Access and Usage via Shield-SDA

White Paper

2017

SHIELD

You be the Hero… We've got your back

Introduction

Your organization is simply at risk of getting hacked. Current perimeter designs are becoming obsolete as the hackers continue to prey on businesses and their data every day. They target exposed endpoints, servers, applications, networks and databases hosted in the cloud. No matter how many layers of security we add, hackers have been able to get through. But what if we could hide our services from the Internet until it is absolutely necessary to allow someone to access the service?

This white paper introduces Shield-SDA (Software Defined Access), which uses Software-Defined Perimeter (SDP) methodology to help resolve cyberattacks and internal threats.

To start off, here's what a typical incursion looks like:

- **A hacker performs reconnaissance on a company.** This may be as simple as using a publicly-available search engine, such as Google, to map an organization's network diagram. This may allow them to uncover large stores of critical data.

- **The hacker steals the credentials for the data store**. They might accomplish this by scraping the information using a man-in-the-middle attack, or in in the worst-case scenario by simply inputting "admin" and "password1" into the form fields.

- **The hacker then uses a channel such as email, FTP, or cloud storage software** to move a copy of the contents of that data store into their possession.

Nearly all cyberattacks, whether they originate from outside an organization or from a malicious actor within its perimeter, follow this same pattern. Find the data, access the data, move the data. Find, access, move.

By the same token, most security and compliance efforts that have ever been attempted represent an approach that aims to disrupt this loop. Most fail. They fail despite cutting-edge behavioral detection and artificial intelligence. In 2015, 707.5 million records were stolen by malicious actors[1]. In 2016, 1.4 billion records were stolen, an 86% increase.[2] The numbers are on track to increase once again this year.

Even with the enforcement of heavy fines, the breadth and complexity of various regulations, and the technological advancement of antivirus, these solutions haven't prevented the number of breaches from rising every year since 2014. In failing, these solutions have added unnecessary complexity to organizations and networks. Given that compliance still can't be avoided, how can companies respond with a security solution that adequately defends their networks?

---

[1]Gemalto, "2015 Data Breach Statistics: The Good, the Bad, and the Ugly," March 2016
[2]Gemalto, "Findings from the 2016 Breach Level Index," January 2017

Shield-SDA Disrupts the Data Breach Decision Loop

From a security perspective, the Shield-SDA (Software Defined Access) solution is designed to disrupt a potential hacker's decision loop at every point in the process. It does so in a manner that simplifies networks overall, without forcing administrators to replace pre-existing solutions such as IDS/IPS, firewalls, SIEM, or antivirus. Instead, it improves these products by placing them in a simpler and more ordered network environment. At the same time, it thwarts hackers' attempts to infiltrate the network, and exfiltrate data.

This involves not just changing network architecture, but also changing the way that users become authorized to access applications. Shield understands the application access lifecycle as having three distinct phases:

Step 1
Adaptive Access to Services and Data

Shield's on-demand Software Defined Perimeter transparently grants access only to authorized users by separating the access layer from the authentication layer, and by segregating internal networks. It authenticates the user and verifies their device using fingerprinting prior to providing access.

Step 2
Controlling Data Usage

Once users have access to their applications and data, Shield-SDA ensures that they only use data in accordance with their respective usage and access policies. The data residing inside the organization or being transferred in and out of the organization will be completely controlled and protected from the inside out of the network - on premise or in the cloud.

Step 3
Report on Data Usage

Throughout the application access lifecycle, Shield-SDA monitors and audits all user actions for each access application or data repository. Granular real-time dashboards, historical reports and analysis on data usage and risks will ensure regulatory compliance and shortest time to breach discovery and remediation.

Shield-SDA authenticates users with a number of flexible methods, including multi-factor authentication. During the session, Shield-SDA monitors data usage and alerts or mitigates proscribed actions.

