SOLVING SECURITY FOR TODAY'S AGILE PERIMETER: A SOFTWARE DEFINED PERIMETER APPROACH

EXECUTIVE SUMMARY

With few exceptions, organizations enable direct access to their sensitive systems over the internet. It's become acceptable, even necessary and unavoidable for productivity and collaboration both within organizations and across organizations, regardless of their size. But as the world has becomes more complex and interconnected, corporate networks and assets have become increasingly vulnerable, increasingly falling victim to cyberattacks.

Industry spending to secure networks and protect informational and intellectual assets continues to grow, yet breaches and breach-related losses continue to outpace investments. The World Economic Forum estimated the cost of cybercrime to the global 2016 economy at $445 billion USD[1].

The root of the problem goes back to providing direct access to sensitive systems over the internet. Exposing network services and accepting anonymous or unsolicited connections poses too much risk.

Existing cyber solutions are not doing the job, but that should be no surprise. Gartner recently stated, "DMZs and legacy VPNs were designed for the networks of the 1990s and have become obsolete." [2] Forrester agrees, stating, "legacy perimeter-based security models are ineffective against attacks." Even supplementing these preventative tools with detective ones has proven insufficient to protect organizations from today's sophisticated cyberattacks.

The root of the problem goes back to providing direct access to sensitive systems over the internet. Exposing network services and accepting anonymous or unsolicited connections poses too much risk.

Software Defined Perimeter technology provides a solution for today's agile perimeter. A Software Defined Perimeter isolates network services and resources from the internet by creating individual tunnels that secure the entire path from user to application, endpoint to service. Software Defined Perimeters allow access only after successful authentication, and restrict connections to only those services that have been pre-authorized. Network assets are hidden from unauthenticated users. Software Defined Perimeters protect organizations by substantially lowering the attack surface.

SAIFE has extended the philosophy of a Software Defined Perimeter to create a solution for today's agile perimeter that virtually eliminates the attack surface for untrusted networks, reducing an organization's financial exposure by substantially reducing its risk of a breach.

...

[1] World Economic Forum, *The Global Risks Report 2016, 11th edition*, 14 January 2016 82.

[2] Gartner, *It's Time to Isolate Your Services From the Internet Cesspool*, Steve Riley, Neil MacDonald, Greg Young, 30 September 2016.

INTRODUCTION

Organizations continue to be compromised and breached at an alarming rate. 2016 has been referred to as the year of the mega breach[3]. According to the IBM X-Force Threat Intelligence Index (2017), more than 4 billion records were leaked in 2016; roughly two times as many from 2014 and 2015 combined. Attacks of varying types –- hacks, compromises, and breaches have become an increasingly common reality in our world as has the wide and diverse adversarial pool behind them. Verizon, in its 2017 Data Breach Investigations Report (DBIR)[4], reported that within the 21 industry verticals they assessed, there were 42,068 confirmed security incidents. In their 2016 Global Risks Report 11th Edition, the World Economic Forum reported that cybercrime could cost the 2016 global economy as much as $445 billion USD[5]. In perspective, that amount is greater than the market caps of Amazon.com ($429 billion USD), Facebook, Inc. ($420 billion USD), Exxon Mobil Corporation ($340 billion USD), and IBM Corporation ($146 billion USD).

Clearly, existing cyber solutions are not doing the job. Continuing to invest in those solutions with the expectation of a better outcome, to paraphrase Einstein, is insanity.

In parallel, industry spending on cybersecurity continues to grow. In its March 2017 update to the Worldwide Semiannual Security Spending Guide, International Data Corporation (IDC) predicted that worldwide spending on cybersecurity in 2017 will reach $81.7 billion USD, an 8.2% increase over 2016[6]. IDC further expects the rate of cybersecurity-related spending to accelerate over the next several years, reaching $105 billion USD in 2020. Despite increased spending on cybersecurity, breaches and breach-related losses continue to outpace investments.

Clearly, existing cyber solutions are not doing the job. Continuing to invest in those solutions with the expectation of a better outcome, to paraphrase Einstein, is insanity. The question is, what is the right new approach? Answering that question starts with understanding why traditional solutions are no longer working.

•••

[3] IBM, *IBM X-Force Threat Intelligence Index*, Security Intelligence Staff, March 2017.

[4] Verizon, *2017 Data Breach Investigations Report*, 27 April 2017, 9.

[5] World Economic Forum, *The Global Risks Report 2016, 11th edition*, 14 January 2016, 82.

