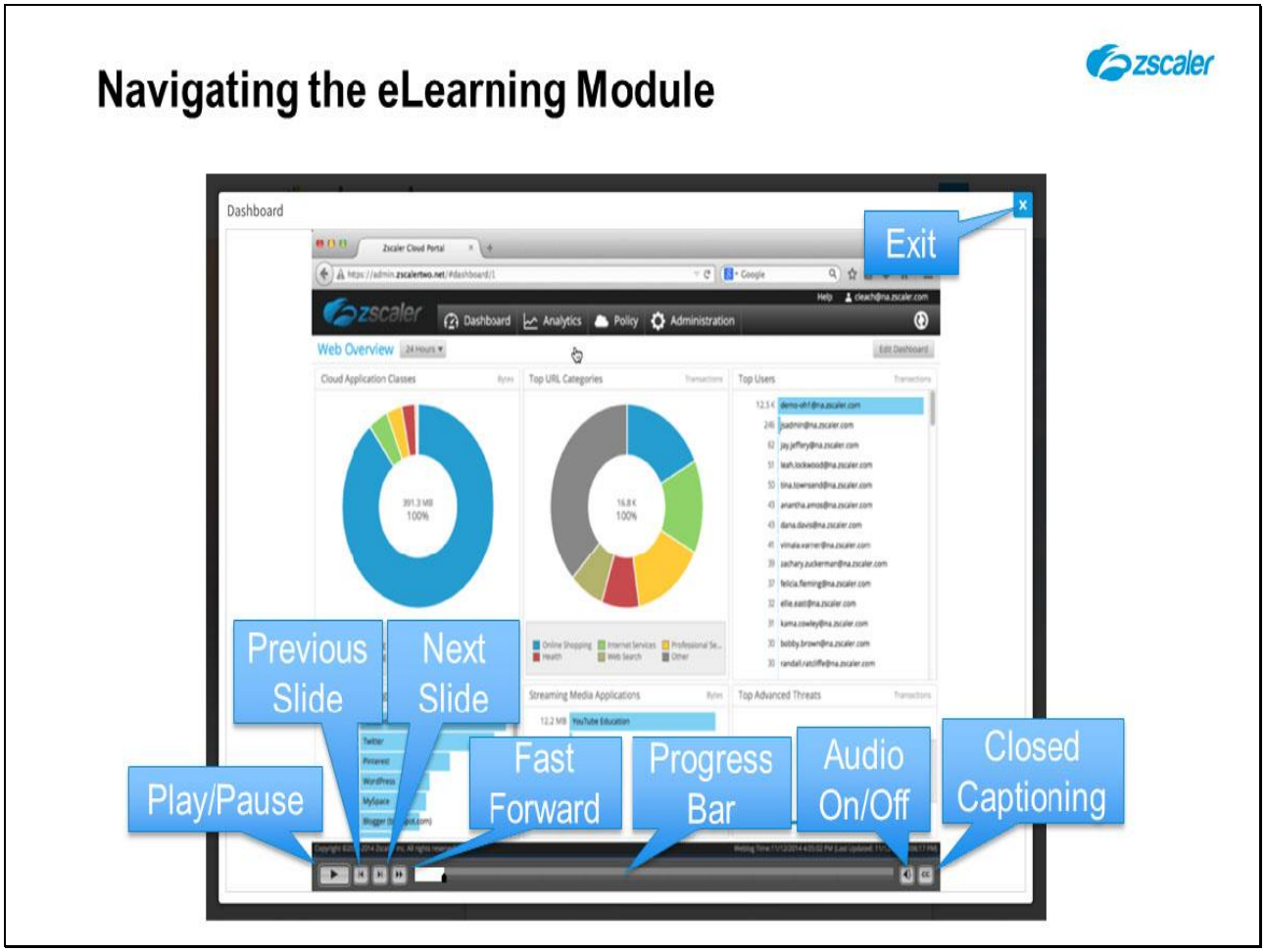
Slide 1 - Zscaler Architecture

Slide notes

Welcome to the Zscaler Architecture Module.

Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this eLearning module. There are various controls for playback including Play/Pause, Previous and Next Slide, and Fast Forward. You can also mute the Audio or enable Closed Captioning which will cause a transcript of the module to be displayed on the screen. Finally, you can click the **X** button if you wish to exit.

Slide 3 - New Product Names

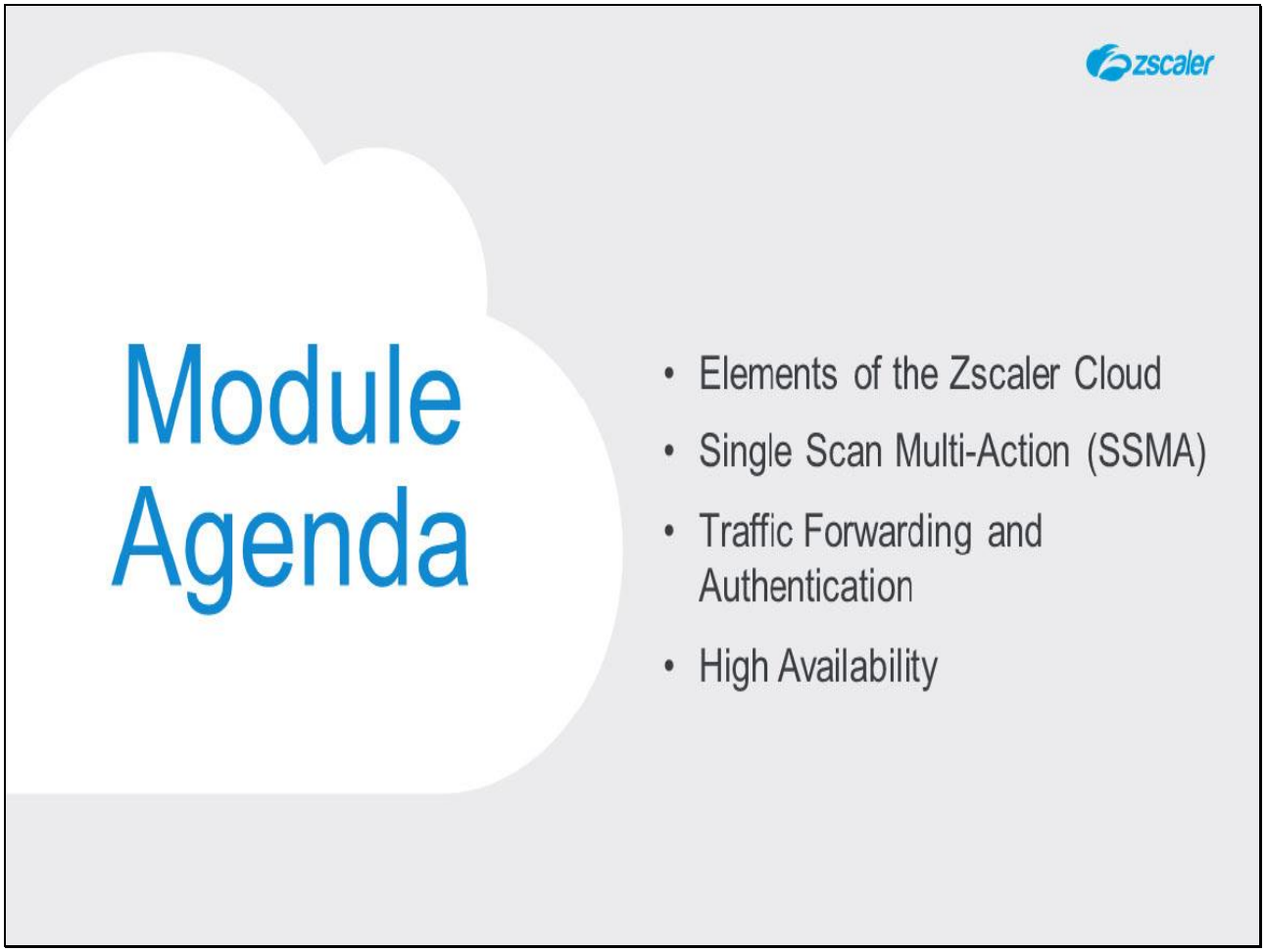
	Current Product Name	New Product Name
Connectors		
	Zscaler App	Client Connector
	ZPA/B2B Connectors	App Connector
Zscaler Service Edge		
	ZPA	
	ZPA Broker	ZPA Public Service Edge
	Private Brokers	ZPA Private Service Edge
	ZIA	
	ZEN/SME	ZIA Public Service Edge
	Private/Virtual ZEN	ZIA Private Service Edge
Other Services		
	Remote Browser Isolation	Cloud Browser Isolation

Slide notes

Before you begin, take a moment and familiarize yourself with the recent changes to Zscaler product names used throughout this course. For example, “Zscaler App” is now called “Client Connector”.

A complete reference of old and new product names for ZIA, ZPA and Z-App is available on the Help Portal at the URLs listed here.

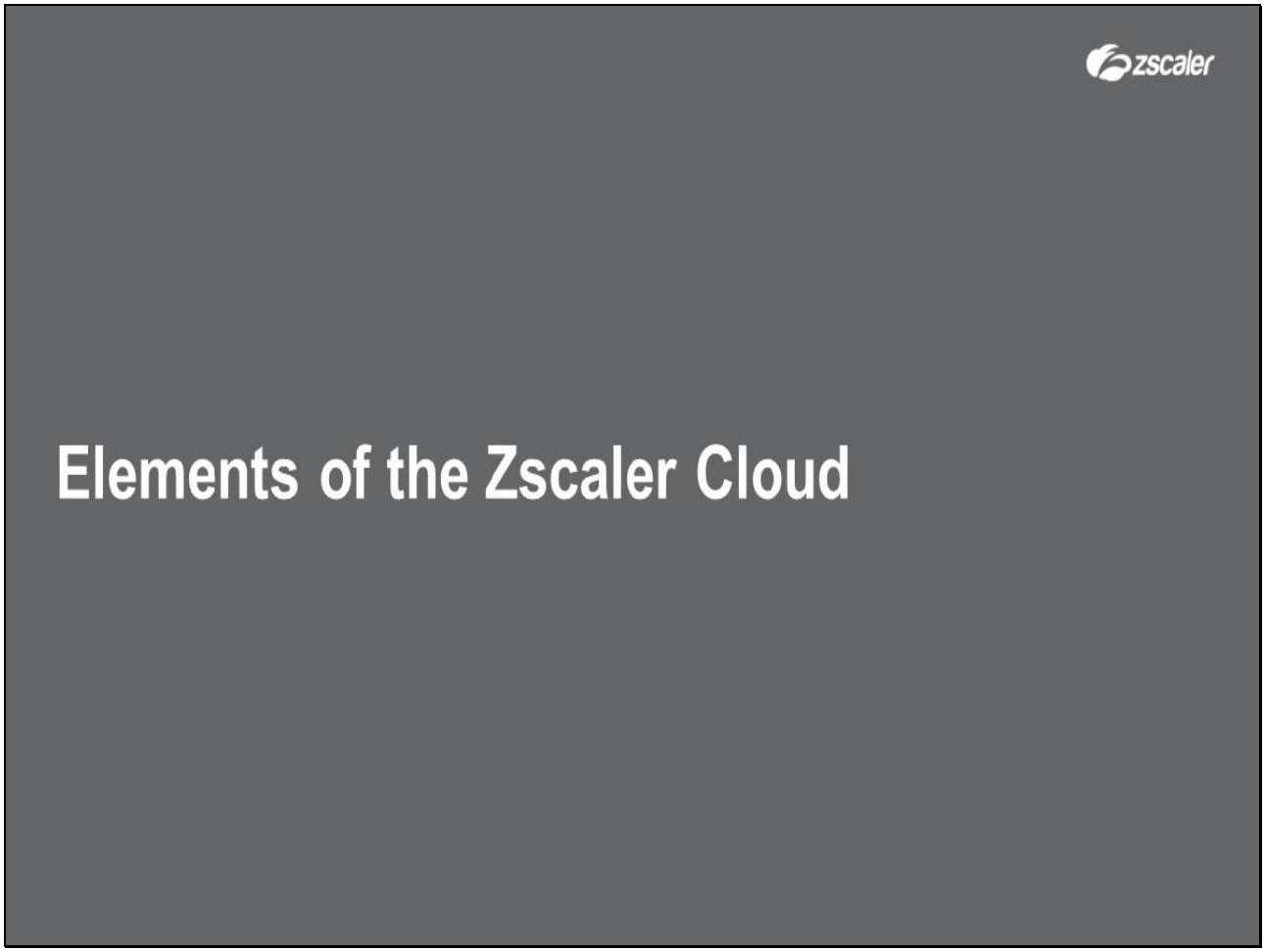
Slide 4 - Module Agenda



Slide notes

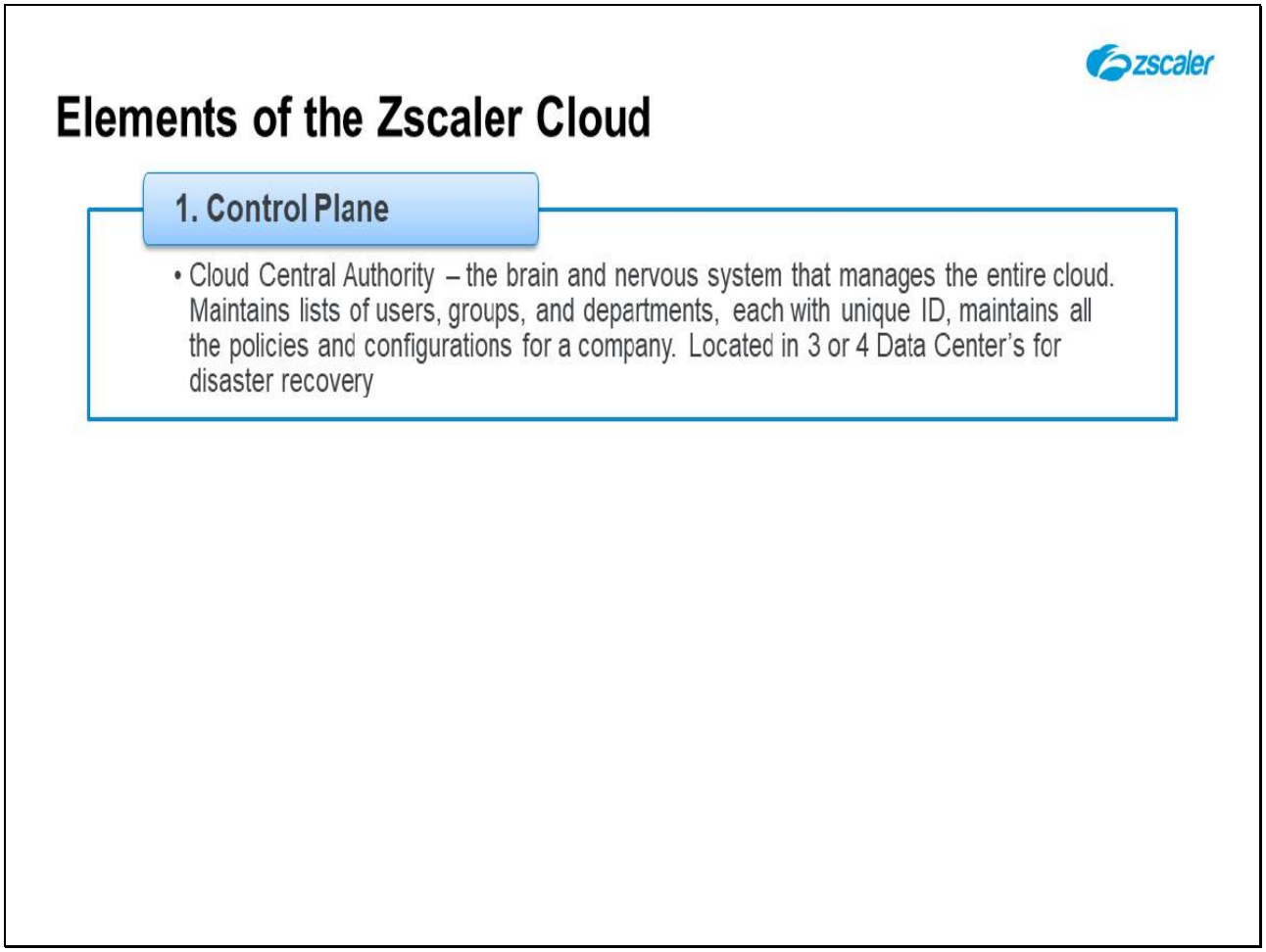
In this module we will cover the elements of the Zscaler Cloud including the Central Authority, Zscaler Enforcement Node, and Nanolog, Zscaler's Single Scan Multi Action technology, Traffic Forwarding and Authentication, and High Availability.