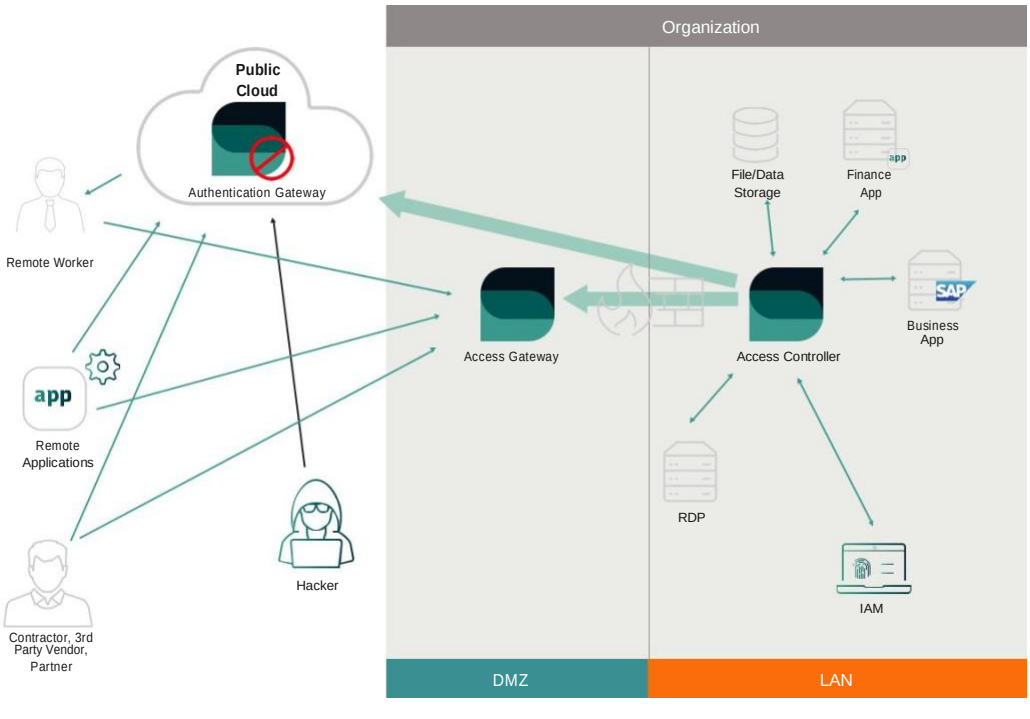
Hackers Can't Breach What They Can't See

SaaS applications and cloud storage have taken previously private assets and put them into areas where basic reconnaissance can detect them easily. Often, these tools will find cloud instances that are undefended by even the most basic security, such as the 7% of Amazon S3 servers that are unguarded by a requirement for a username or password[3].

Shield-SDA changes the game by making the corporate perimeter invisible from the perspective of the general-purpose internet, while access is provided without the need to install additional software, and without the need for a VPN. In addition, administrators can place their firewalls permanently into “deny all” mode. There are no longer any open ports and no exposed DMZ components. Meanwhile, pre-existing security and IAM solutions can be placed in line with all incoming and outgoing data.

A typical workflow looks like this:

- User logs into dedicated authentication portal published by the Authentication Gateway.
- The user enters the credentials into the portal, and the Controller then authenticates the user using methods chosen by the administrator: 3rd party IAM/IDP solutions, NoPost, POST based login, Microsoft Active Directory, SAML, OTP, etc.
- Once authenticated, the user selects the application which should be accessed.
- The Controller instructs the Access Gateway to allow access to the specific user to the specific application, and instructs the Authentication Gateway to redirect the user to the new published URL/IP.
- The user accesses the newly published service.
- Once the user disconnects from the service, Controller instructs the Access Gateway to block access to the specific user to the specific application.



[3]BleepingComputer, “7% of All Amazon S3 Servers Are Exposed, Explaining Recent Surge of Data Leaks,” September 2017

By protecting mission-critical services under an on-demand access session, Shield removes these services from the public internet unless needed. This short-circuits the reconnaissance aspect of the data breach decision loop – hackers are no longer able to map a network diagram using search engines or other tools. While this doesn't completely mitigate the risk of an attack, it lowers it a great deal. According to referenced from Gartner, companies that isolate their applications, databases, and cloud services from the public internet will see a 70% reduction in attacks[4].

