Deep Secure

3 Steps to a Threat-free Cloud

How to stop malware from infecting your cloud-based portals and workflows

GUIDE

Step 1: Go Serverless

A serverless architecture is inherently more secure than one based around machine images

Anyone building an application or workflow that must accept documents and images from an untrusted source into a Virtual Private Cloud (VPC), should consider using a serverless, cloud-native architecture.

Serverless is the native architecture of the cloud and it is inherently more secure because the infrastructure layer is cleanly separated from the data processing layer. The infrastructure doesn't look at the data and so doesn't get compromised by it, and the data can't see the infrastructure beyond what it is running on.

It is widely acknowledged that un-patched systems are one of the main causes of cybersecurity breaches. Serverless architectures enable the developer to shift operational responsibilities and routine security tasks such as patching, maintenance and upgrades to their service provider.

The alternative to serverless architectures, machine images in the cloud, have the associated risk that if malware succeeds in compromising the machine, it remains compromised thereafter. With a serverless, cloud native architecture, there is no residual "machine" and therefore no residual risk.

Step 2: Transform your Data

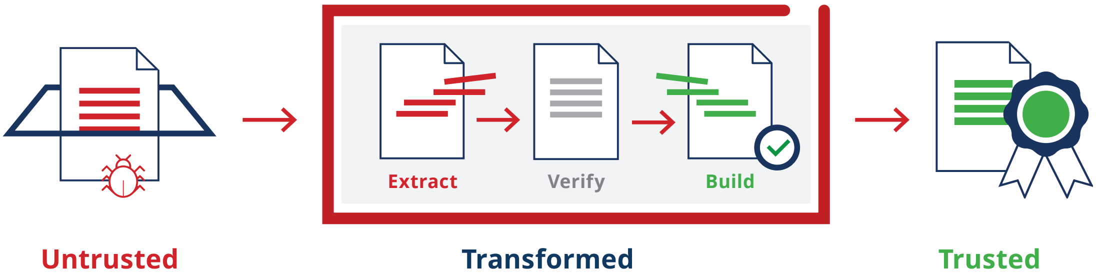
Ensure your cloud is threat-free by transforming data to remove any threat

Data is routinely embedded with known, zero day and even totally undetectable threats. This malware is now so sophisticated and well-concealed that it repeatedly evades detection by conventional anti-virus tools and even modern artificial intelligence technologies. Keeping the cloud clean means finding a zero-trust technology to combat this.

The only way to be certain data is threat-free is to stop trying to detect whether it contains malware, assume it does and use a process to transform it into a safe document in line with recommendations laid down in the NCSC "Pattern: For Safely Importing Data", a set of leading practice guidelines for accepting data from untrusted sources..

To be truly effective, every untrusted document should be transformed with only the necessary business information extracted from it. The original file should then be discarded, along with any encoding context, un-necessary metadata, active code and malware.

The extracted business information can then be formatted to match the original and a wholly new file created that is feature rich, fully editable and in the same file format type as the original, all in real-time. None of the original untrusted digital file should reach the application or workflow.



Step 3: Design-in “Security As Code”

APIs enable you to design-in security into your applications and workflows as code

Developers should look to “design-in” “security as code” into their applications and workflows by accessing security controls, such as ‘transformation’, using APIs.

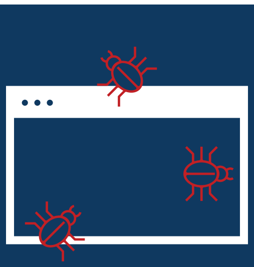
The developer will need access to a choice of APIs, selecting the one that best fits the particular application or workflow. For example, some applications will require a simple “upload/download” API to transform a file, while other applications will need APIs capable of handling more complex tasks such as event-driven workflows or moving files between different storage buckets.

Whichever API is required, it is important for reasons of privacy and security that the service does not store the document in the cloud and that the service provider offers an SLA of 99.9% and a choice of region to provide control over cost, latency and address any data residency concerns.

Designing new applications and workflows around a serverless, cloud-native architecture, transforming every document in real-time to render it 100% threat-free and implementing “security as code” via a range of APIs will stop malware from infecting your cloud-based portals and workflows.

Use Case: Web Portals

A web portal is a key vector for attack



The Problem

Web portals are used for multiple purposes but generally are chokepoints in organisations for accepting and/or publishing digital content.

A web portal is a key vector for attack, often an overlooked ‘side entrance’ to your organisation that, at best, relies on OWASP Top Ten principles to protect your critical assets.

The problem is that technologies that try to prevent weaponised content being used to attack an application via a portal, such as antivirus or WAFs, rely on detection and analytics to find the threat and can be beaten.

The Solution

Deep Secure’s *‘Threat Removal as a Service’.*

Once integrated into the portal application, the API intercepts the upload and sends the original content to Deep Secure’s cloud-based Threat Removal technology. In a fraction of a second, a new file is created that looks and feels identical to the original upload – delivering a clean and threat-free document back to the application or process flow.

The application receives the business information it needs – but all known and unknown threats remain outside the organisation.

Use Case: Storage and Migration

Data Storage and Migration

The Problem

Typically, when a workload is migrated to the cloud it is commonplace to scan the files on entry for malicious content. The problem is that detection technologies cannot identify unknown or zero-day threats. So, it's entirely possible that organisations moving content from a traditional data centre move content to the cloud assuming it has been 'cleaned' successfully by anti-virus engines.

This is not a safe assumption to make.

So how is it possible to migrate to a cloud storage platform, ensuring that you don't inadvertently migrate documents and images laced with malware during the process?

The Solution

Deep Secure's *'Threat Removal as a Service'*.

The service pulls and pushes content from and to cloud storage buckets. During this process, Deep Secure's cloud-native Threat Removal technology will build brand new fully functional versions of the content. Everything looks and feels the same – but crucially – whilst the business information needed is built new, any threats are automatically left behind.

The service pulls content from one cloud storage bucket and delivers a new version to another bucket in real-time– even to another account if needed!

Deep Secure

'Threat Removal as a Service'

Threat Removal as a Service (TRaaS) is a developer platform that combines Deep Secure's Threat Removal technology with a range of APIs. The service allows developers to integrate threat removal into their applications and content workflows, using a cloud-based subscription model, to provide risk-free data exchange.

TRaaS is built using AWS Lambda to provide a serverless security solution for application(s) with limitless scalability.

As a cloud-based service accessed via an API, TRaaS has no setup overheads and can be integrated into workflows and applications in a matter of seconds. There is no upfront cost - no CAPEX spend, no hardware cost or depreciation, no patching, maintenance or upgrade considerations and you only pay for what you use.

Delivering real-time, risk-free data in the cloud.