Slide 5 - Elements of the Zscaler Cloud



Slide notes

Slide 6 - Functions of the Zscaler Cloud



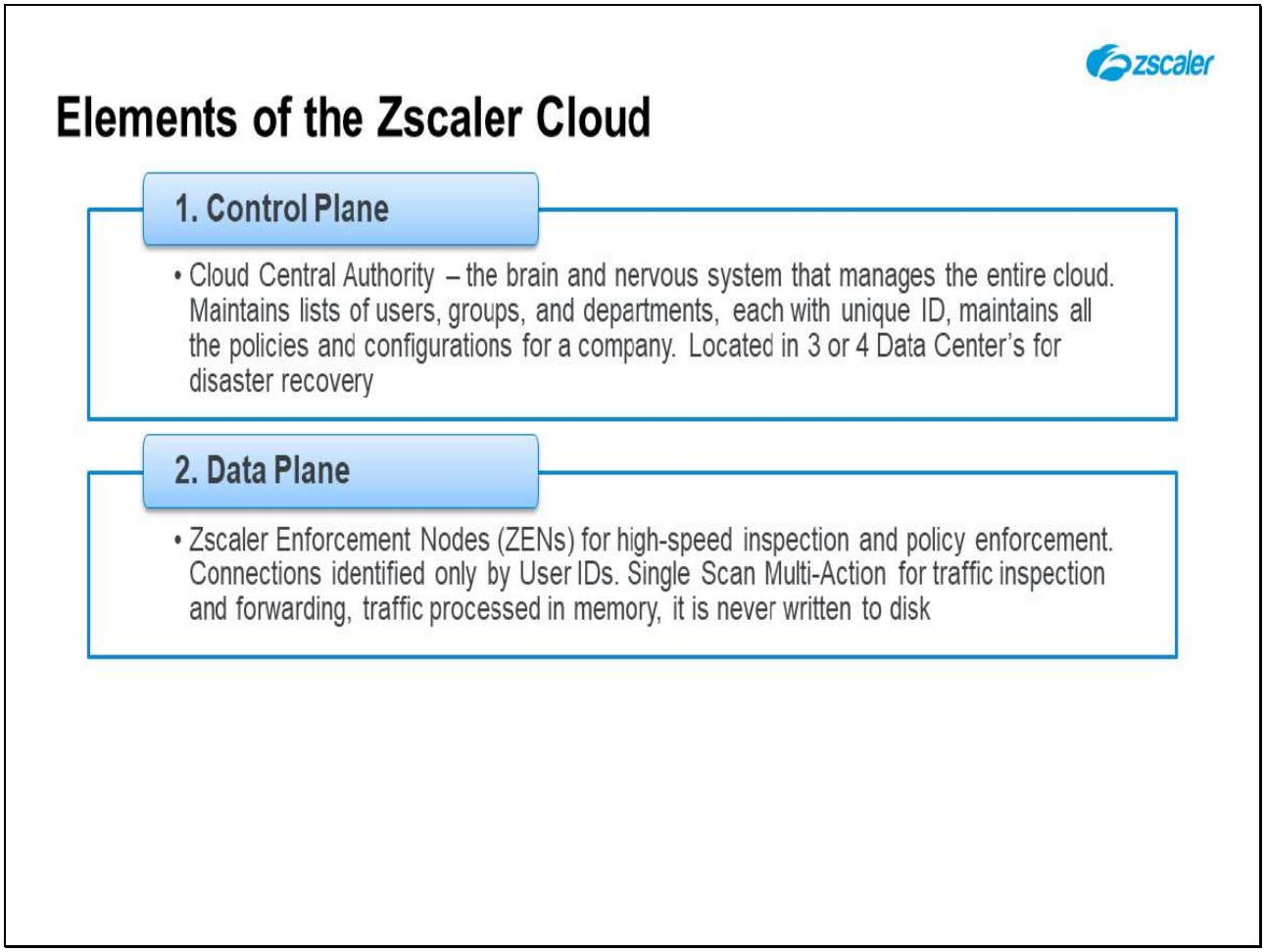
Slide notes

Zscaler operates several clouds, you were assigned one when you became a Zscaler customer. What we're going to describe here is replicated for each Zscaler cloud.

So, what are the various functions needed to build the solution? First, you need to provide Management of policy; next, you need to provide high-speed in-line inspection and policy enforcement; and finally, you need to provide visibility into what is going on. In building the platform from scratch we realized that we needed to split the entire architecture into 3 areas.

One is the control plane to manage policies.

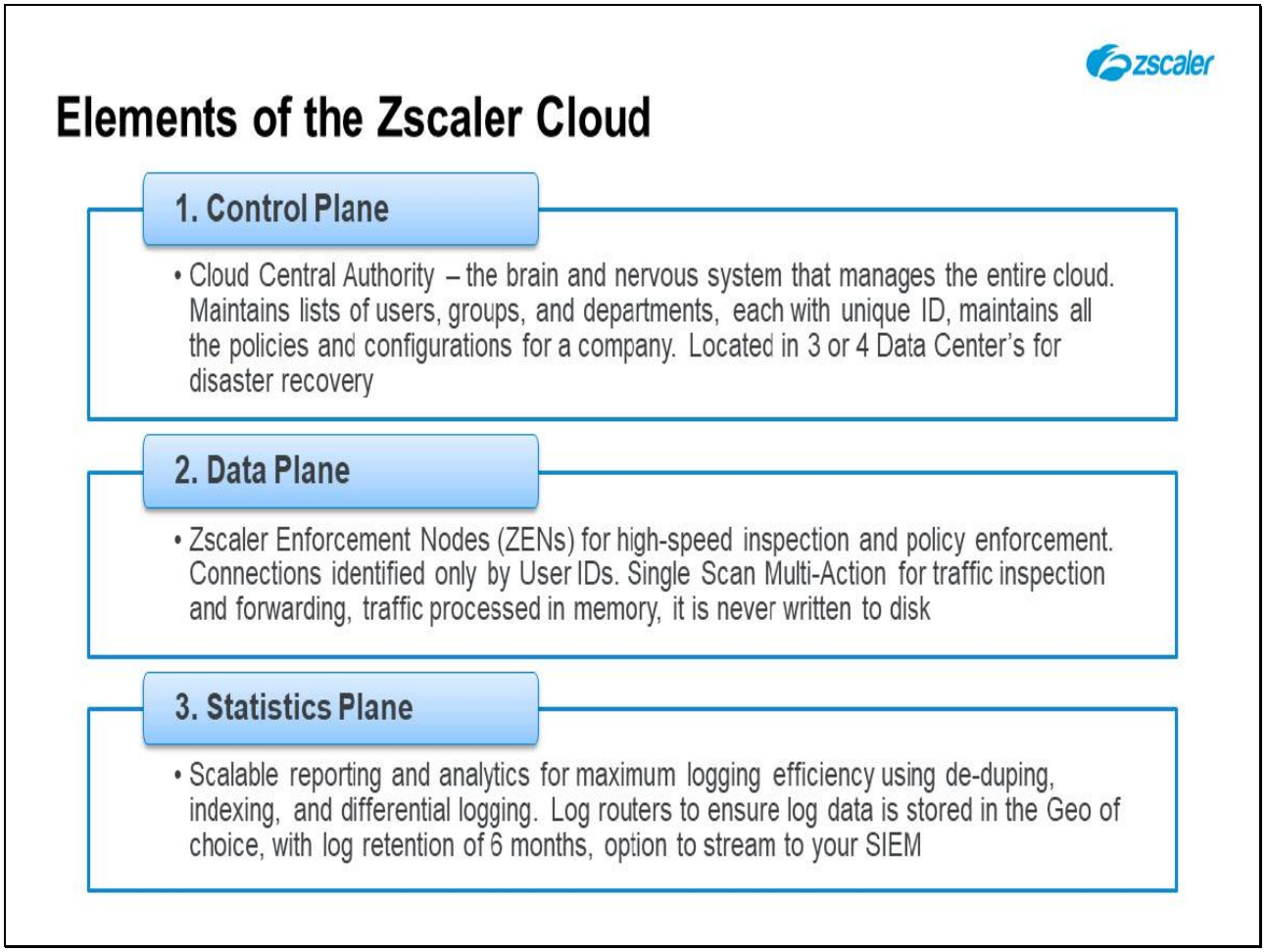
Slide 7 - Elements of the Zscaler Cloud



Slide notes

The second is the data plane where traffic will flow, …

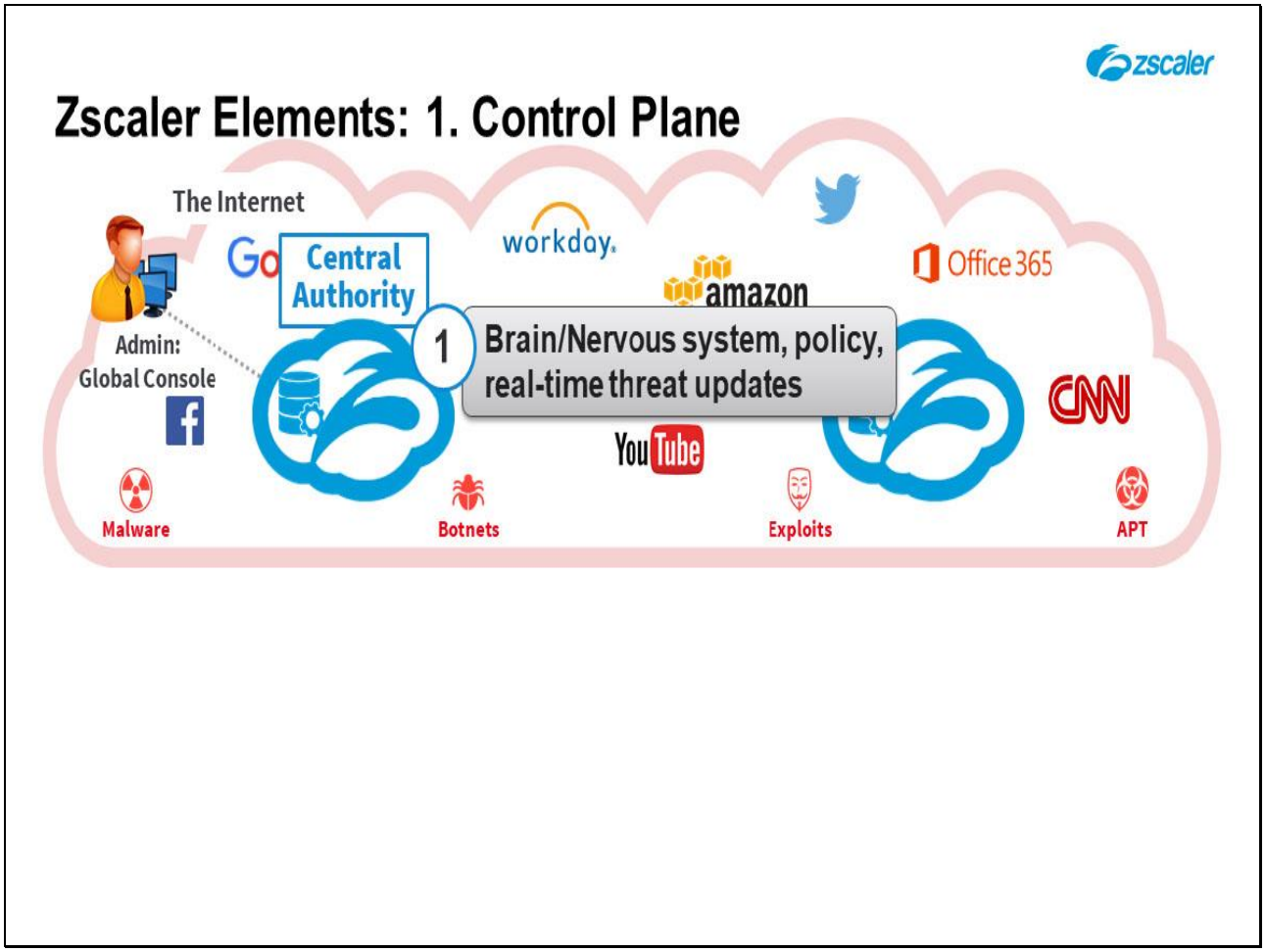
Slide 8 - Elements of the Zscaler Cloud



Slide notes

…and the third is the statistics plane where we collect all the logs and get it back and correlated for your analytics. Unless we looked at those as 3 separate planes, we knew we would get into resource contention versus each other and not do a good job.

Slide 9 - Zscaler Elements: 1. Control Plane



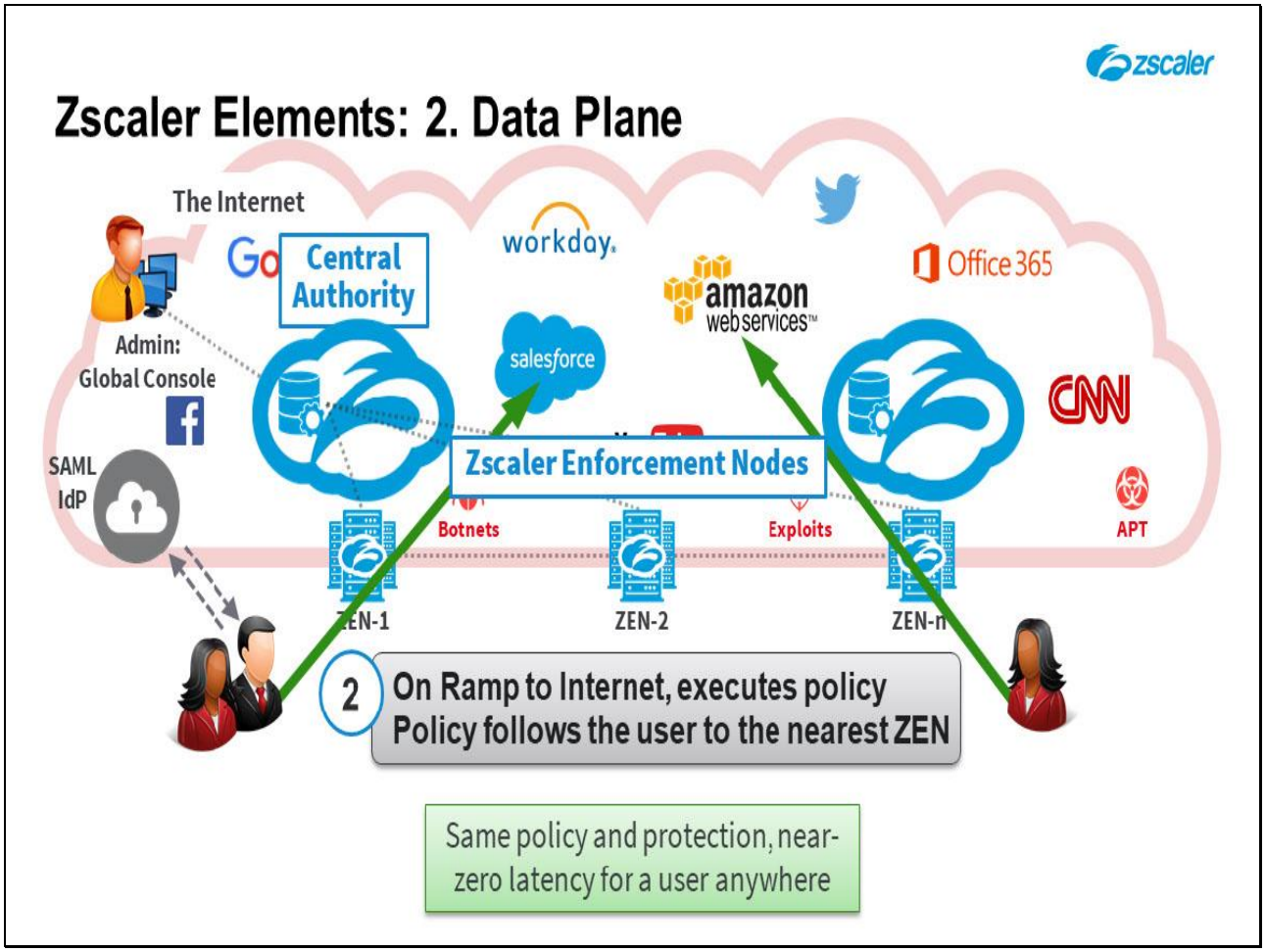
Slide notes

The Central Authority is our brain and nervous system. It manages the entire cloud. What the Central Authority does is give you an administration console for every organization so that you can log in and set up your policies. The CA holds the list of users, groups, and departments along with all the policies and configurations for a company. There are no user credentials stored in the ZENs or Nanologs.

Instead, the CA assigns a unique ID to each company, location, and user. The ZENs and the Nanologs are only aware of these token IDs; they are both unaware of the real value of the company, user, and location fields. So even if someone compromised a Nanolog cluster, the logs are useless without the Central Authority's reference to Companies and User names.

From a distribution standpoint, we don't really need the Central Authorities to be in every datacenter around the world. They need to be in 3 or 4 DCs for disaster recovery and we're covered.

Slide 10 - Zscaler Elements: 2. Data Plane



Slide notes

When your users actually go out to the Internet they go through what is called a Zscaler Enforcement Node or ZEN. The requirements on the enforcement node are very different from the requirements of the Central Authority. The enforcement node is a high-speed inspection and policy enforcement device.

It does not need to know that that the user is Joe or Sarah from Company X or Y. It needs an ID and it needs that user's policy. Initially our enforcement node has no idea of any organization's users. When a user shows up and the TCP connection is formed it calls the central authority and says give me an identity and the policy. That happens in about 200 milliseconds.

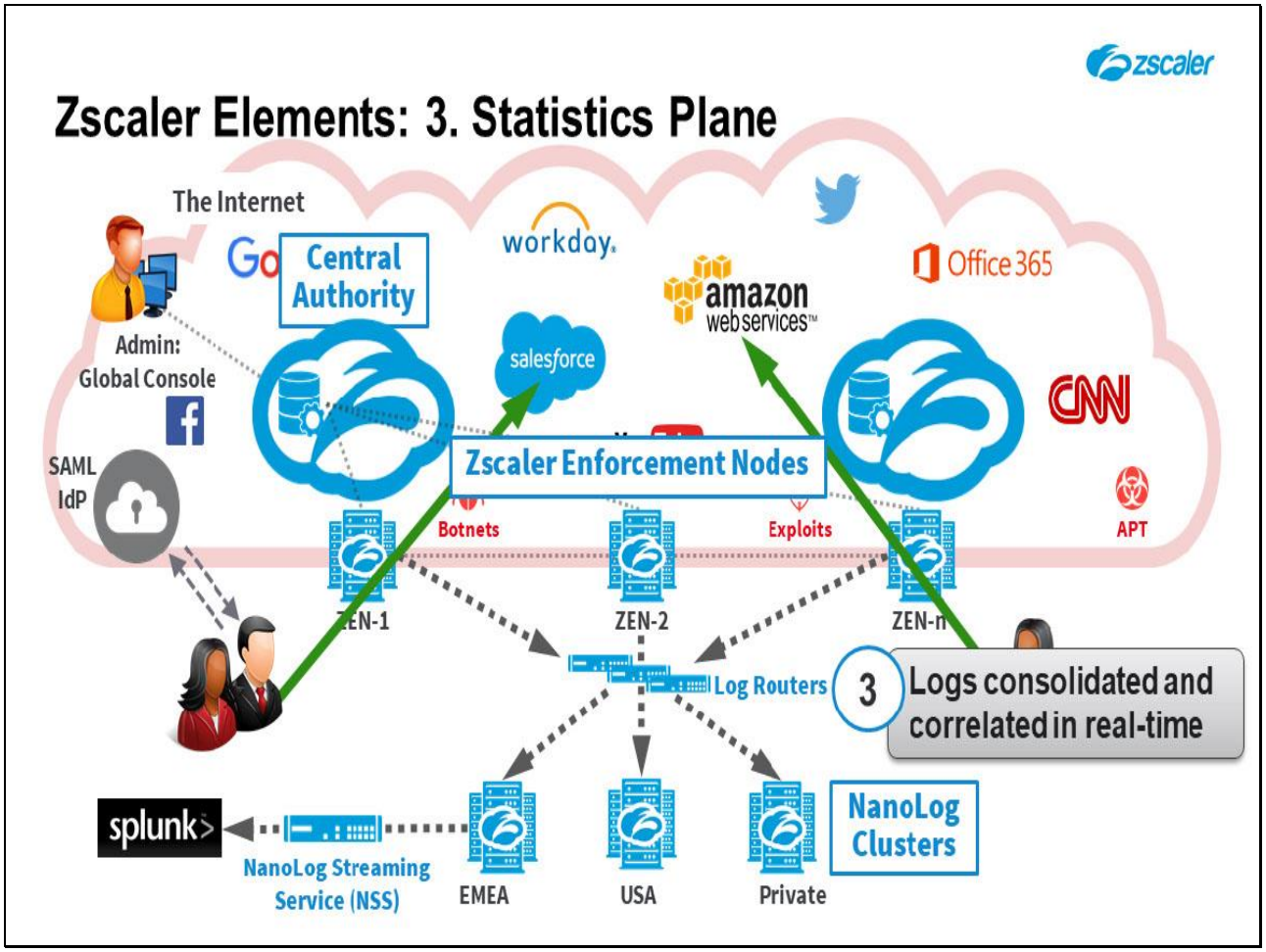
And for that session, Ethernet onwards, that entire IP stack is allocated to this user. We isolate that user from all other users regardless of whether those users belong to the same company or different companies. It makes no difference to the enforcement node. We wrote the entire IP stack to be multi-tenant and extremely fast from day one.