In addition, Shield's myriad authentication options via the dedicated authentication portal, provide the following benefits:

HTTP-GET Method Only: Block HTTP Methods (POST/DELETE/HEAD) – Allow only HTTP GET Method, which makes authentication functionality of any HTTP Web Applications and Services - Read-only.

Zero Data Injection Vulnerabilities: Protect SQL, Directory Services, and all other identify services from being injected by harmful queries.

Zero Broken Authentication and Session Management Vulnerabilities: No more leaks or flaws in the authentication/ session management functions.

Insecure Direct Object References: Verify the user authorization for the target object.

Zero Security Misconfiguration: Eliminate attacks due to an insecure application as a result of Misconfiguration.

Zero Sensitive Data Exposure: Protect sensitive information- passwords, session tokens, etc.

Mitigating Credential Theft

Another benefit of hiding services from the public internet is that it in some ways it can mitigate credential theft. Ordinarily, if an attacker steals credentials and maps an organization's network diagram, they have as much as they need to move on to the exfiltration phase. If they steal credentials without mapping the network diagram, they will have no understanding of what those credentials are supposed to unlock – they have nothing.

In the rare event that attackers can capture both stolen credentials and the address to a login portal, there's yet another way to stop them from getting in. Most logins to critical systems come from a very small number of endpoints and mobile devices. If the attacker is unable to understand how to impersonate these devices, then attempts to log in using stolen credentials can also be put off. This technique, known as device fingerprinting, will be added to Shield in the very near future.

[4]Gartner, "It's Time to Isolate Your Services From the Internet Cesspool," September 2016

Keeping Data Stored Safely

Much of security and most of compliance is aimed towards preventing individuals from accidentally or maliciously moving data from where it should be to where it shouldn't. This includes hackers mailing data to themselves, or malicious insiders transferring data from private clouds to personal clouds, or even neophyte employees who accidentally press "print" on the wrong document.

There are nearly infinite ways to move data from one location to another, and nearly all of them can put that data at risk. Shield Software Defined Access is designed with a plethora of use-cases in mind, which will let administrators become alert to any number of potential compliance and security risks, mitigating them with a press of a button. Here are just a few use-cases where Shield makes security manageable.

Anonymous Application Access

Challenge

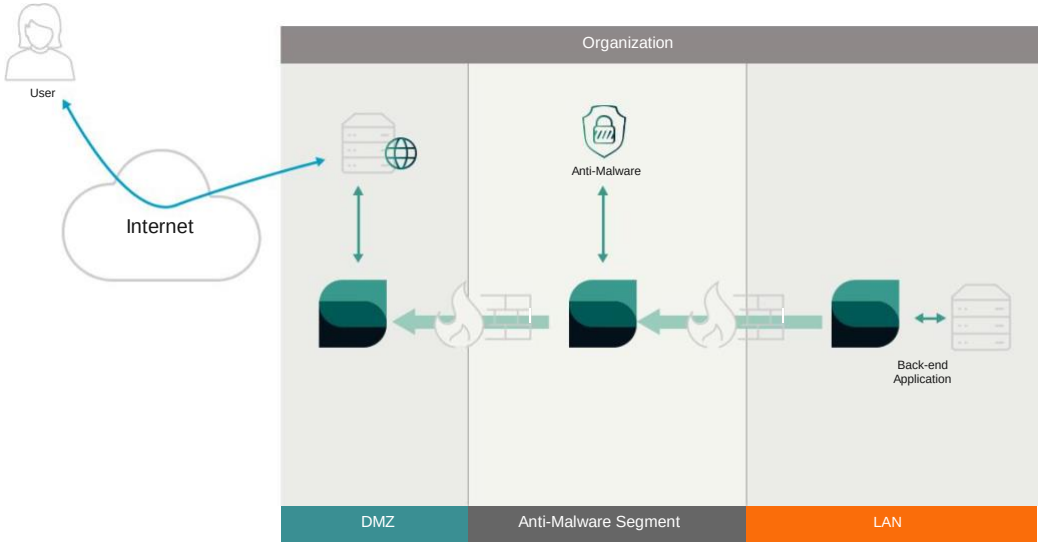
How can organizations safely provide equivalent levels of application access to both verified customers and anonymized users?

