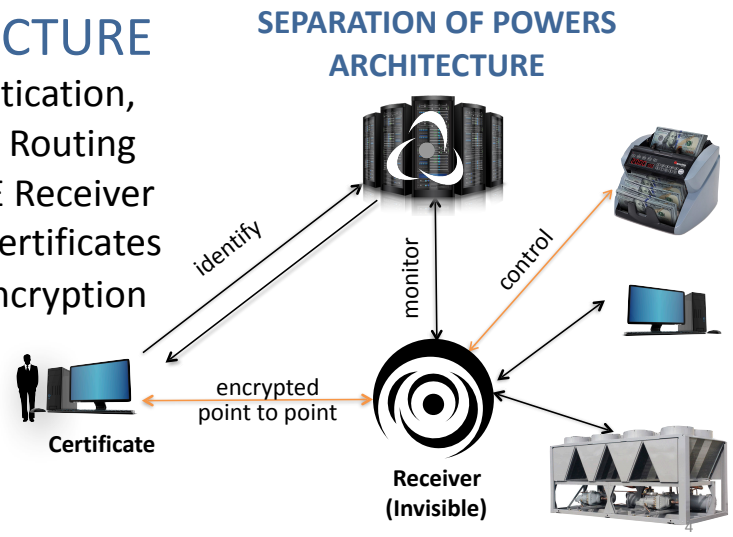
- Blacksands creates invisible private networks providing a drastically reduced threat vector for critical fin-tech infrastructure
- Blacksands dynamic Authentication, Authorization, and Routing allow real-time session control and network architecture
- Blacksands dynamically creates and manages unique, point-to-point, encrypted connections without exposing anything else on the host network, controlling the traffic from OSI layers 3-7
- Blacksands can be combined with existing tools to form a cohesive and comprehensive tactical network defense plan

SOLUTION

Secure Connection as a Service

INFRASTRUCTURE

- Dynamic Authentication, Authorization, & Routing
- Virtual INVISIBLE Receiver
- Unique Device Certificates
- Point-To-Point Encryption



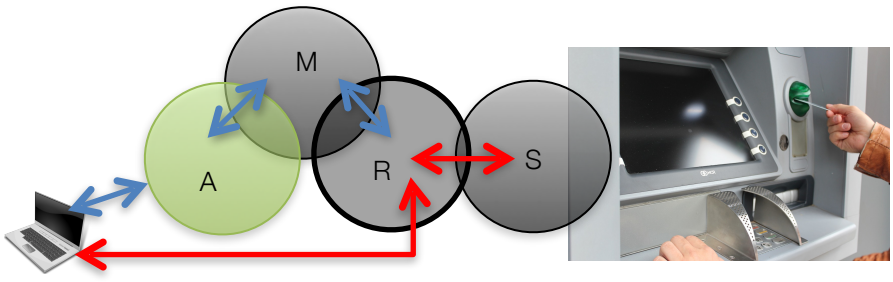
Blacksands provides Access Management, Networking, and Auditing in a single technology with a user friendly interface. The simple, secure and scalable, point-to-point, encrypted, micro-threaded connections are offered under a SaaS business model, called “Secure Connection as a Service” (SCaaS). It requires minimal training and labor to deploy and operate. The business case for installation and operation is very favorable based on much lower installation, operation and support costs, improved customer service and speed to market. Blacksands' SCaaS significantly reduces cybersecurity risk and greatly improves compliance, policy, deployment, and governance.

Blacksands is OS and device agnostic, working with and on existing TCP/IP network infrastructure. The deployment can occur in Blacksands’ cloud, an organization’s private cloud or entirely on premise (virtual or hardware). The Receiver is deployed as software in a virtual environment or an embedded enterprise hardware device. User computing devices do not require installation of client software.

SOLUTION

Blacksands, patent pending, ‘Separation of Powers’ architecture includes:

1. Authorizer - forward facing identification system
2. Manager - invisible, external cloud management system
3. Receiver - invisible, software/hardware edge device and gateway
4. Unique industry standard certificates for every user device



DIFFERENTIATORS

- Invisible Edge Receiver (unable to discover or fingerprint - premium security)
- Granular Knowledge & Control of Every Connection (Every Packet)
- Dynamic External Authentication, Authorization & Routing (Immediate, user friendly, architecture modification)
- Point-to-Point Encrypted Connections (TLS - NOT VPN or SDN - never exposes whole network)
- No Agent or Client (OS and Device Agnostic)

INVISIBLE EDGE

Blacksands' edge, Receiver (R), holds no static information (i.e. routing tables, revocation lists, rules, or signatures). It does not initiate any sessions and does not allow internally initiated sessions. When scanned from non-authenticated IP addresses, the Receiver does not respond, and is, thus, unable to be fingerprinted or engaged in a session. The resulting lack of response creates both edge and protected service invisibility. Invisibility is maintained for illegitimate entities, even when legitimate users are accessing protected services.

VALUE: Drastically reduced threat vector

GRANULAR KNOWLEDGE AND CONTROL OF EVERY CONNECTION

Blacksands controls every connection in real-time. The control begins at OSI layer 3 (network layer) and escalates through layer 7 (application layer). Every packet is identified and controlled without engaging in packet inspection. Blacksands' utilizes cutting edge certificate based authentication primarily for identification. All edge communication, routing, and backend connections are dynamically identified and controlled by the Blacksands Manager (M). Blacksands maintains granular knowledge and control of *Who* is connected, *What* services are connected, *When* connections occur, and *Where* connections originate.

VALUE: Unprecedented control and audit

DYNAMIC EXTERNAL AUTHENTICATION, AUTHORIZATION, AND ROUTING

User devices (e.g. PC, Tablet, Application, IoT Device), Blacksands' Authorizers, and Receivers are dynamically populated with appropriate connection information after User identification is confirmed. The simple management interface allows for immediate adjustments in User access and Service architecture. Blacksands' secure, high-speed, redundant bus management communication provides unlimited scalability and flexibility for global deployments or dynamic supply chain connectivity.

VALUE: Vast scalability and unparalleled flexibility

POINT-TO-POINT ENCRYPTED CONNECTIONS

Every connection is made from a User device to a particular Service within the secured network without exposing any other active Service on the given network. Blacksands utilizes SNI routing to accommodate global internet networking flexibility. Each Service is provided a unique, obfuscated FQDN, which is only accessible through he Blacksands SCaaS. Internally, Blacksands connects Users to specific ports identified by internal IP or DNS. Blacksands does NOT route traffic through its Authorizers or Cloud Management system. All User/Service connections are routed directly from the User device through the Receiver to the pre-authorized Service. Blacksands utilizes Diffie-Hellmen Elliptic Curve with perfect forward security and supports TLS 1.1 - 3.0. Blacksands is also a privately held, DV (Domain Validation) Class, Certificate Authority.

VALUE: Dramatically improved control and reduced internal network exposure

NO AGENT OR CLIENT

Blacksands does not require agent or client software to be installed and supported on User devices. The User installs a unique, industry standard, certificate in the native OS certificate repository (e.g. PC Certificate Manager). The User can then access the Blacksands' protected services through an industry standard browser. For application to application connectivity, Blacksands can provide a simple API that establishes the appropriate secure connections.

VALUE: Significantly reduced deployment, support, management, and development costs

SUMMARY

Blacksands' technology is currently deployed in global manufacturing distributed supply chain environments and Critical Infrastructure. Blacksands is also expanding into the Fin-tech, Healthcare and other marketplaces.

The Blacksands unique, 'Separation of Powers' architecture, provides unparalleled security, scalability, and flexibility, within a simple, user friendly interface.