[6] International Data Corporation (IDC), *Worldwide Spending on Security Technology Forecast to Reach $81.7 Billion In 2017, According To New IDC Spending Guide.* 2017. Web. 26 May 2017.

THE PERIMETER MOVED, YOUR DEFENSES DID NOT

Network infrastructure has evolved in ways the earliest pioneers of inter-networking could only have dreamed of. From safe and secure behind the locked door of the data center, the network escaped. Local Area Networks (LANs) emerged in concert with the 'PC Revolution' of the 1980s, making it possible for diverse groups of users in a limited geographic area to share data and messages, as well as access shared resources. Wide Area Networks (WANs) allowed organizations to interconnect LANs, enabling them to become interconnected across broad geographies. Ultimately, switched inter-networks not only enabled global data and resource sharing and message exchange within the organization, but also provided access to an organization's external resources, to known third parties, and often to unknown parties and organizations.

This is the world traditional perimeter defenses are meant to secure. While those network defense tools have evolved substantially to respond to changes in the threat landscape, the network they try to protect looks a lot like the network of the late 1990s and early 2000s.

Firewalls were among the earliest defense tools to protect an organization's network from external threats. Firewalls controlled outside access to the network through rudimentary packet-filtering — basic sets of rules that looked at simple attributes like port number and destination address. Firewalls were used to segment connections to remote WAN sites, extranets, and the internet. Early firewalls were stateless, having no intelligence to monitor data flows, making them vulnerable to spoofing. These were replaced by stateful firewalls that monitored traffic flows between devices communicating through the firewall, verifying that packets being sent and received were coming from the original devices in the existing connection. Web gateways added URL filtering, blocking access to websites appearing on predefined blacklists. Current generation (called next-generation) firewalls evolved to combine packet filtering (levels 3 and 4), with deep packet inspection, IPS, and awareness of users and applications — but still reside at the perimeter within the internal network.

The flaw in developing ever more sophisticated defense tools for the perimeter is simple: The perimeter isn't where you left it, it moved!

The flaw in developing ever more sophisticated defense tools for the perimeter is simple: The perimeter isn't where you left it, it moved! Cloud applications, mobile device use, BYOD, virtualization, third-party (consultants, vendors, and trading partners) access, and IoT devices have redefined the perimeter. Today, the perimeter is wherever your intended users (and things) are on whichever internet connected device they're using.

Securing today's dynamic perimeter demands a different approach to providing anywhere, anytime, any means access.

From a risk perspective, the attack surface has never been as large, as exposed, or as porous. Gartner reports that attackers will target any exposed surface and that most attacks originate from the public internet. Gartner concludes, "Network designs that expose services and accept unsolicited connections present too much risk," and suggests that such designs are now obsolete. Securing today's dynamic perimeter demands a different approach to providing anywhere, anytime, any means access. Among Gartner's recommendations is to favor "isolation technologies capable of precise, context-based, application-level access only after successful authentication."

Conventional perimeter security solutions leave networks vulnerable to:

Port Attacks
Organizations need to expose sensitive network services on the internet to get business done. They require open inbound ports on firewalls. They rely on imperfect protocols, imperfect software implementations, and imperfect configurations of security services, creating a virtual open door and welcome mat to would-be threat actors.

Stolen Credentials
Network systems rely on the secrecy of the credentials of its users to keep sensitive data protected. Once a credential is stolen that user's identity can be used to gain unauthorized access from anywhere in the world the network system is accessible.

Man in the Middle Attacks
It is not possible to trust all the network equipment that is outside of our control yet is between us and the services we need to access. Domain names and IP addresses are not enough to know if something is trustworthy, and mutually-authenticated public key infrastructure requires extensive overhead to deploy and maintain.

Distributed Denial of Service Attacks
Denial of service attacks are easier to deploy than ever and are escalating in magnitude and complexity, presenting challenges to mitigation providers. The price of mitigation service contracts continues to rise.

Lateral Movement (Advanced Persistent Threats)
Once a credential has been used to gain unauthorized access to a network, a threat actor can lurk, continuing to escalate their permissions and access additional systems and data on the internal network. Often systems that were thought to be isolated are not, and their data can be exposed.

A SOLUTION FOR TODAY'S AGILE PERIMETER

Software Defined Perimeters (SDPs) overcome the limitations of conventional security tools and mitigate the network vulnerabilities associated with them by creating dynamic, individual micro-perimeters for each user, inside of which the privacy and integrity of all traffic is assured. Endpoints attempting to access a given resource are authenticated and authorized before being connected to the infrastructure and any resource within it.