Use-Case

For any given application, some users will be attackers, either insider threats or outside attackers, and the files they upload may contain malware. This might affect banks, who accept images of checks as a form of mobile deposit, job applicants uploading resumes, or doctors uploading x-rays to a healthcare system.

Benefits

Shield lets anonymous users, devices, and APIs interact with application endpoints in the DMZ without providing any access to data behind the firewall, letting businesses launch new services without worrying about security. Pre-existing security solutions can be placed in line to scan incoming files in a secure zone, a process that can be scaled easily across dozens of applications.



Secure Application Access

Challenge

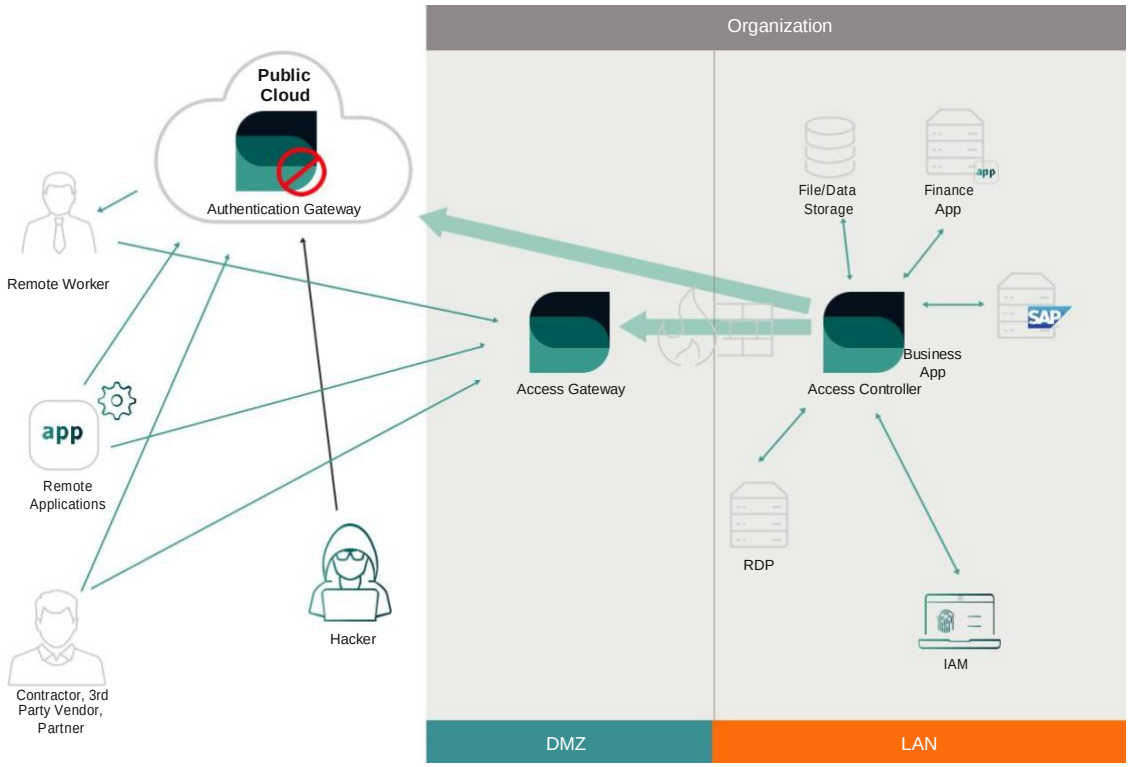
Major enterprise applications and services share a common flaw – they provide access before they authenticate. For example, if attackers can identify published SAP portal, they can hack it to steal sensitive information. The same goes for VPN, reverse proxy access, and RDP. These services all place major mechanisms in an area where they are easy to subvert.