Now when traffic is hitting the enforcement node, we want to make policy decisions as fast as possible and move it on, so we wrote a proxy and the entire software stack from scratch that can perform with a proxy latency of a few microseconds.

One critical mechanism for reaching those kinds of speeds was never touching the disk. Never touching the hard drive also gives us a very solid data security answer. If you are going to a cloud service that is built with appliances your data is written to disk in the region your users are in, not necessarily where you want your data to be written.

With Zscaler the data comes into memory and leaves from memory, it is never on the hard drive until it reaches the Nanolog cluster in the region of your choice. More on that later.

Slide 11 - Zscaler Elements: 3. Statistics Plane



Slide notes

The last major function of a system like this is reporting and analytics. So when we're doing 30,000 connections per second from each of these devices we also generate 30,000 logs every second. Logs are very, very large. Especially in HTTP. Usually a Get request is a couple hundred bytes and the response is also usually pretty small as well because you're loading a lot of little objects. But the log for each is 2,000 Bytes long.

So now we are generating 2,000 Bytes times 30,000 logs a second from every device. Plus, your user may fly over to Japan and her policy will fly over to Japan as well and now those logs are there. How do we make sure that all of these things are correlated together and brought back? Today doing 15 billion transactions we record almost 40 Terabytes of raw log per day.

If we didn't solve that problem way ahead of time we would have made some storage vendor really rich. What we did was we looked at WAN optimization technologies and we thought that if we take those techniques like de-duping, indexing, differential logging, etc then we could probably do much better on logging. WAN optimizers are doing unstructured data and optimizing to 30X.

With structured well-understood data we should be able to do 60X easily. So we put a team together and built our Nanolog system. So, every enforcement node as it's generating logs compresses those logs using these techniques and then every second sends them out to what we call Log routers.

Now, why are log routers needed? That is because on a ZEN, let's say in San Francisco I could have an employee of a US multi-national, a Swiss manufacturer, and a French bank. The US multi-national wants their logs to be in the US, the French bank wants them in the EU, and the Swiss manufacturer, because they are Swiss, wants them in its own datacenter.

And their employees could be anywhere. Log routers have the association of the user's ID to the location where that log needs to be stored. The log routers send the logs where they need to go and then the log is recorded to disk for the first time in the geography of your choice. This is very important if you're going to cloud and looking at your data security requirements or your regulatory requirements for where your data can be stored.

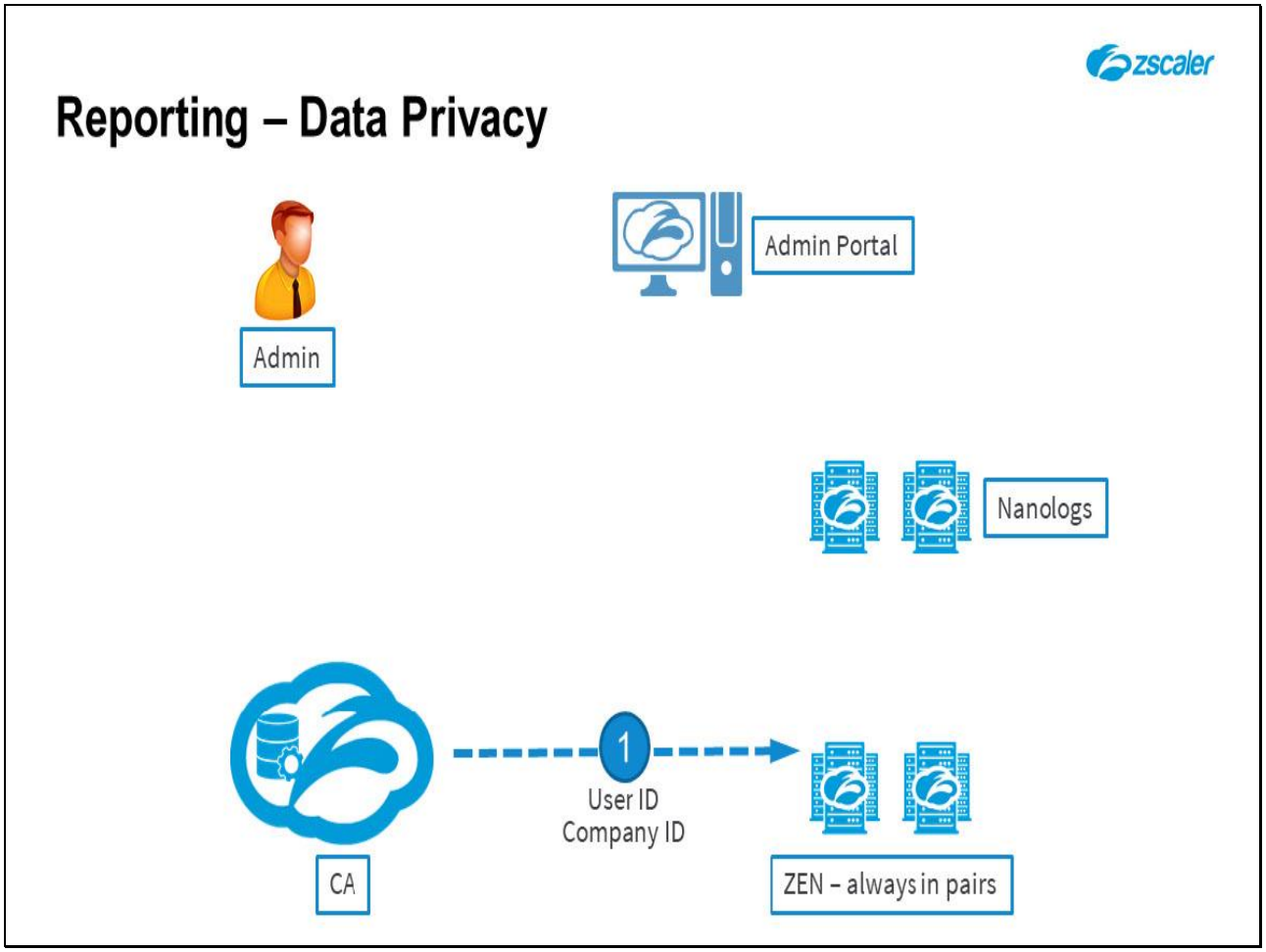
Zscaler can unequivocally guarantee that your logs, no matter where they are generated, will only be written to disk in your geography of choice.

Zscaler will store your logs for 6 months. If you want to store your logs for a longer period and/or want to do correlation with your other devices, Zscaler can also funnel it out to your SIEM in real-time using our Nanolog Streaming Service. Simply put, the NSS is a virtual machine, running under VMWare hypervisor on the customer's premise.

The virtual machine has two network interfaces, one for the inside of the network and one for the DMZ. Once deployed, the NSS establishes a connection with the Nanolog cluster, which hosts the logs for the company running the NSS. The Nanolog cluster then streams logs to the NSS using a secure connection. The NSS then can send the data to virtually any SIEM, such as Arcsight, Splunk, and even Syslog.

All this brings us back to the fact that the Zscaler architecture is highly scalable. By separating the different functions, it allows us to scale horizontally very easily. If we need more logging, we can just add capacity to the Nanolog clusters and don't have to touch any other part of the system. Same goes for ZENs, Central Authorities, or whatever we need to increase all without going through big infrastructure upheavals.

Slide 12 - Reporting – Data Privacy

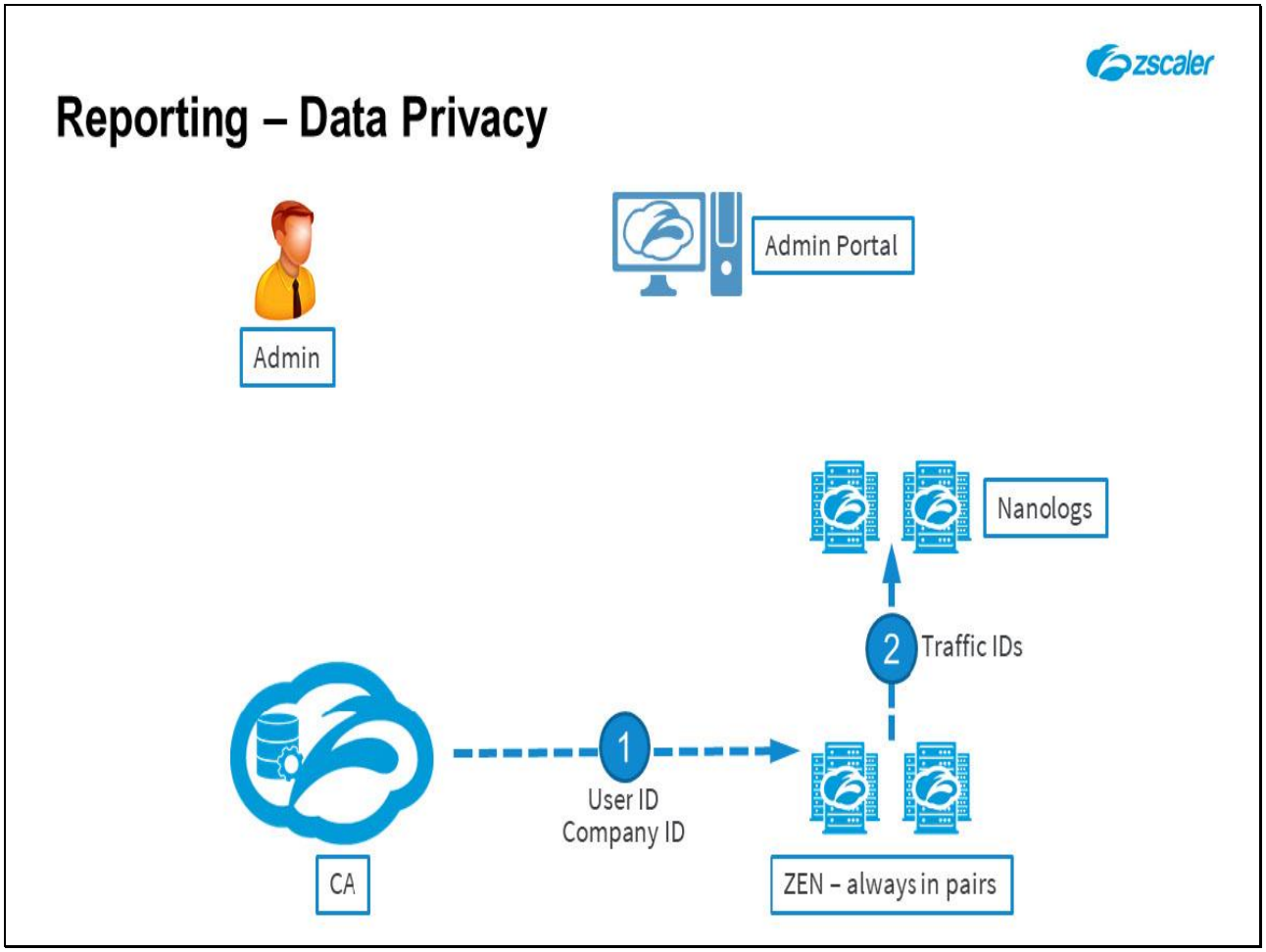


Slide notes

Here's a little more detail on logging and reporting. Zscaler natively offers a reporting architecture which complies with even the most restrictive privacy policies, such as those in effect in the European Union. Let's go through the data storing process and detail how it ensures privacy and security.

1) The Central Authority only communicates with the ZEN using a User and company ID, which is a binary string and is completely meaningless to any device but the CA itself.

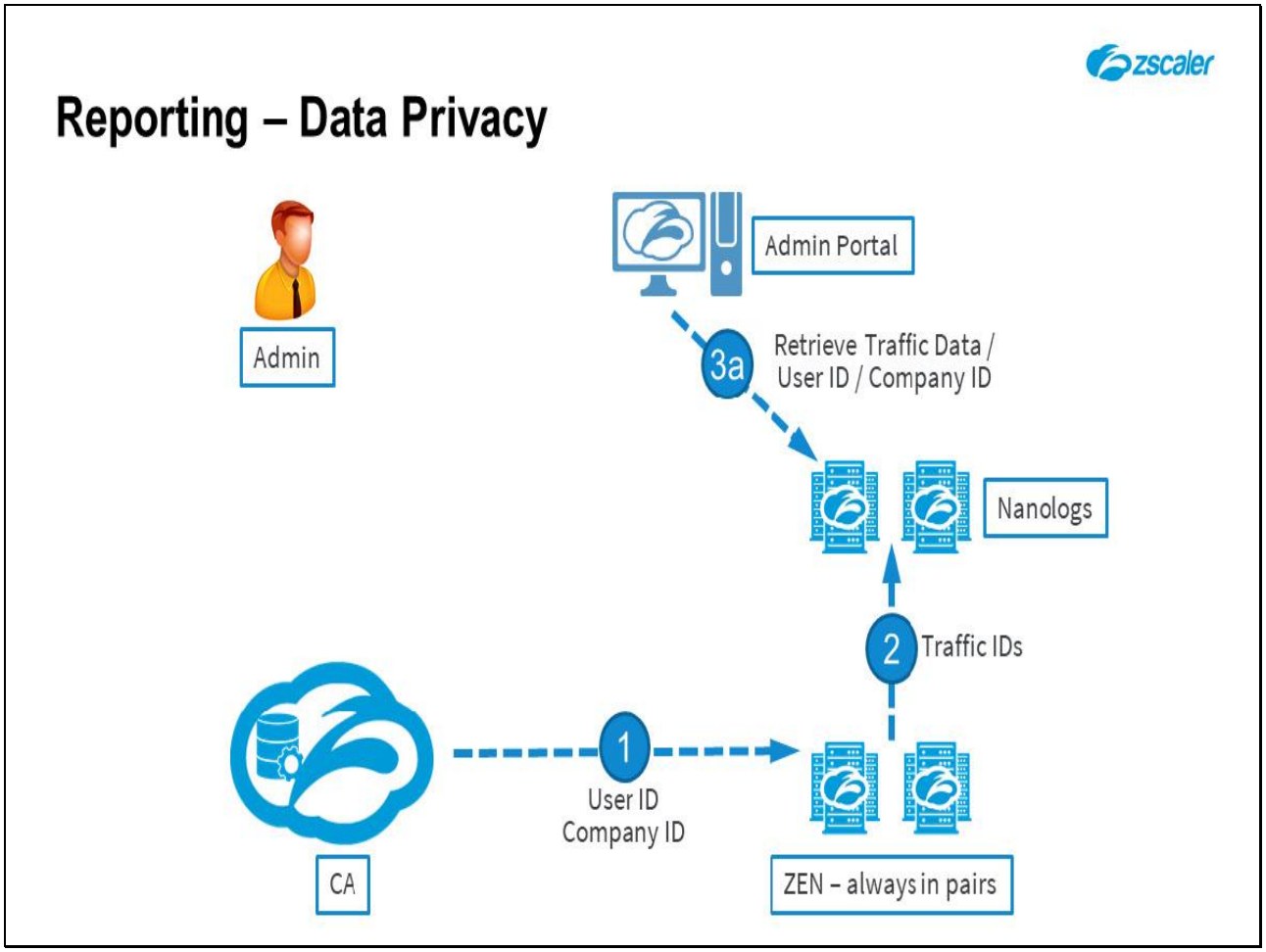
Slide 13 - Reporting – Data Privacy



Slide notes

2) The ZEN writes in the Nanalog, via the log routers, only traffic metadata and not actual data. For instance, if a user sends emails via Gmail or similar services, the ZEN only logs the information about this transaction but never its content. The content is used only for policy scanning in memory and is then discarded.