Authorized users see only the services and resources they're entitled to access. Everything else on the network is invisible to them, precluding access to unauthorized services or lateral movement. This is an important distinction from conventional tools designed to protect against external attacks and unauthorized access. Those tools are ineffective if an intrusion compromises elements inside the network perimeter. Instead of trusting access from inside the security perimeter and not trusting external access by default, the default for a Software Defined Perimeter is to trust no one, and only allow access on a case-by-case basis.

A Software Defined Perimeter is a secure enclave of logically defined network-connected participants where access is restricted via a trust broker to the specified participants of the enclave, hiding them from public discovery and public visibility, thus reducing the attack surface.

A second important distinction is that conventional secure connections follow a "connect then authenticate" paradigm. A Software Defined Perimeter takes an opposite approach: "authenticate then connect." Unauthorized, unauthenticated users including would-be attackers are unable to connect because the SDP-protected infrastructure is virtually invisible to them. They cannot scan or attack services on the network because they're inaccessible, making them unaware of their very existence! By hiding network resources from unauthorized or unauthenticated users, the attack surface is dramatically reduced.

Simply put, a Software Defined Perimeter is a secure enclave of logically defined network-connected participants where access is restricted via a trust broker to the specified participants of the enclave, hiding them from public discovery and public visibility, thus reducing the attack surface.

A Software Defined Perimeter is built upon the following key principles:

» **Access control and data transmission are managed independently**; the control plane and the data plane are separate.

» **Logical and physical components are separated.** Endpoints are connected via secure virtual tunnels through internal or external networks using a dynamic security overlay network that establishes logical connections over a physical network. This enables secure routing across any network topology.

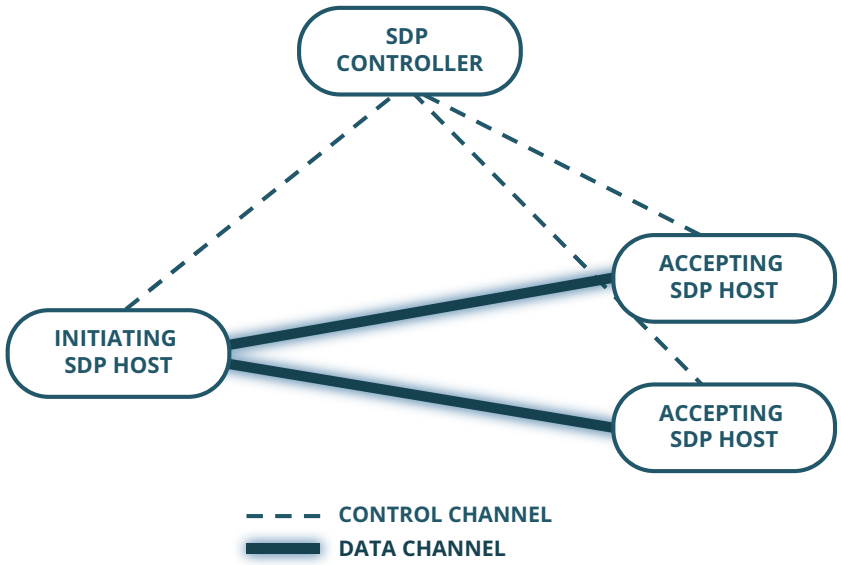
» **Endpoints are authenticated.** Only endpoints that have been authorized can communicate.

» **Endpoints are contextually validated** against a set of policies to verify security compliance with security constraints, which may include geo-location, time of day, or health of the endpoint.

HOW A SOFTWARE DEFINED PERIMETER WORKS

A key component of a Software Defined Perimeter (SDP) is the SDP Controller, which serves as the trust broker between the client and backend security controls (i.e., Certificate Authority and Identity Provider). The SDP Controller is the authentication point within the Software Defined Perimeter. Management services are separated from the SDP Controller and accessed via a graphical management console or dashboard. A single Software Defined Perimeter may involve multiple, geographically dispersed, inter-networked SDP Controllers which automatically federate policy and other key information.

Figure 1: Software Defined Perimeter Architecture



The interface to the SDP Controller for both endpoints and network services can either initiate or accept a connection. In the case of an endpoint, the interface is a client application that resides on the endpoint. For network services, a gateway, commonly deployed as a virtual server, provides the interface. The SDP Controller performs device verification, user identity verification, and policy enforcement, and maintains the list of authorized connections. It uses the externally provided Identity and Entitlement Management service to ensure the mutually-authenticated connection allows only pre-authorized connections. Once the identity of the initiating party has been verified and its pre-authorized connections determined, its certificate is received by the accepting party and the SDP Controller tells the

SDP Gateway to open a pinhole in its firewall to allow connection between the endpoint and the network service behind the firewall. In the case where a SDP Gateway serves as the interface to the SDP Controller for multiple services or multiple VLANs, it enforces connection to only those services for which the endpoint is pre-authorized.