Use-Case

Any application that depends on openness to provides functionality and revenue is potentially vulnerable. This might include banks providing Open API access to vendors, users accessing internal applications on mobile devices, or application-to-application communication.

Benefits

Shield hides the vulnerable components of Web, WebDAV, S/FTP, SSL VPN, RDP, and other services. It removes the need for VPN access altogether, and performs SSL decryption in a secure zone, making MITM attacks that much more difficult.



Secure Email and File Access

Challenge

Email remains the most potent vector for hackers to exfiltrate data from organizations, and for employees to leak data via accident or malice. Non-email file transfers also make up a large amount of corporate data traffic, and can also be hijacked by attackers looking to exfiltrate data.

Use-Case

Employee collaboration, S/FTP replacement, NTFS access over HTTP, secure email.

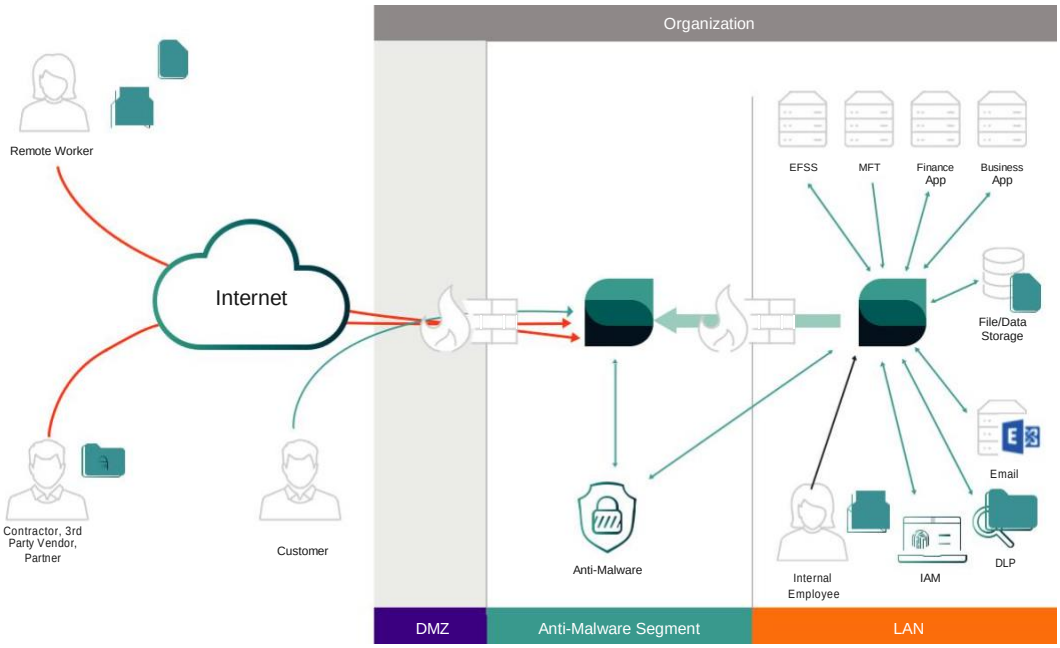
Benefits

Shield offers a mobile app, Outlook plugin, OWA plugin, Gmail integration, and a network deployment that aims to track the access, usage, and migration of email and files across an enterprise.

When sending attachments, users can employ a secure email solution that controls all emails leaving the organization, regardless of destination, file type, etc. Recipients (both registered and anonymous) do not require to install any client application in order to access shared emails and attachments.

For file usage and transfer, connectors built into the solution integrate with multiple business application, security solutions, and storages. This allow controlling all file operations, and who can access them.

The solution allows replacing legacy S/FTP deployments. Now, Shield acts as both an S/FTP client and server, and can directly receive files uploaded by S/FTP and store them in a secured NTFS drive.