Slide 14 - Reporting – Data Privacy

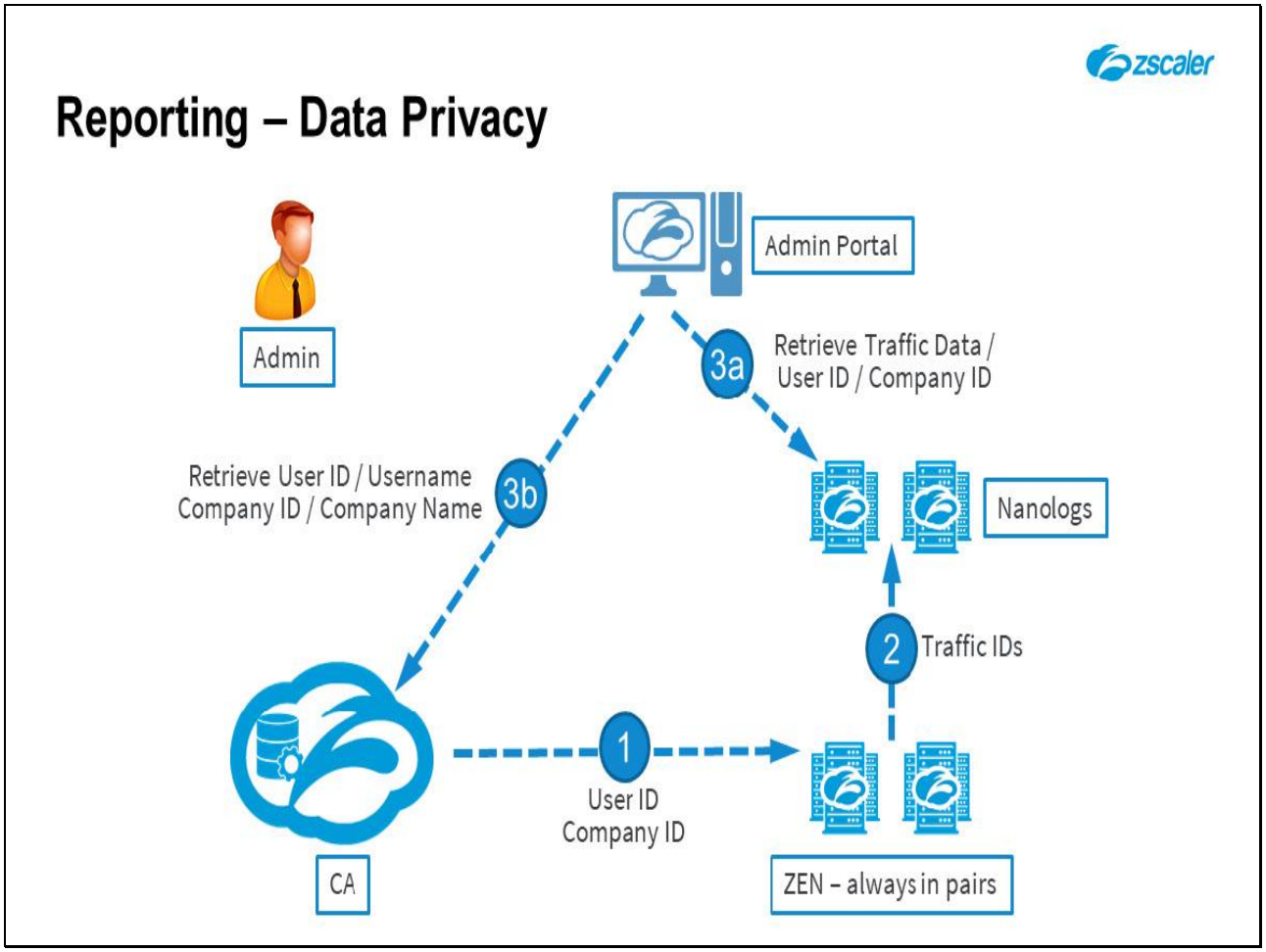


Slide notes

3) When an administrator runs a report, it connects to the administrative interface, which is hosted on a separate and independent server. Each administrator can create users who can generate reports. These users may see all data, all data except a user's ID, some data, and so on.

a. The admin server retrieves the logs from the nanolog cluster.

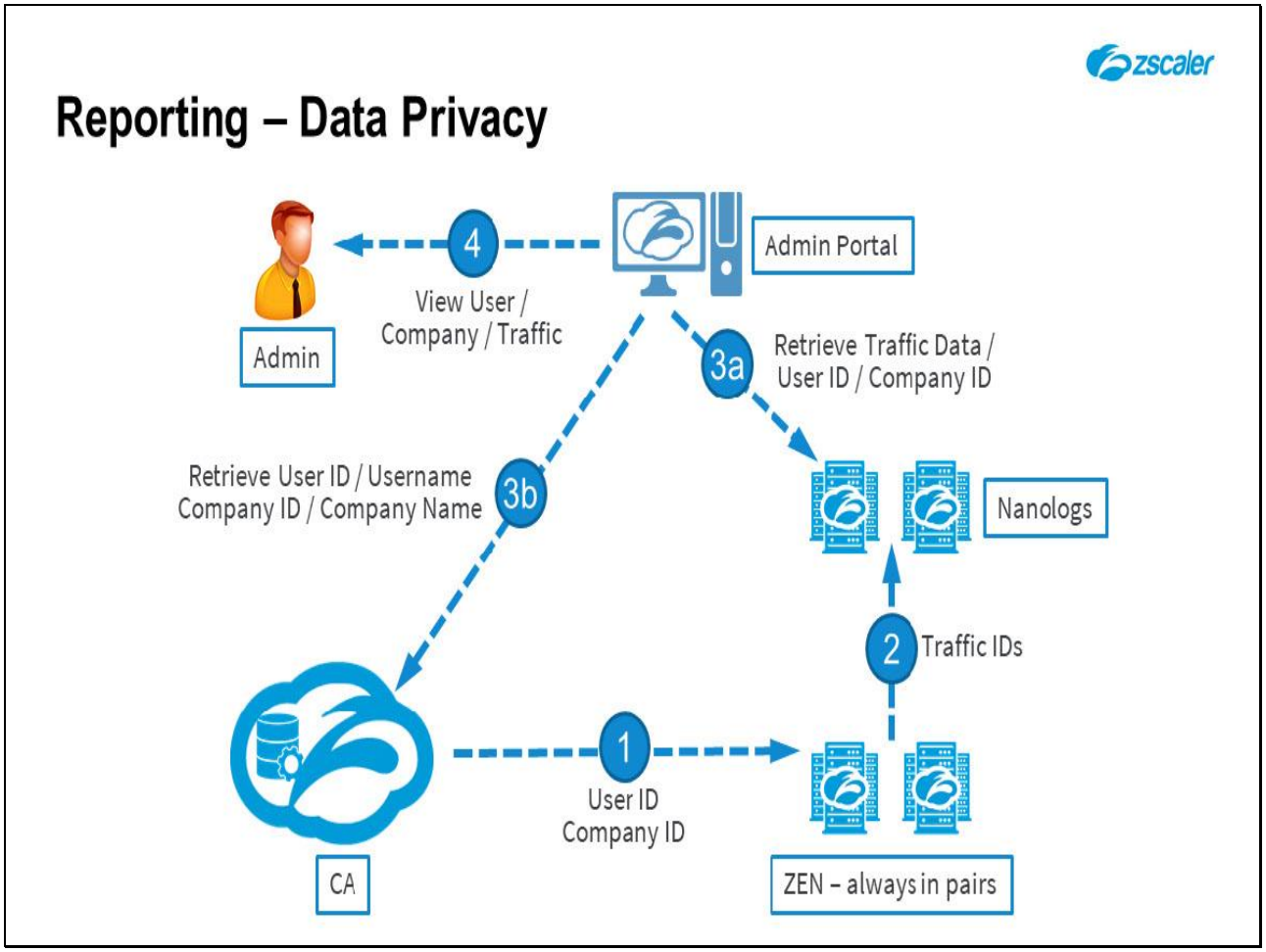
Slide 15 - Reporting – Data Privacy



Slide notes

b. The admin server retrieves the mapping of userID to their actual values from the CA only for the users who have that privilege

Slide 16 - Reporting – Data Privacy



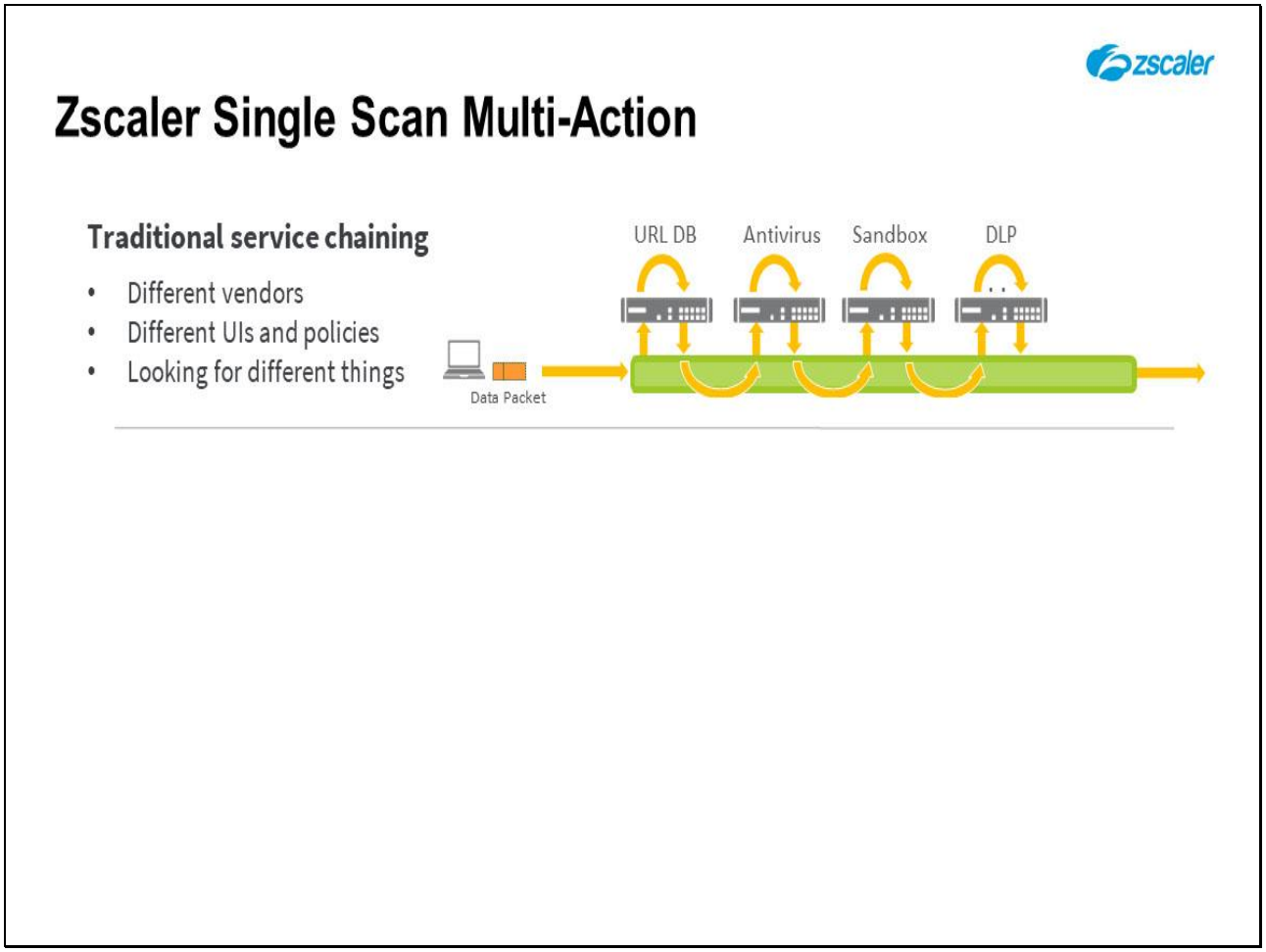
Slide notes

All transactions happen over SSL and the data itself is in a format that is not humanly legible. Logs are stored in compressed format. They are effectively meaningless by themselves.

Slide 17 - Single-Scan, Multi-Action (SSMA)

Slide notes

Slide 18 - Zscaler Single Scan Multi-Action



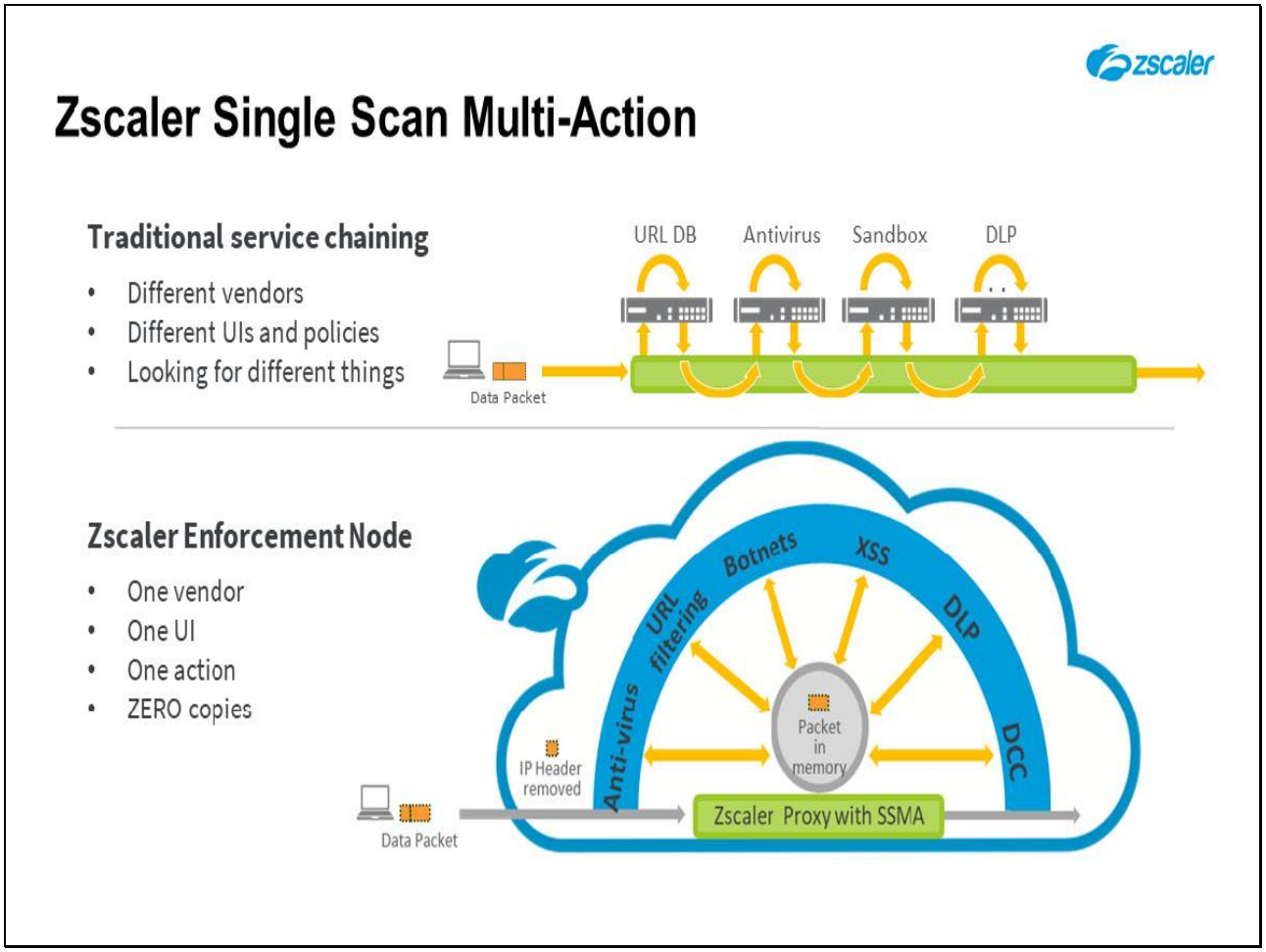
Slide notes

At this point you might be thinking, Ok, but how are you that fast and do everything? Before we talk about how Zscaler does it, let's look at how the traditional method works. For anything beyond basic URL filtering, all other vendors use what's called a service chain. Whether that means box to box, virtual machine to virtual machine, or process to process it's still a chain.

So traffic comes in and you go and look up a database for URL filtering. Then the AV engine, then the AS engine, then the Phrase matching and so on and so forth and then finally you go out to the internet. This is done because most of these systems are only loosely coupled. If you look at the world outside Zscaler they have all grown through acquisition which means different company's engines are running there.

Each one does all of the work of the TCP handling, Authentication, Connection ID, all of that all over again each time. That is wasteful and adds a lot of latency.

Slide 19 - Zscaler Single Scan Multi-Action

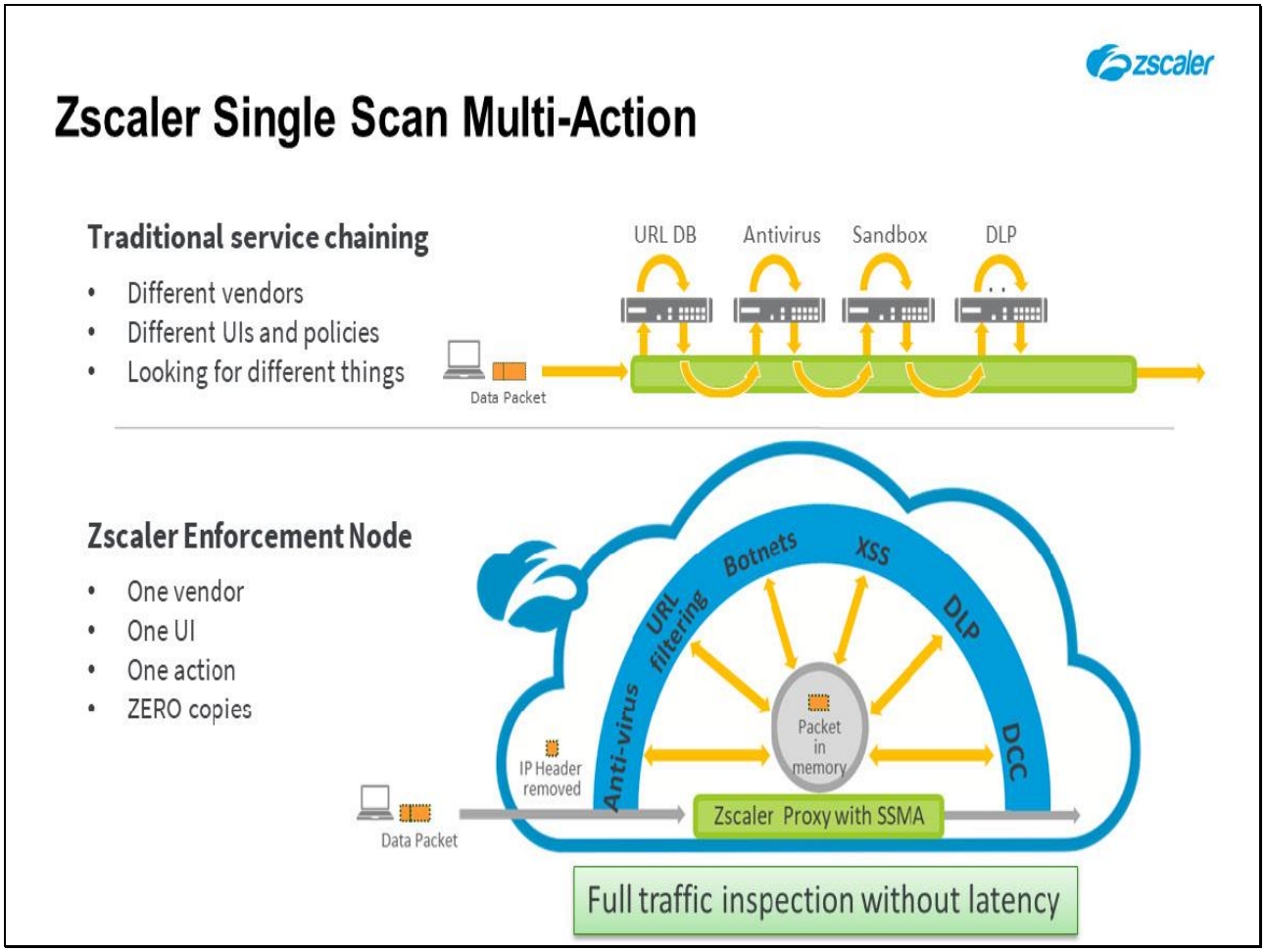


Slide notes

With Zscaler the architecture is very different. When packets come in, they get placed into a massive shared memory. We're in a 64-bit world and so every processor can address the entire memory now. This allows all of the CPU's to run in parallel, each one with a dedicated function. For example, there is one CPU that is dedicated to doing the Proxy/NAT function.