Remote user access is the most obvious use case for a Software Defined Perimeter. In this case, the Software Defined Perimeter can be deployed client to server, where both the endpoint and the network service directly connect with the SDP Controller or client to the SDP Gateway, where the SDP Gateway arbitrates the connections between the client and protected services.

The Software Defined Perimeter architecture uniquely enforces security through:

01. **INFORMATION HIDING.** The private IP address and port number of the protected services are never exposed. Only the IP address of the external firewall and the NATed port being used is visible to the outside world and the clients connecting to the protected services. Only authenticated users are able to connect to the protected service interface.

02. **PRE-AUTHENTICATION.** User identity and device fingerprint are verified before connectivity is granted.

03. **PRE-AUTHORIZATION.** Allowed connections are established with the SDP Controller per connection, enforcing the pre-authorized entitlements defined in the externally provided Identity and Entitlement Management service. Connection is only allowed after authentication and authorization have been established.

04. **APPLICATION LAYER ACCESS.** Only application level access is granted, precluding lateral movement to other applications or services from compromised devices.

05. **EXTENSIBILITY.** Software Defined Perimeters can be integrated with existing security policies and tools.

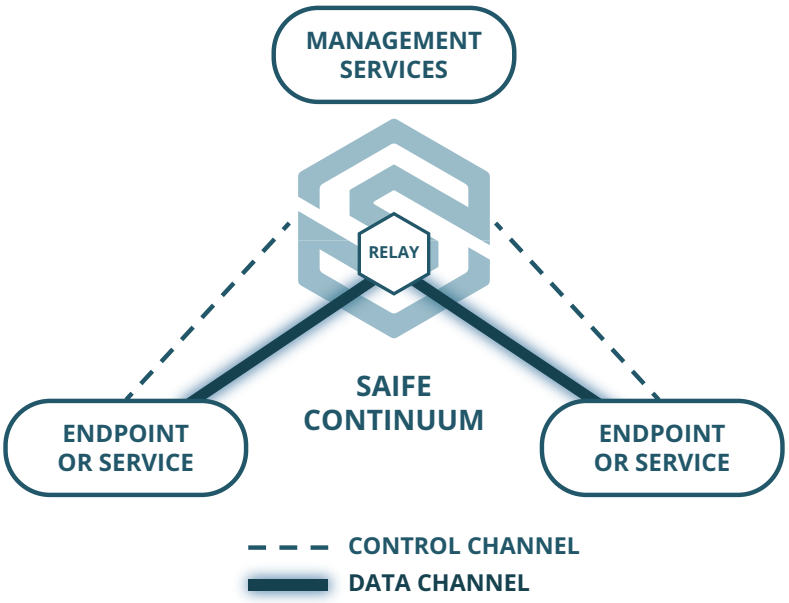
THE SAIFE SOLUTION

A fundamental tenet of a Software Defined Perimeter is isolation of network services and resources from open internet connections. Isolation eliminates certain attack vectors and reduces the attack surface for others. But while Software Defined Perimeters materially reduce an organization's risk of a breach, those that strictly adhere to the design prescribed by the Cloud Security Alliance (CSA) leave organizations vulnerable in a number of meaningful ways.

SAIFE has embraced and extended the philosophy of a Software Defined Perimeter (SDP) to create a solution that virtually eliminates the remaining attack surface and removes residual vulnerabilities.

A fundamental difference in the SAIFE solution is the use of certificate-based rather than IP-based routing. While an SDP Gateway hides the identity of the specific network service an endpoint is attempting to connect to, an analysis of network traffic will reveal the origin IP address and the destination IP address of the SDP Gateway. While traffic in the SDP solution is encrypted, the association of the endpoint or remote user with the destination is exposed. A threat actor can determine that a specific, identifiable remote user is connected to an unknown service within a specific identifiable organization. Furthermore, to enable the connection, the SDP Controller opens a pinhole in the firewall, one pinhole for every connection. Once opened, these pinholes can be detected and exploited to gain unauthorized access.

Figure 2: SAIFE's Approach to Software Defined Perimeters



By contrast, with SAIFE, all network connections terminate within the SAIFE Continuum, a global, cloud-based, resilient overlay network that provides secure routing over the internet, while the security of your data remains end-to-end. SAIFE Continuum facilitates this by dynamically assigning a relay server as a rendezvous point for endpoints to directly communicate with one another even though there is no routable network path between them and without knowing the public or private IP address of the other endpoint. Connections are invisible and traffic is undecipherable. Traffic can't be analyzed; no patterns can be inferred.