Cloud Storage Access

Challenge

North American enterprises typically use 1,245 cloud applications per company[5]. Most of these deployments are unsanctioned by IT - and they all represent a vector for risk.

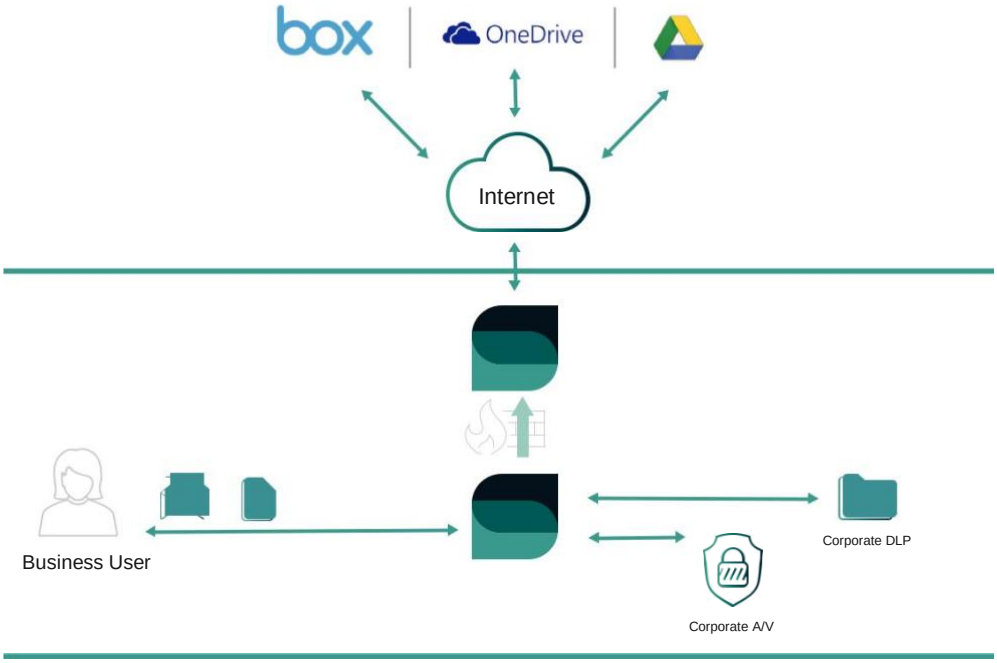
Use-Case

- Integrating cloud storage with on-premises security solutions.
- Utilizing on-premises encryption keys with cloud storage.
- Converting cloud storage into digital vaults.

Benefits

Shield-SDA is designed to gather these shadow IT deployments under a single umbrella:

- **Intercepts uploads to cloud storages and brings them in line with pre-existing security solutions**
- **Adds a layer of "where/what/who/ and when" auditability to all major cloud solutions**
- **Automatically encrypts data that is sent to the cloud**
- **Alerts and mitigates when data is transferred in an inappropriate manner**



[5]Ciphercloud, "CIPHERCLOUD REPORT IDENTIFIES OVER 1,100 CLOUD APPLICATIONS IN USE BY COMPANIES, 86 PERCENT OF CLOUD APPLICATIONS ARE "SHADOW IT," February 2015