It's basically creating the IP stack and IP information, changes the source IP, redoes all the checksums, and then the packet is ready to be sent. At the same time the AV engine, the URL filtering engine, the cloud application classification engine, and all the rest of them are scanning through the packet and calculating their own results. Once the results are ready, we cross-check that against the user's policy and decide Allow or Block.

Slide 20 - Zscaler Single Scan Multi-Action



Slide notes

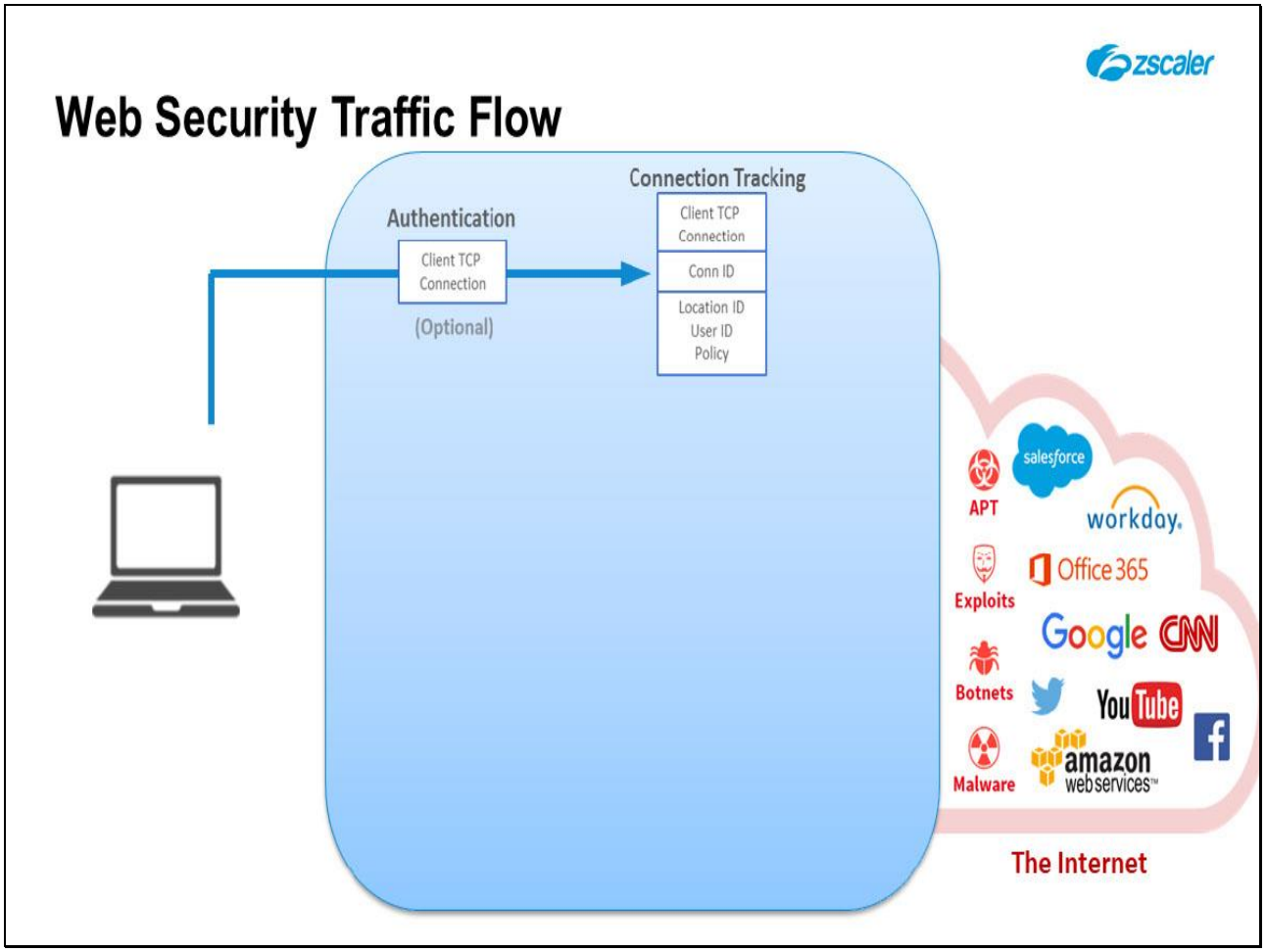
Because all of these engines are running in parallel, it makes it very very fast for us to be able to compute the results of what needs to be done. There are 2 other things that are very interesting in this architecture. All of those engines are running regardless of your policy and regardless of your subscription. So even if you have just URL filtering, all engines run on all your content and you will actually see that in your reporting.

You'll get reports for everything regardless of your subscription level. We did that because we are a service. We are not selling you a box and walking away. If a ZEN's performance starts changing based on how many knobs you turn on our Operations team would quit. We simply can't do that across 100 datacenters.

So Zscaler made an important strategic decision on Day 1 which is we don't care what your policy is, what your subscription is, we will always run every engine and we will scale our cloud to be able to do that. And once we are there then you don't worry when you turn on a new subscription. The other thing it does is once you decide that the code that we are writing for scanning are going to always run they get pinned in the L1 cache on the processor.

This means each CPU is doing the same thing over and over and over, so it operates almost like an ASIC. Every clock cycle we are retiring an instruction and there is no action to go to longer term memory or disk. We get tens of X of performance from just doing that because there is no interrupt. So that single-scan multi action is really the key for the performance numbers that we get.

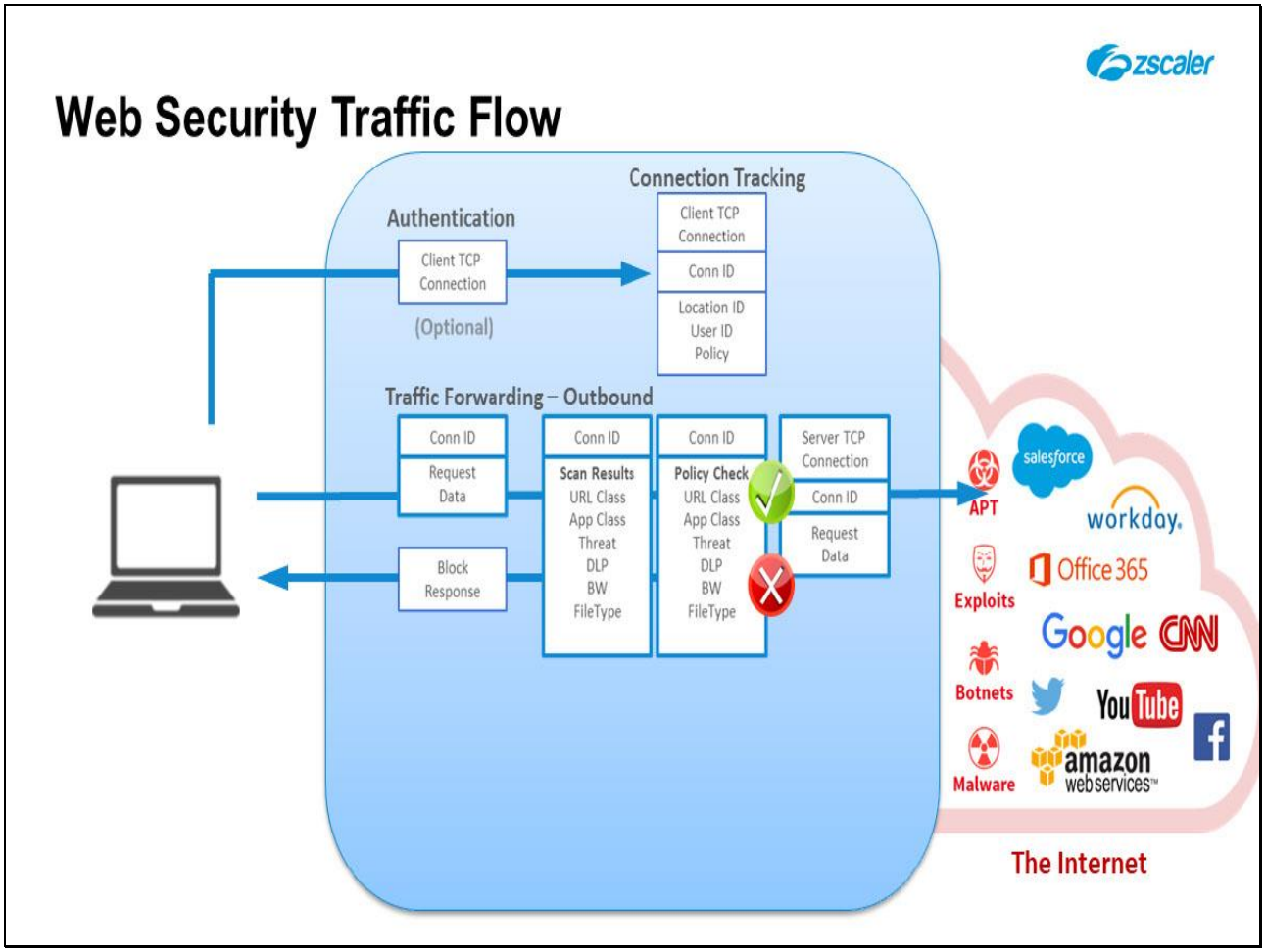
Slide 21 - Web Security Traffic Flow



Slide notes

This is a high-level diagram of how traffic flows through our system and which checks are engaged when. Our first step is to figure out who the user is and assign a connection ID.

Slide 22 - Web Security Traffic Flow

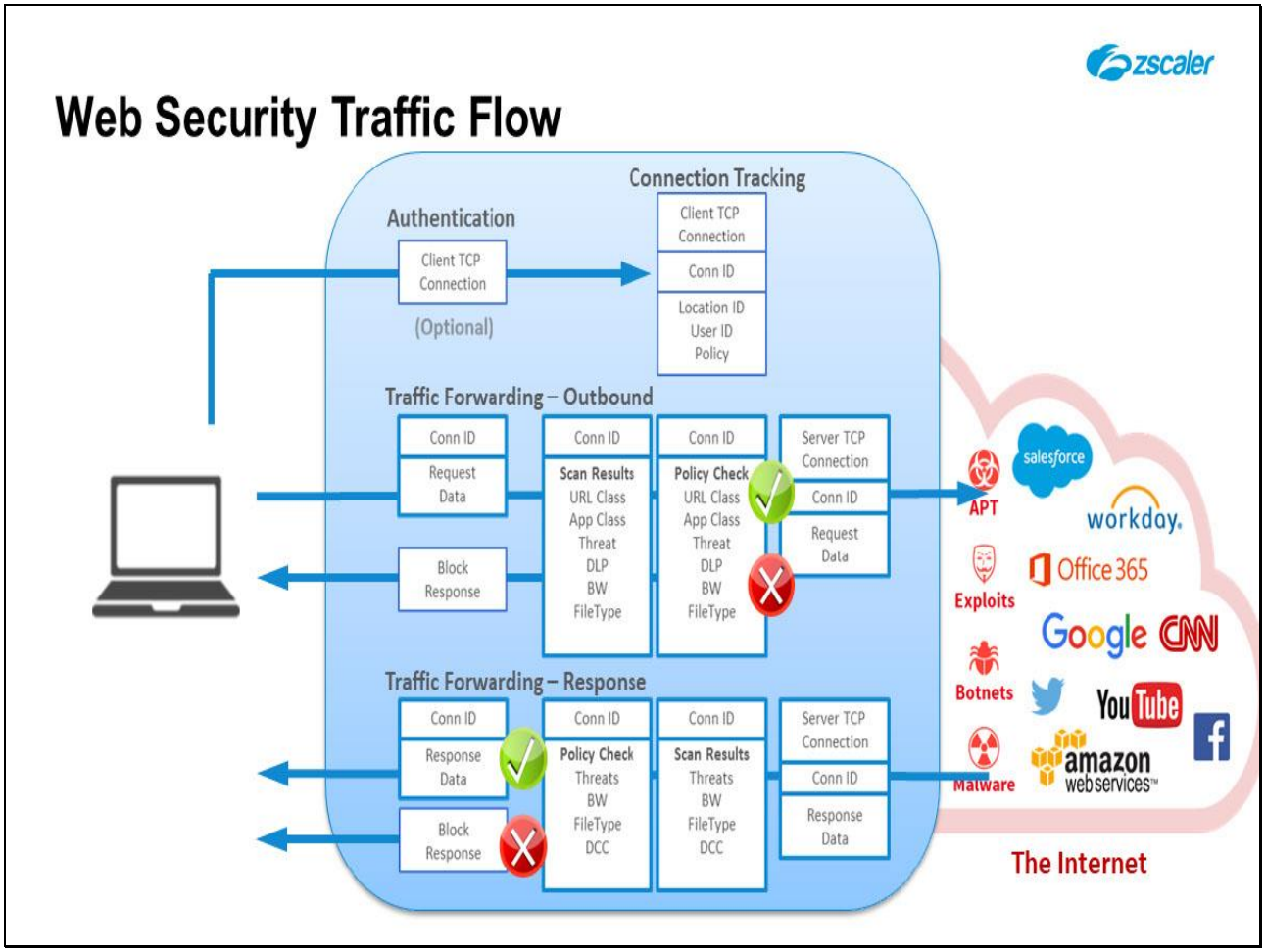


Slide notes

With the connection ID we'll request the policy and we'll do all the checks. If for instance you have a policy to block access to Gambling sites and the Connection is for a gambling site, we will block it right there and send a block response.

We will not set anything up on the content server side because we are a true proxy and we provide connection isolation. We look at policy and if policy doesn't allow it or if it's malicious then nothing goes out.

Slide 23 - Web Security Traffic Flow



Slide notes

When traffic comes back, we do the same thing with a different set of engines like BW/QoS, Dynamic content classification, etc and then if the policy checks out, we'll deliver the response back to the user.

There's one other aspect here and that is Denial of Service protection. Since you are relying on us for your Internet access, how can we make sure that we can survive an attack like that? We actually built a mechanism into our IP stack implementation. When a TCP connection comes in we figure out what the user ID is and the organization ID based on either authentication that has been done before or through federation.

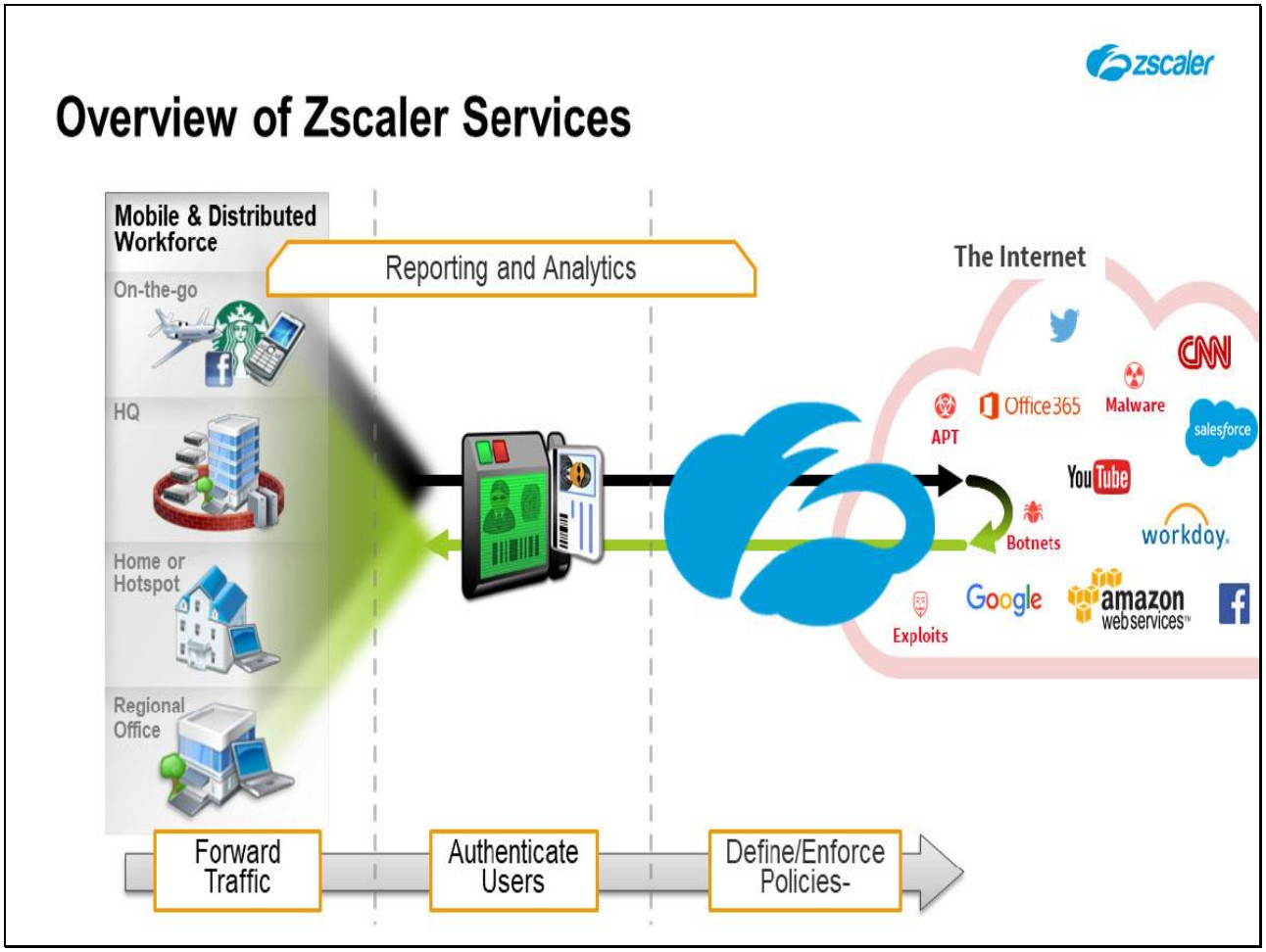
Once identity has been established that identity is used to figure out what policy needs to be enforced. That ID is how we track the session. This part is done from a run-time memory. If the connection ID is not created, we don't even allocate memory, so you can't DOS us right at the beginning. If you send us a SYN we send you a SYN ACK with a cookie and forget about you.