SAIFE has extended the SDP philosophy to create a solution for today's agile perimeter that virtually eliminates the attack surface for untrusted networks, reducing an organization's financial exposure by substantially reducing its risk of a breach.

The SAIFE solution also hides endpoints and services behind all-inbound-filtering firewalls, making them invisible on the internet. There are no open firewall pinholes to exploit — temporary or permanent. A would-be attacker is unable to scan or attack services on the network because they are unavailable to unauthenticated devices. The would-be attacker never knows those services exist.

Additionally, unlike the SDP Controller, which is a high-value target, SAIFE Continuum nodes are low-value targets. The SDP Controller in the CSA design maintains a directory of authorized connections to services, which contains the IP address for every endpoint in the directory. If the SDP Controller is compromised, endpoints can be exposed. If the SDP Controller is defeated as the consequence of a DDoS or other successful attack, accessibility to services is lost and the solution is potentially unable to automatically recover.

The SAIFE solution does not rely on a central directory. Rather, each individual endpoint has its entitlements shared in advance by storing the certificates of every other endpoint it is entitled to connect to and for every endpoint that is entitled to connect to it. Certificate stores on endpoints are automatically and immediately updated as new endpoints are provisioned or de-provisioned and entitlements revised. Consequently, there is no central directory bottleneck for requesting connections, and the SAIFE Continuum node stores no valuable data. Additionally, if one SAIFE Continuum node is attacked or lost to failure, endpoints can gracefully fail over to another SAIFE Continuum node, while new SAIFE Continuum nodes with new IP addresses are automatically spun up and securely made available to endpoints, making the SAIFE solution highly resilient.

The SAIFE solution also allows connections to be initiated from either side, enabling server-to-server, subnet-to-subnet, gateway-to-gateway, and cloud-to-cloud in addition to basic user-to-server connections. The SAIFE solution can be deployed in a public cloud, private cloud, or on premise. It fully automates key management, rather than leaving it as a user responsibility, which extends all the benefits of PKI without its overhead.

While the basic Software Defined Perimeter design materially improves an organization's security posture, SAIFE has extended the SDP philosophy to create a solution for today's agile perimeter that virtually eliminates the attack surface for untrusted networks, reducing an organization's financial exposure by substantially reducing its risk of a breach.

SUMMARY

Despite year-over-year increases in cybersecurity-related spending, breaches and their impact on the global economy continue to outpace the investment. Conventional perimeter-based security solutions that organizations continue to invest in are failing to protect them, but that should be no surprise.

The perimeter security defenses organizations depend on were designed for the networks of the 1990s, and those networks no longer exist. Simply put, legacy perimeter security defenses are obsolete — ineffective against today's more sophisticated attacks.

Software Defined Perimeter technology provides solutions for today's complex, interconnected world. A Software Defined Perimeter isolates network services from the internet, allowing access only after successful authentication, and restricting connections to only pre-authorized services. Network assets are hidden from unauthenticated users, leaving would-be attackers with no visible target. Software Defined Perimeters protect organizations by substantially reducing the attack surface.

SAIFE has extended the philosophy of a Software Defined Perimeter to create a solution for today's agile perimeter that virtually eliminates the attack surface for untrusted networks, reducing an organization's financial exposure by substantially reducing its risk of a breach.

ABOUT SAIFE

SAIFE eliminates the inherent vulnerabilities of traditional perimeter defenses that cost organizations hundreds of millions of dollars in breach-related losses every year. We are redefining perimeter security, enabling secure, trusted access to services and data sets over untrusted networks, while making those same services and data sets invisible to unauthorized users and would-be attackers. We've extended the concept of a Software Defined Perimeter to create the first solution that enables dynamic, agile, network overlay perimeters that are device, user, and application-centric, and which can span on premise, cloud, mobile devices, and applications. SAIFE protects customers by substantially lowering their attack surface and enables information sharing across untrusted networks to reduce third-party risk.

As the world gets more interconnected, it becomes smarter, more aware, more productive — and more vulnerable, our job is keeping it SAIFE.

Email: **info@SAIFE.io**
Phone: **+1 703.229.5924**
www.SAIFE.io

For more information:
Email: **info@SAIFE.io** | Phone: **+1 703.229.5924** | **www.SAIFE.io**

SAIFE

R170605