Hybrid Cloud Deployment

Challenge

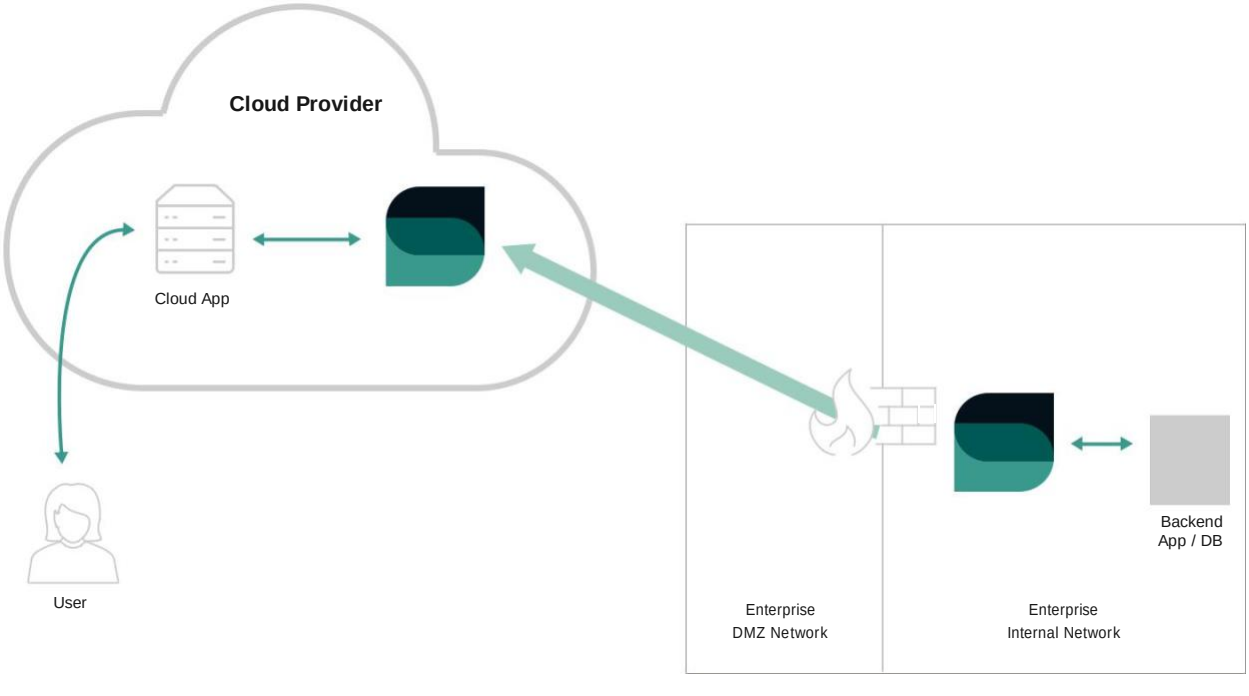
Enterprise DMZ and perimeter architecture has only become more complicated over time. This deep perimeter layer can cause network and application slowdowns and hinder attempts at troubleshooting.

Use-Case

Migrate to the cloud without compromising on security.

Benefits

Deploying Shield-SDA as part of a hybrid cloud strategy makes sense for the enterprise. Shield pulls incoming data from the cloud, obscuring the external IP address and physical location of a cloud or on-premise data center. This prevents reconnaissance for more sophisticated attacks and even mitigates DDoS risks.



Shield Technology Platform

Shield-SDA is powered by an Integrated Data Security Platform (IDSP) comprised of six modules. Enterprises can start with individual modules based on business needs, and then scale up as required, with each individual module integrating seamlessly with the platform.

SecureStream™ Policy & Workflow Engine

This module represents a turnkey compliance and security engine for data exchange and data access. Administrators can use this module to monitor data exchange and access across an organization, and automatically enforce policies such enabling multi-factor authentication and authorization, scanning outgoing email attachments through DLP, and encrypting files in motion and at rest.

SmartTransfer™ SIFS (Secure Internet File System)

SmarTransfer enables anonymous and NTFS storage access. Customers and anonymous users can use SmarTransfer as a network drive, but it functions as a secure, encrypted, and access-controlled HTTP channel that can interact with files without the vulnerabilities presented by SMB.

Authentication Gateway

The component provides authentication and enforcement through several commonly-used engines, including:

- Microsoft Application Directory
- LDAP
- Open ID/SAML
- Microsoft Radius Server
- Kerberos authentication server
- NTLM
- Post / NoPost

Reverse Access

This dual-server patented technology makes it possible for users to keep their firewall in constant deny-all mode, while allowing secure application access between networks. There is an external server and an internal server:

External server – Located in the organization's DMZ (on-premise or cloud), the external server acts as a front-end to all services/applications published to the Internet. It operates without the need to open any ports within the internal firewall and ensures that only legitimate session data can pass through into the internal network. The external server performs TCP offloading, allowing it to support any TCP based application without the need to perform SSL decryption.