Until you send us an actual data packet with an authorization token, we allocate no memory. So that is a very important piece of the architecture.

Slide 24 - Traffic Forwarding and Authentication

Slide notes

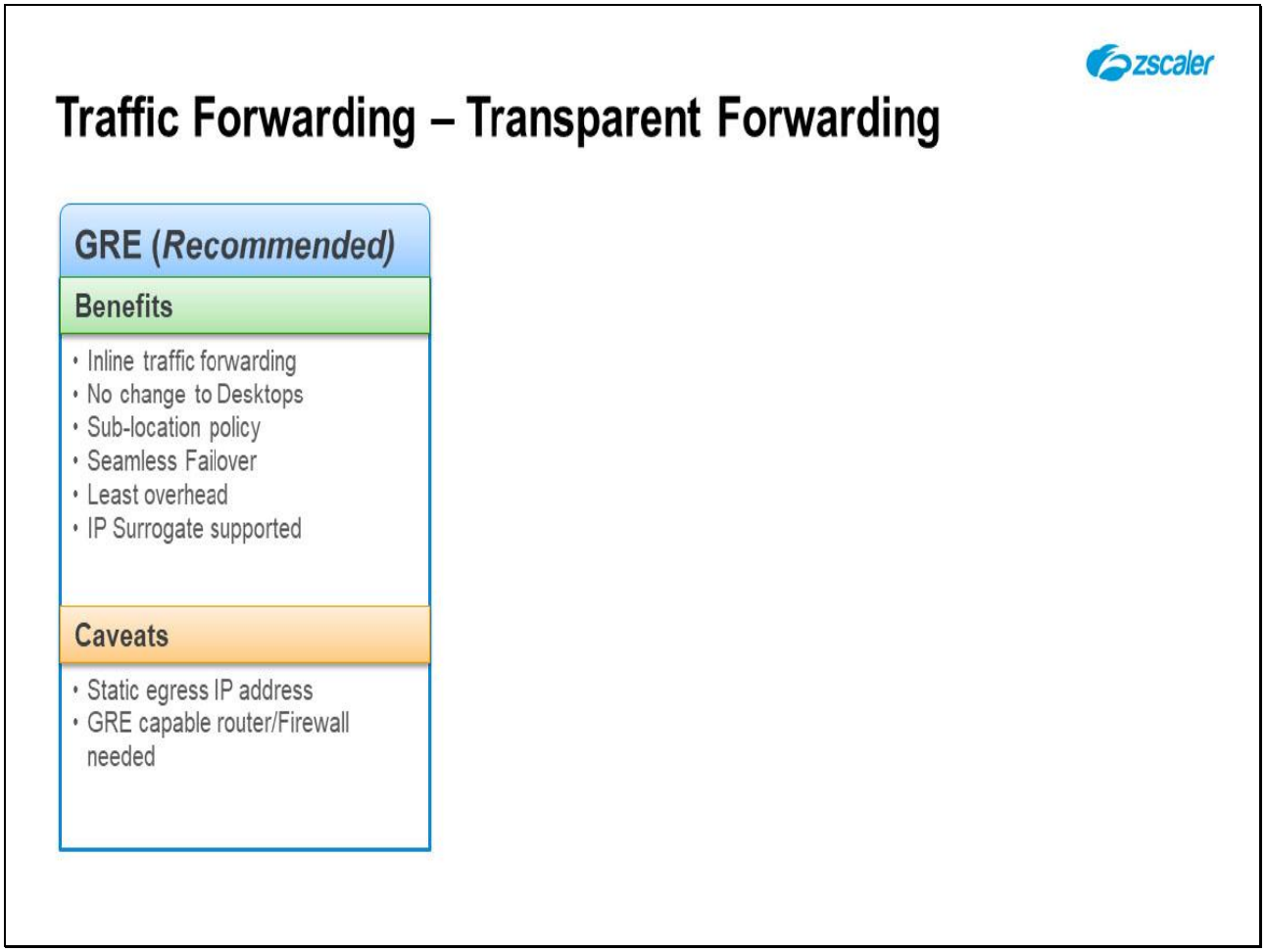
Slide 25 - Overview of Zscaler Services



Slide notes

When implementing Zscaler there are four main functional areas that must be considered: the forwarding of traffic to the Zscaler Cloud in the first place; whether or not to authenticate users; the configuration and application of all the available Policies, and their enforcement by us; and finally, the reporting and analytics capabilities of the system.

Slide 26 - Traffic Forwarding—Transparent Forwarding



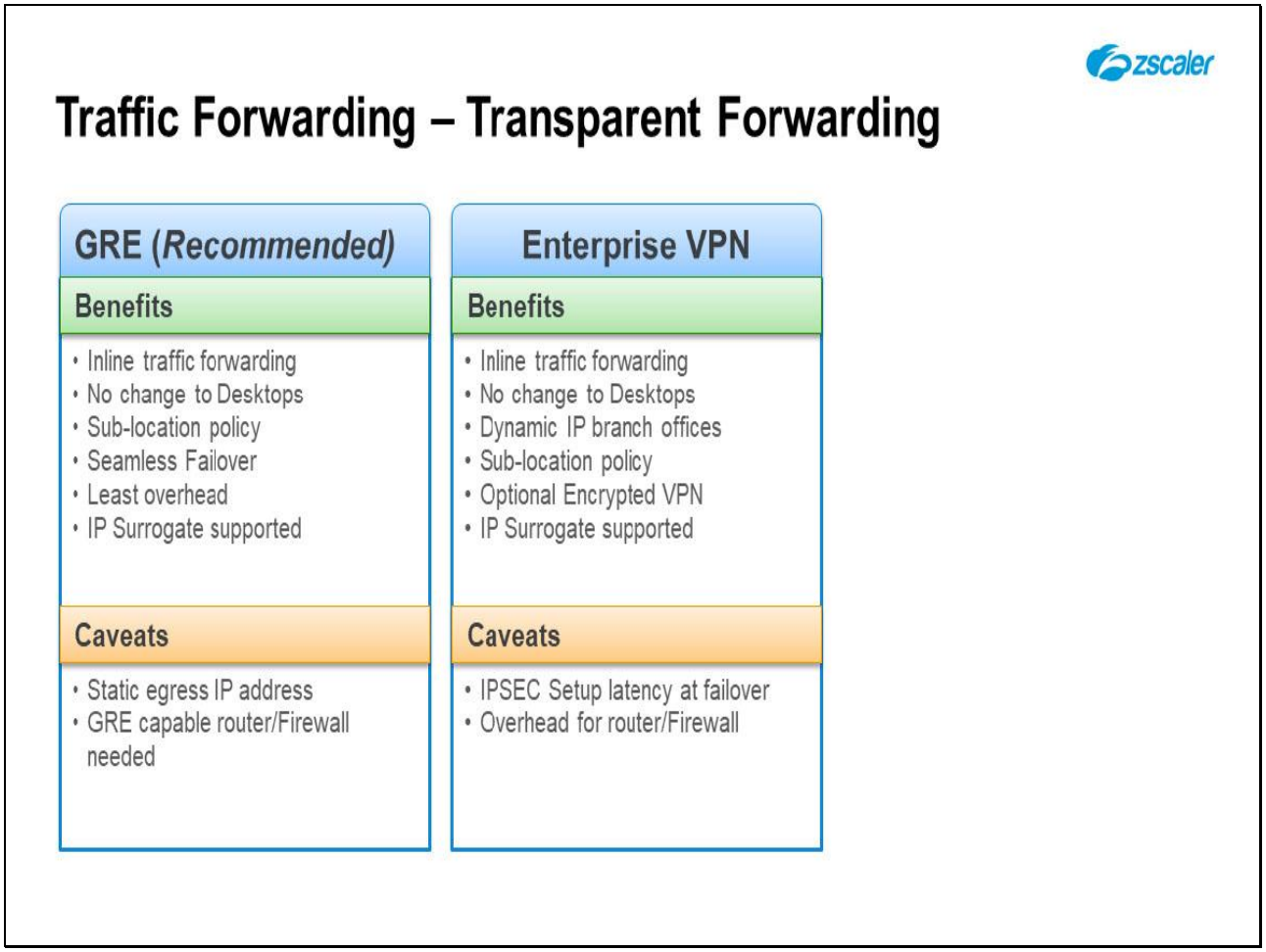
Slide notes

Traffic Forwarding options for Zscaler are numerous. The basic idea is to get traffic as it leaves your network into us before it goes to the Internet. Our recommended method of forwarding is to do a GRE tunnel from a router or a switch that is inside your NAT firewall. That way we are creating a tunnel where Zscaler has visibility into your internal IPs.

This allows us to give you much better reporting as well as the ability to set policy by subnet for Internet of Things applications. We can also give you much more capabilities in terms of bandwidth quality of service controls or identity federation that all benefit from internal IP visibility. We are a full proxy firewall DMZ so your IPs are never exposed outside.

When you set up your GRE tunnels, we recommend setting up IP SLA alongside the GRE tunnel that monitors the health for that tunnel. The failover for GRE is instantaneous because there is no handshake. If you failover from one DC to another it's literally a couple of seconds and you're back online.

Slide 27 - Traffic Forwarding – Transparent Forwarding

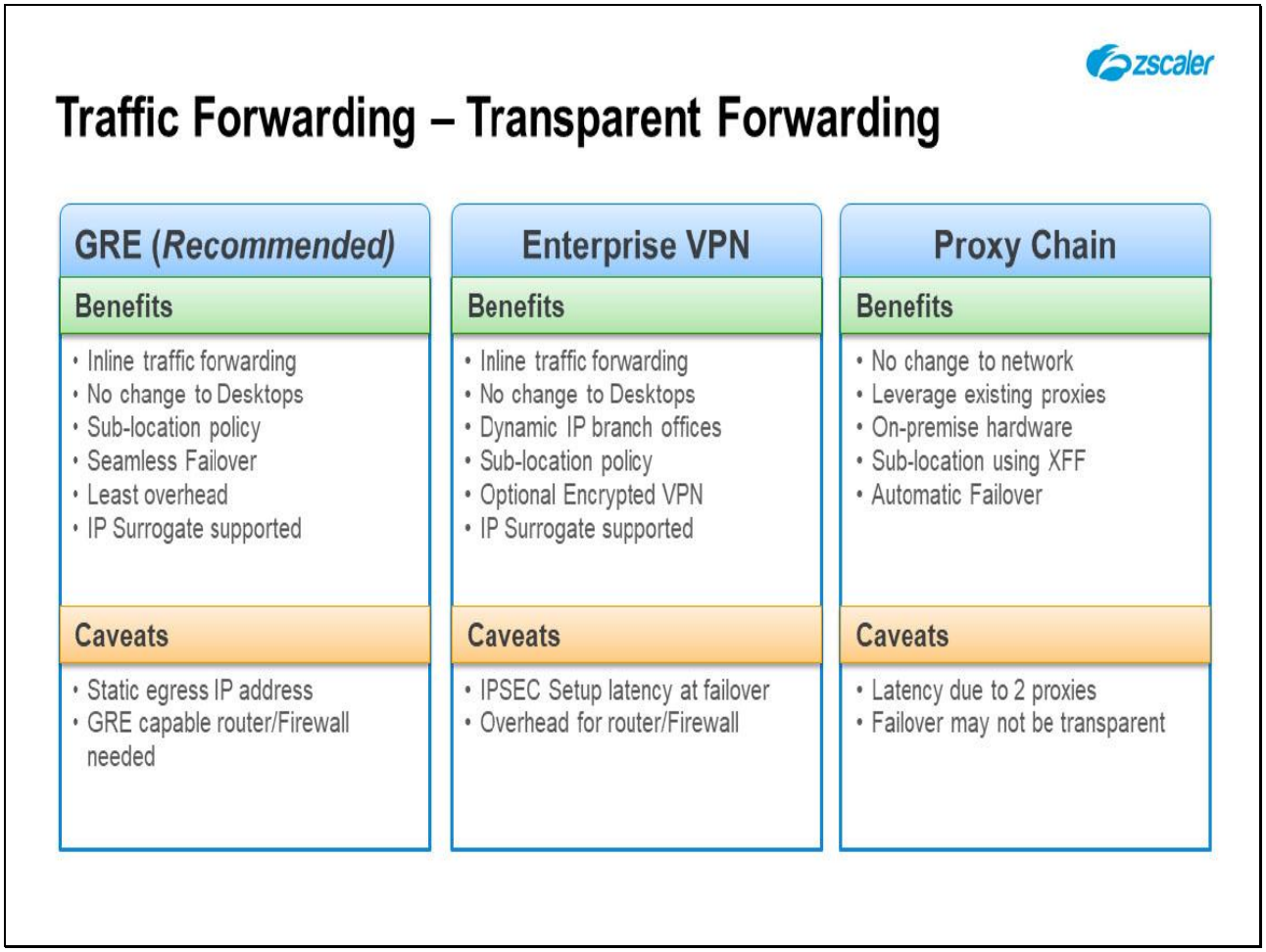


Slide notes

In places where you don't have equipment to do GRE or you have dynamic IP addresses because you have a small branch then we support IPSec VPN.

You would build a VPN connection from your branch firewall to Zscaler that becomes your default route to the internet and all traffic comes to us.

Slide 28 - Traffic Forwarding – Transparent Forwarding

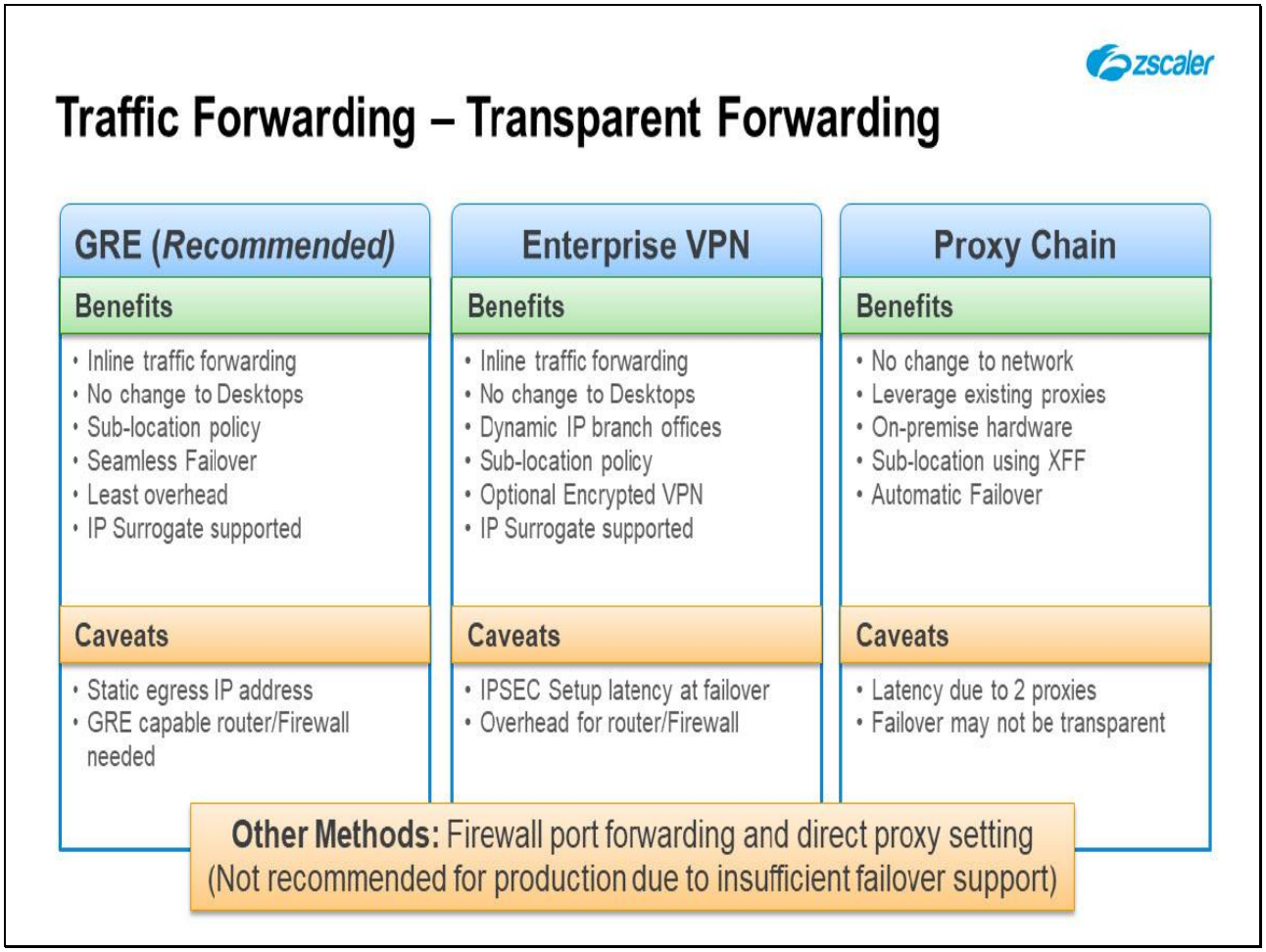


Slide notes

Lastly if you are using Zscaler as an extra layer of security on top of your existing solution, you can set up a Proxy Chain. Setting up a proxy chain requires 2 minutes and you are online with a much higher level of security. But depending on your existing proxy failover may not be transparent.

Generally, we recommend GRE because GRE has lower overhead on both your routers and our side. And we can scale those tunnels much faster.

Slide 29 - Traffic Forwarding – Transparent Forwarding

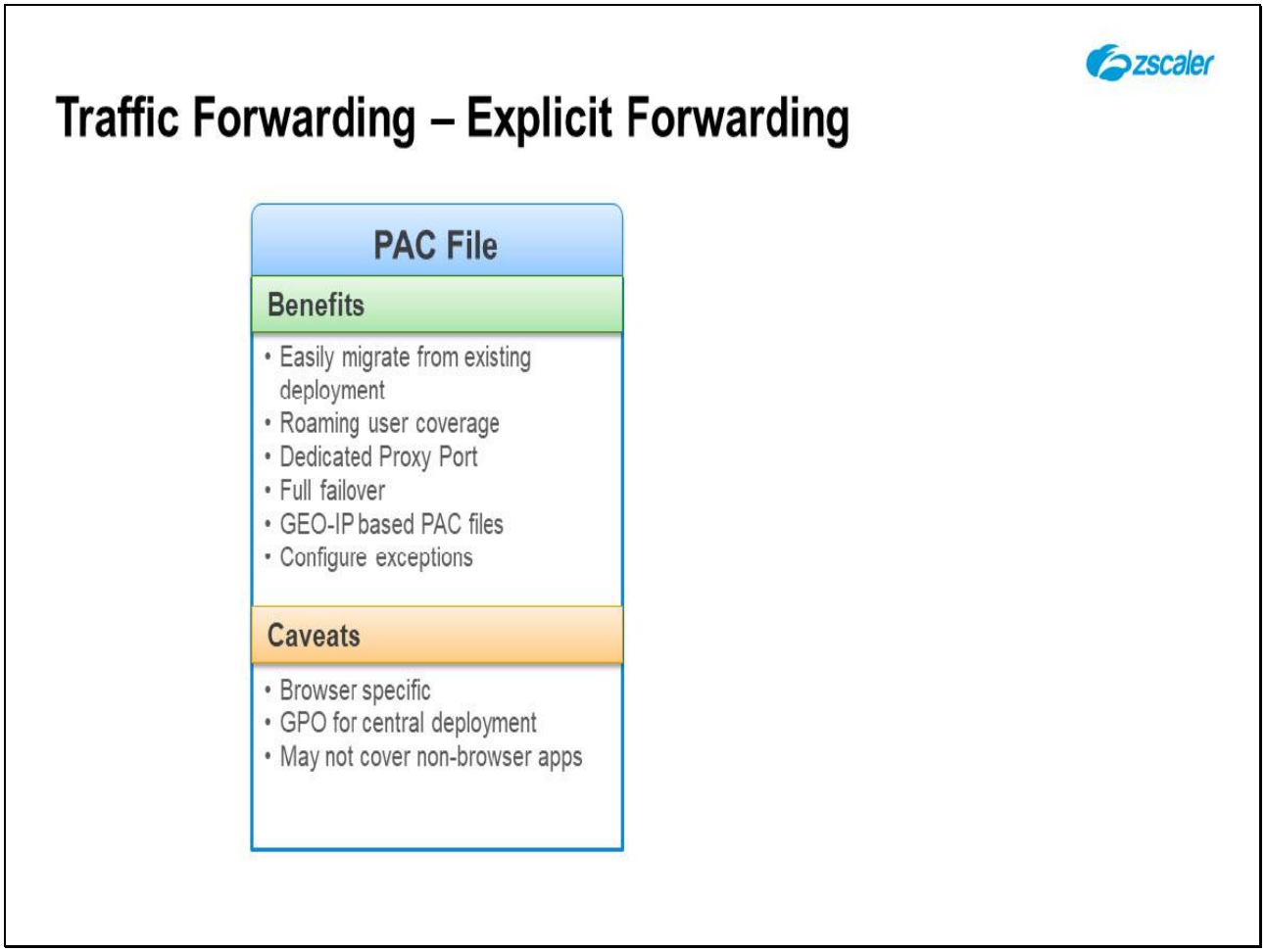


Slide notes

In terms of other methods, we do support FW port forwarding or directly setting proxies on your systems. We don't recommend doing that for production because they don't have great failover capabilities. Nothing to do with Zscaler, just based on the technologies.

If you want to do FW port forwarding you can but we can't give you an uptime SLA.

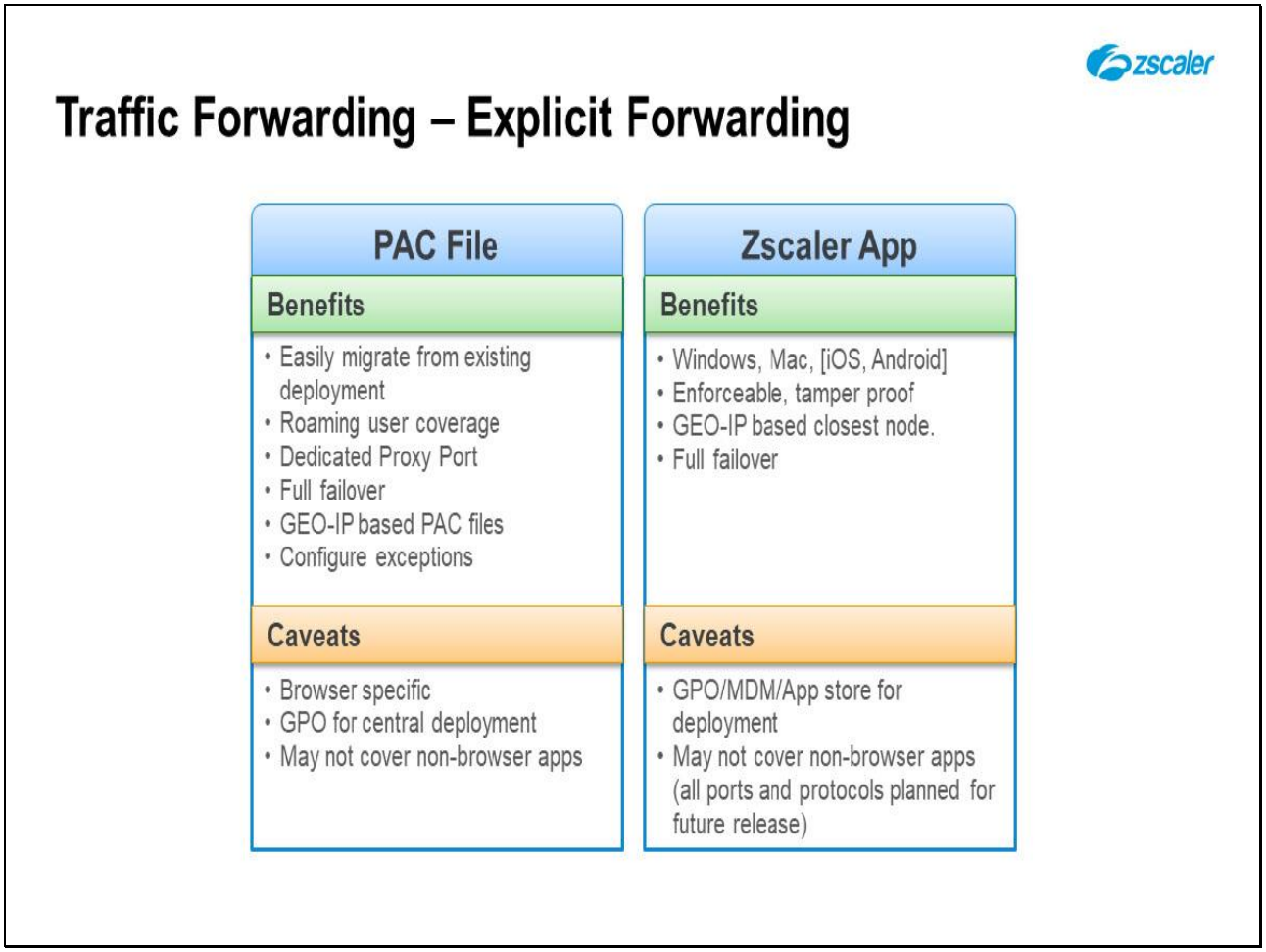
Slide 30 - Traffic Forwarding—Explicit Forwarding



Slide notes

The previous slide listed the transparent traffic forwarding methods for use at your physical sites. When users are not at work the way traffic comes to us is by using a PAC file or using the Zscaler App. The downside of PAC files is that it may not cover applications that are not browser compliant.

Slide 31 - Traffic Forwarding – Explicit Forwarding

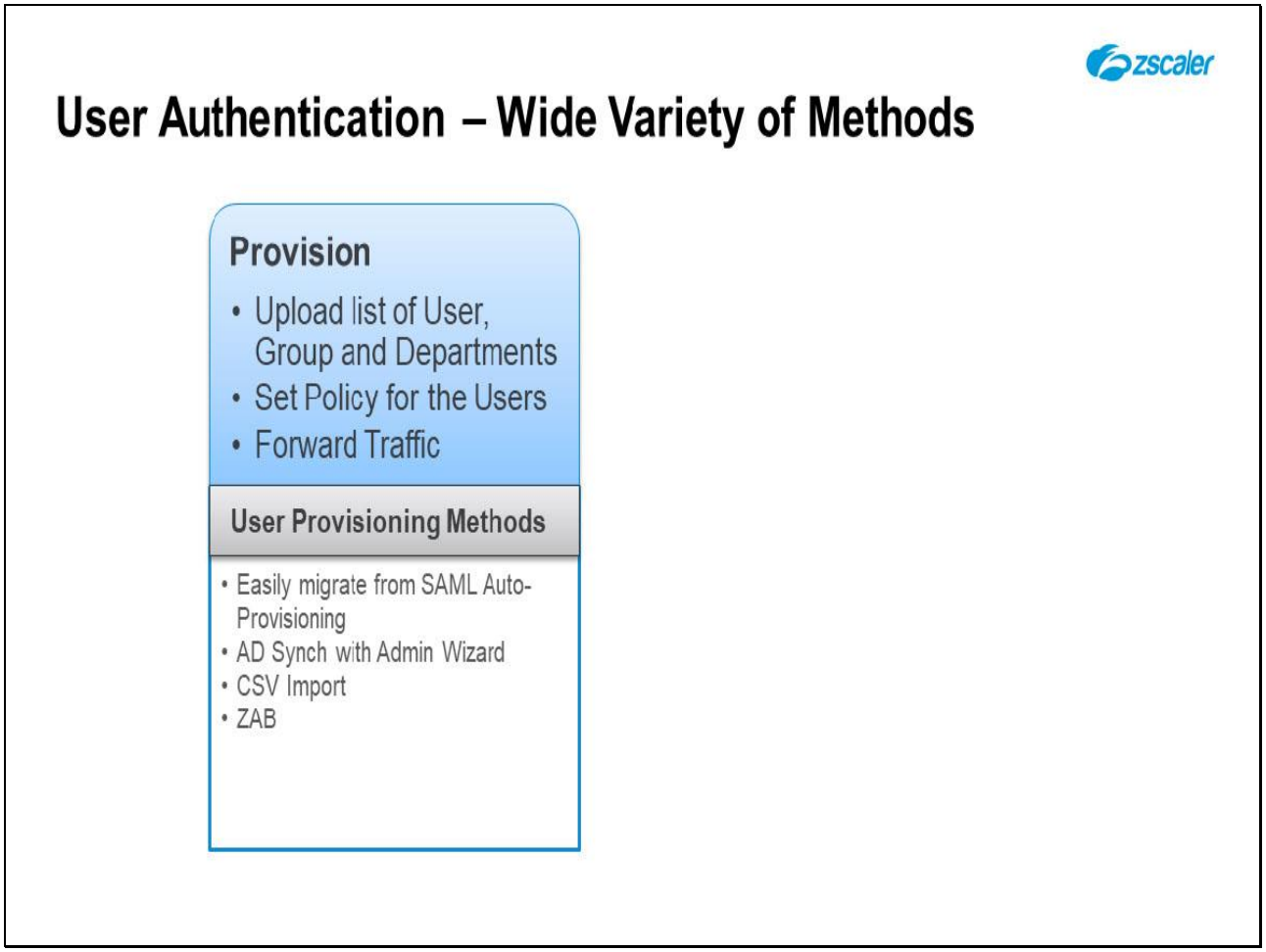


Slide notes

There are very few of them now but that is a clear possibility and so if you're worried about that you can use our App. It creates a tunnel at the network level so whether the application cares about PAC files or not it doesn't matter, all Web traffic comes to Zscaler regardless. The Zscaler App is also available for iOS and Android devices.

In addition to these if you are being provisioned by a carrier, the carrier can do an MPLS handoff from their PE router to us. If you have a private or virtual ZEN, you can put that ZEN in L2 mode right next to your router and that works too. At the end of the day there are a lot of options to get traffic into Zscaler.

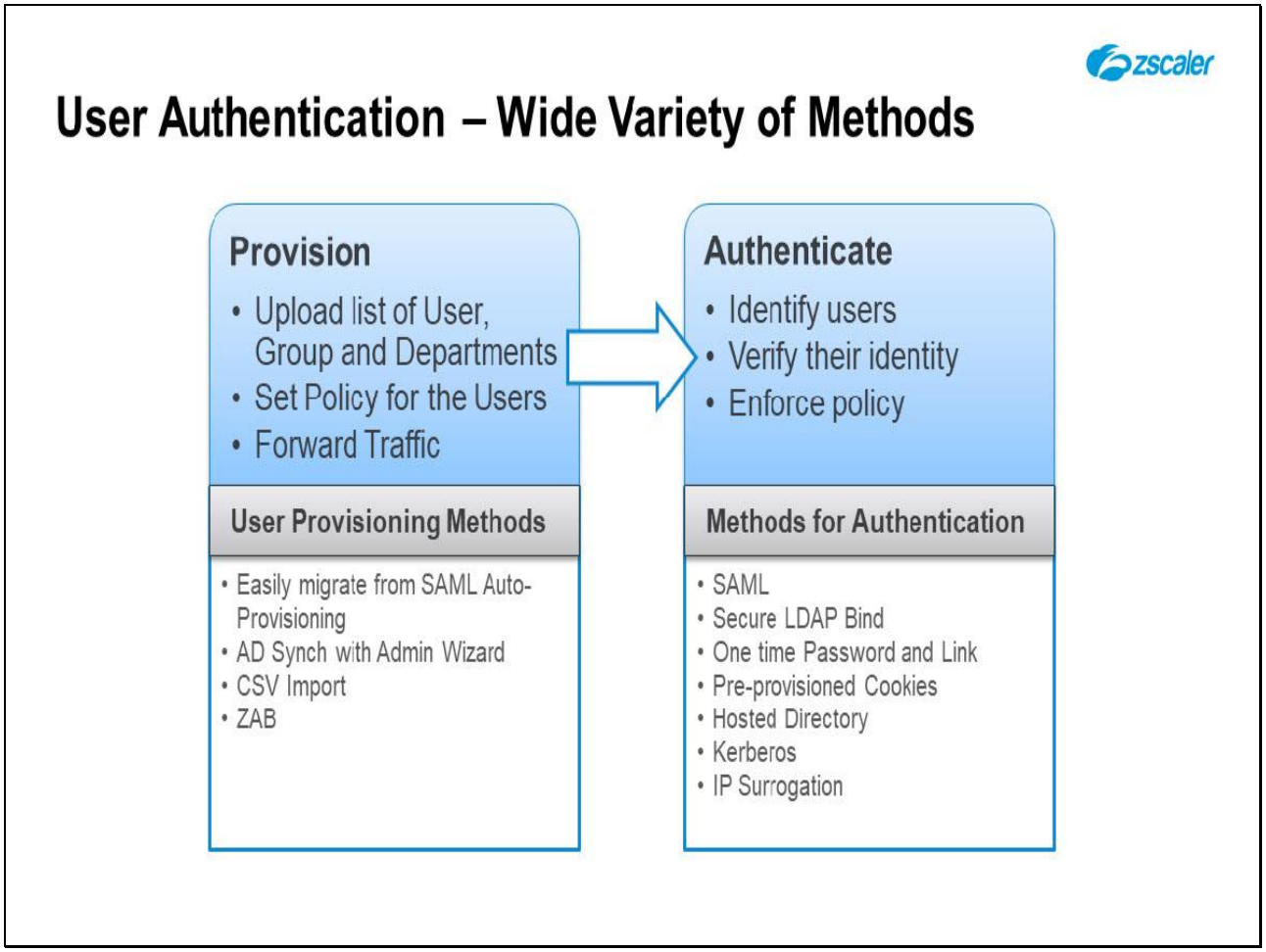
Slide 32 - Wide variety of Authentication Methods



Slide notes

Once your traffic starts flowing to us the next step is to figure out who the users are in order to apply policies and for reporting. We look at authentication as 2 steps. There is provisioning, which means letting the cloud know who the users are and what types of groups and departments exist.