Internal server – Installed in the internal/secured segment, the internal server pulls the session data into the internal network from the external server, and only if the session is legitimate, perform layer 7 proxy functionality (SSL offloading, URL rewrite, Deep Packet Inspection, etc.) and pass it to the destination application server.

Connectors

Shield-SDA supports API connectors that allow integration with business applications: Sharepoint, Oracle, Outlook, data storage (SQL, MySQL, NFS, NTFS, SSH, DropBox, Box), and security solutions (IAM, IDP, DLP, AV, ActiveDirectory, etc.). These connectors ensure that Shield-SDA will function right out of the box with nearly any enterprise environment.

Unified Protocol

Shield-SDA supports multiple protocol conversions within a single workflow – HTTP to SFTP to SQL to OneDrive. This standard API makes the data transfer process completely transparent and customizable.

Shield isn't just about safety. Its technology modules support transparency and security, but they also promote usability and efficiency. Administrators can get Shield-SDA out of the box, running, and tailored to fit their needs in record time, minimizing the training wheels aspect of running a new security platform.

Shield-SDA Deployment Requirements

Shield-SDA is a virtual appliance and available as an OVA or AMI file depending upon where the pair of serves will be deployed. Two servers (nodes) are used to create the Shield-SDA network protection solution, which we refer to as a logical unit.

These two nodes are the internal Shield-SDA server node (which normally resides in an internal network) and the external Shield-SDA server node (which normally resides in the DMZ). While each Shield-SDA logical unit can support a vast amount of connections and users, it is also built to scale horizontally very easily using existing infrastructure.

Shield-SDA Node Requirements:

CPU	**2 cores**
RAM	**4 GBs**
STORAGE	**25 GBs**
Each Node spec'd as above provides:	
Concurrent connections	**30,000**
New connections	**Up to 1,500 per second**
Throughput	**Up to 1 GB/s**

If multiple Shield-SDA logical units are deployed they require the following:
Load Balancer – Setting up a state-aware layer-7 load balancer in front of the external Shield-SDA node is required to balance the load across the deployed logical units.

If the load balancer detects one of the extremal Shield-SDA nodes is not responding to HTTP requests (if the designated back-end server is HTTP) – it can deem a failure in the logical unit and route the request to a different node.

It's important to note that since each logical unit is comprised of 2 servers, the failure can be in the internal node or the external node or both. Standard monitoring tools can monitor each server individually to determine where the actual fault is and notify administrators. However, the load balancer only needs to know that this route is unavailable in order to route the requests through a different external node.

.

Simplify Data Security with Shield

Shield-SDA makes it possible for organizations to interact with cloud services without opening themselves up to bad actors. In the meantime, it offers a turnkey solution for compliance. Companies can identify the elements they need – application access, network segmentation, or secure file transfers – and then apply them across the entire organization from a single pane of glass.

The increasing complexity of both security products and compliance restrictions over the past few years have done little to slow the growth of data breaches. In some ways, this is because the theory of network architecture was never designed with security as a component. Therefore, Shield doesn't just introduce a new product to bolt onto a network – it fundamentally re-molds network architecture in a way that makes security elemental.

About Shield

Shield (www.Shield4uc.com), is a leading provider of cyber-security solutions which mitigate attacks on enterprises' business-critical services and sensitive data. Shield-SDA solves the data access challenge by hiding data at the perimeter, keeping information assets safe and limiting access only to authorized and intended entities in hybrid cloud environments.

Shield products enhance operational productivity, efficiency, security, and compliance by protecting organizations from data exfiltration, leakage, malware, ransomware, and fraud. With Shield's patented, multi-layer Shield-SDA solution, financial services, healthcare, utility companies and governments are able to secure their data, services, and networks from internal and external data threats.