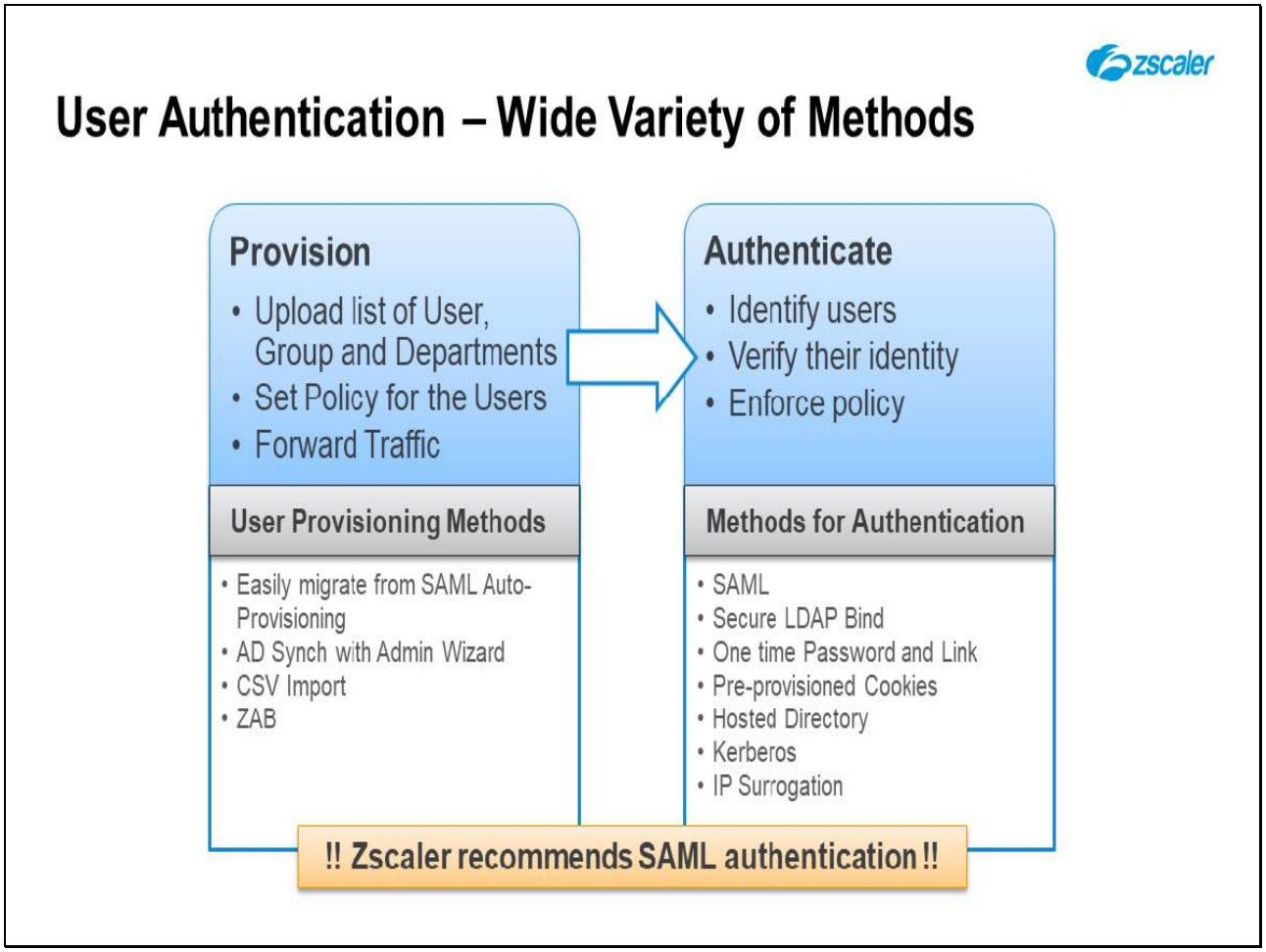
Slide 33 - User Authentication – Wide Variety of Methods



Slide notes

Then there is doing actual authentication of the users when they are going out to the internet. There are multiple ways of provisioning your information into the cloud and there are multiple ways to authenticate. Our recommended way to do authentication as well as provisioning is to use SAML.

Slide 34 - User Authentication – Wide Variety of Methods



Slide notes

SAML is an authentication mark-up language but we can also use it for provisioning. The way SAML works is when a user is going out to the internet and we don't know who it is we send a redirect to their Identity Provider or IdP.

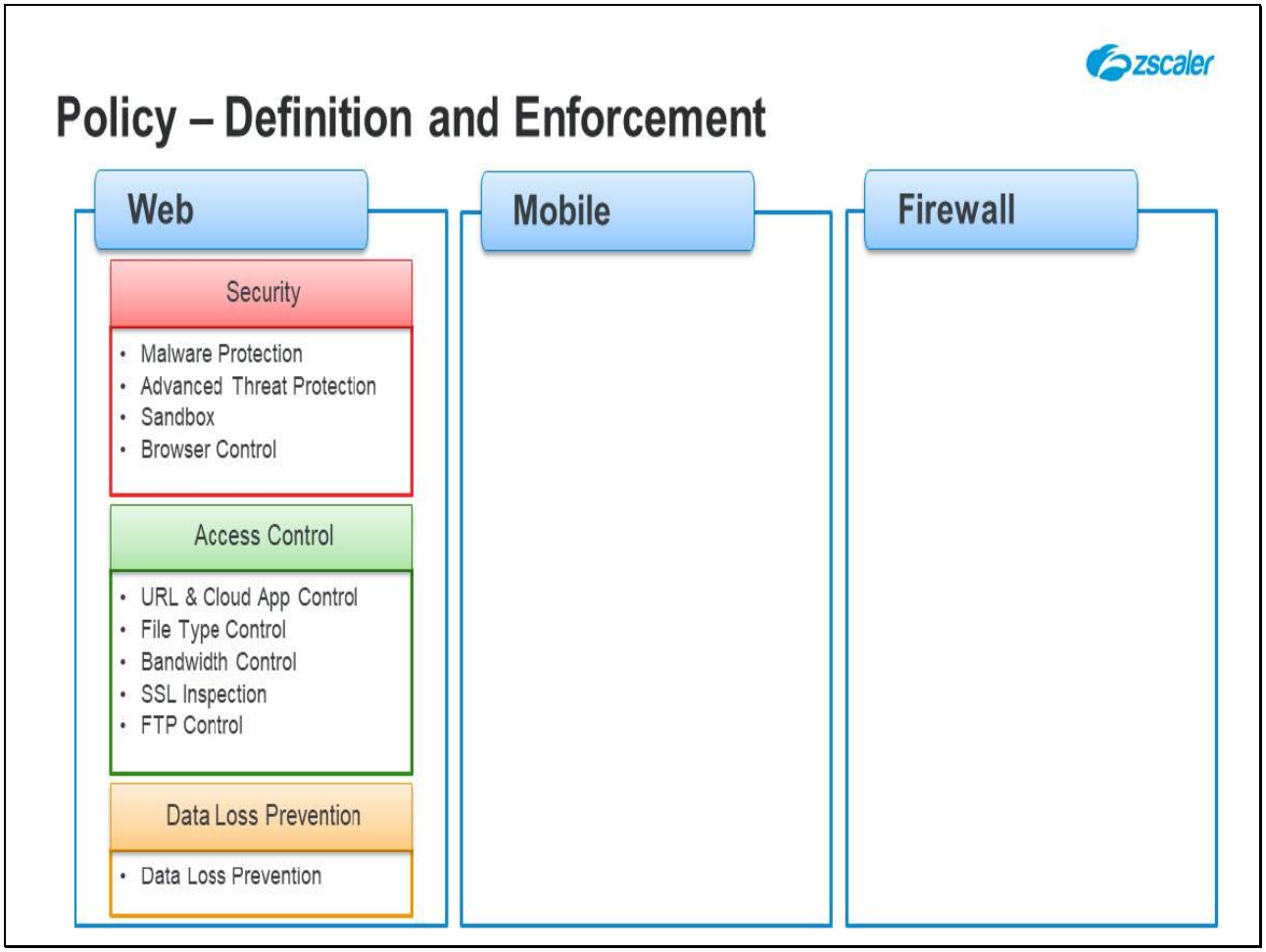
The IdP figures out who the user is and sends an assertion to Zscaler with the user, group, and department information. When we see that assertion, we use it not only to authenticate but also to provision if the user group, or department doesn't already exist in our database. So it simplifies your deployment tremendously. You can simply point to the ID federation system, turn it on, and it starts working.

Now in addition to that we can absolutely do the regular LDAP BIND and LDAP sync approach. We also provide an authentication bridge that sits on your network that will do the auth and sync to the cloud if you don't want to open up firewalls for us to sync from your AD directly. So you can put a Virtual Machine in your DMZ that will sync from your local AD and send that user information to the cloud.

For smaller companies or if you have a different requirement you can always import CSVs of everything and/or use our hosted DB. You could do one-time password and a link, similar to what you get with guest WiFi. You could do pre-provisioned cookies which are mostly used for kiosks that people are not going to log in individually.

You can create the accounts up front, generate all the auth cookies, and then deploy them in the local object stores and then no one has to authenticate again. We also allow you to do full Kerberos auth. Once you do the AD sync, instead of doing an LDAP Bind which is form-based authentication, you can use window's native capability with Kerberos. And we support Kerberos for people at work as well as road warriors.

Slide 35 - Policy – Definition and Enforcement



Slide notes

The Policy configuration area can be found by clicking on the **Policy** menu in the admin portal. The **Policy** menu is then broken down into the **Web**, **Mobile**, and **Firewall** areas. The **Web** policy area is the most extensive and allows the creation of **Security**, **Access Control**, and **Data Loss Prevention** policies.

The **Security** policies available to be configured are: **Malware Protection**, for configuring protection from viruses, Trojans, Worms, Adware, Spyware and other unwanted applications; **Advanced Threat Protection** (ATP), to detect and block malicious activity, spyware call-backs, or command and control traffic (CC);

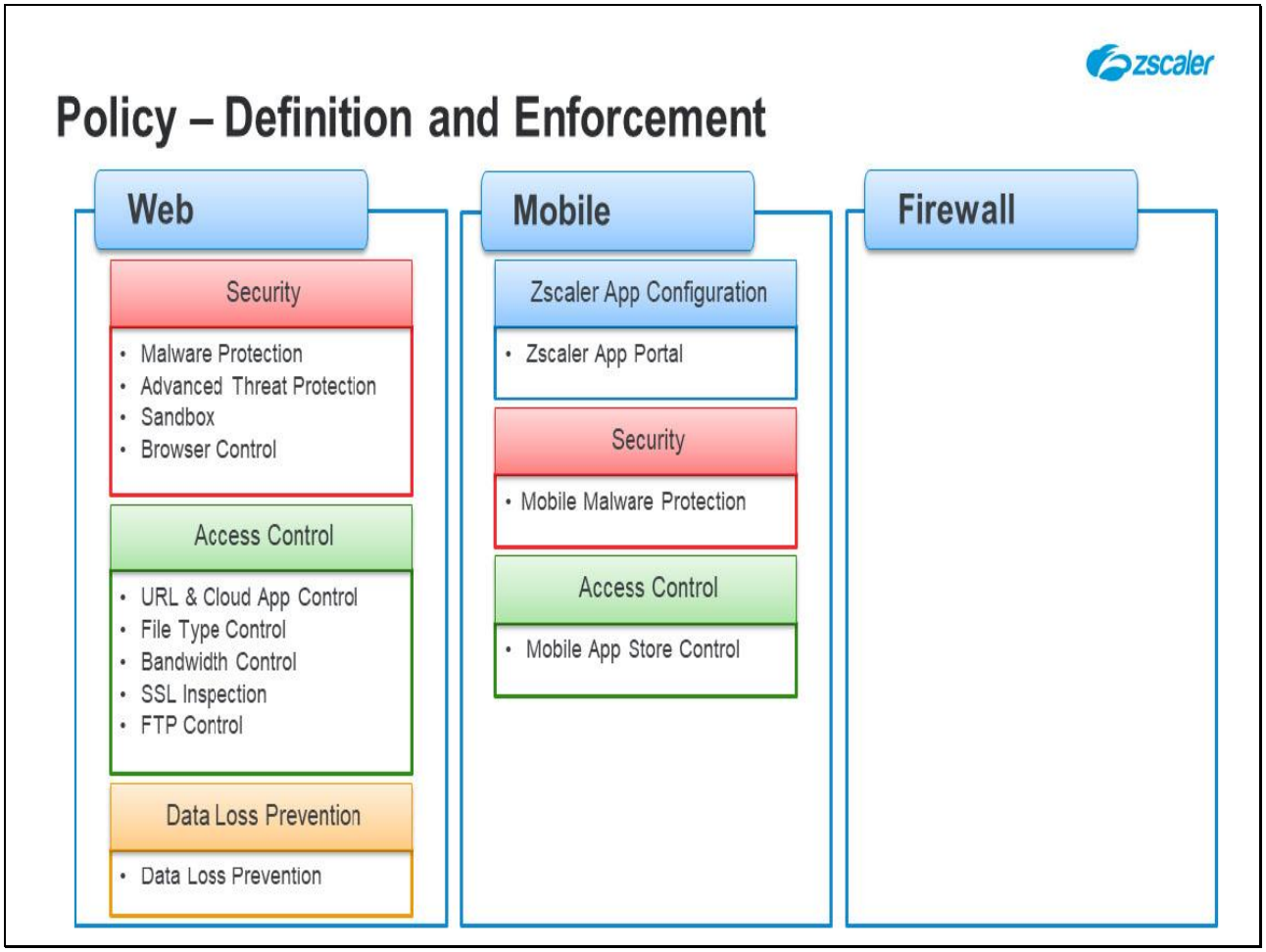
Cloud Sandbox, that allows the quarantining of suspect files for scanning in a protected sandbox environment; and **Browser Control**, that allows the specification of minimum Browser versions, and Browser vulnerability protections.

The **Access Control** policies available are: **URL & Cloud App Control**, that can be used to control access to destination Websites or applications; **File Type Control**, to specify the file types that may be uploaded, or downloaded; **Bandwidth Control**, for assigning maximum, and minimum bandwidth percentages for classes of traffic.

SSL Inspection, with settings and resources for intercepting and inspecting SSL traffic; and **FTP Control**, for restricting access using the FTP protocol.

The **Data Loss Prevention** policy area allows the creation of policies to monitor, and if necessary block, the unauthorized exfiltration of data using Zscaler internal, or external DLP engines. It also allows the streaming of data to an on-site ICAP server for analysis.

Slide 36 - Policy – Definition and Enforcement

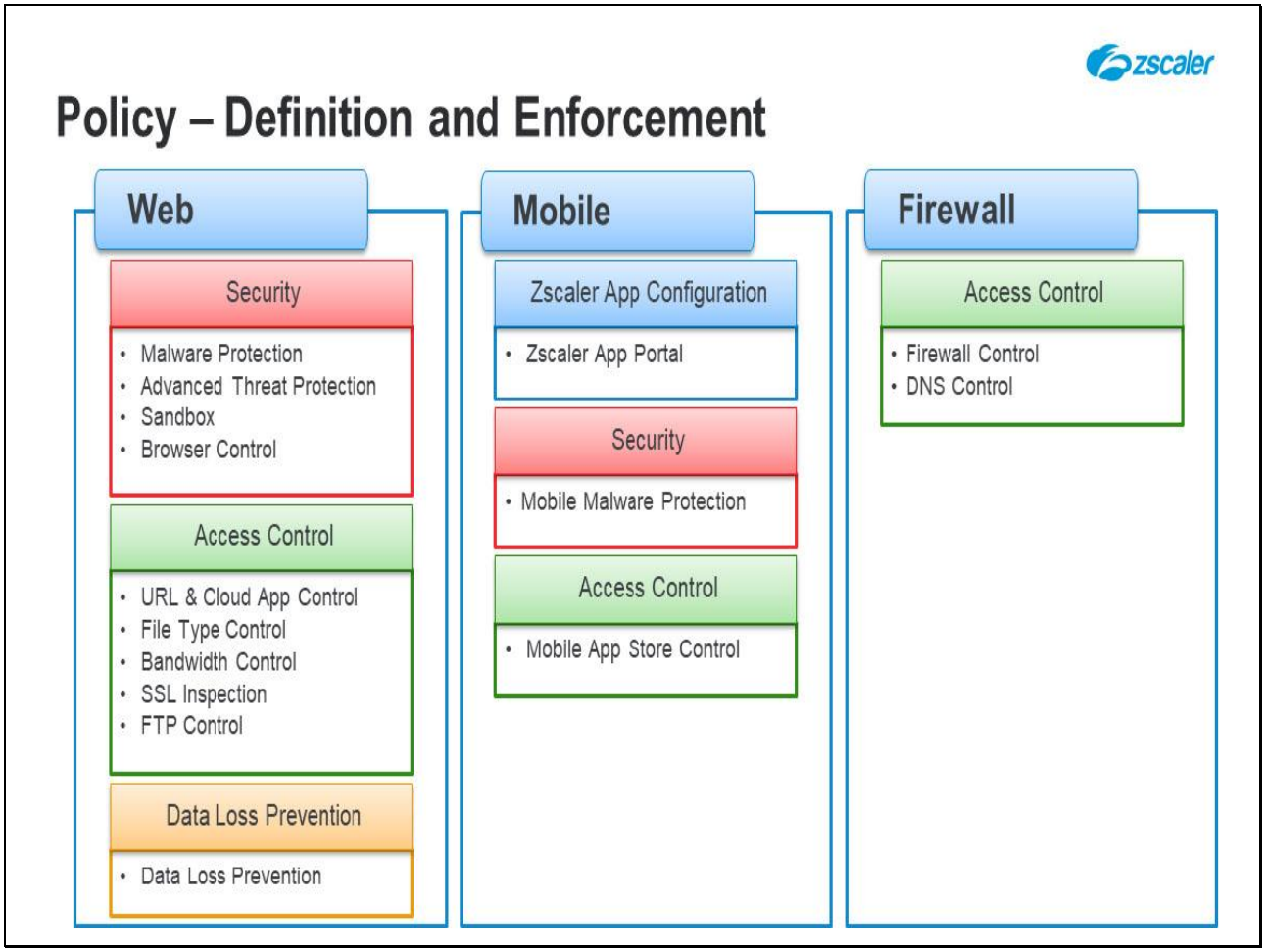


Slide notes

The **Mobile** policy area also has three policy categories; **Zscaler App Configuration**, **Security**, and **Access Control**. The **Zscaler App Configuration** category contains a link to the Zscaler App Portal, where configurations and policies for the Zscaler App, and secure agent for mobile can be defined.

The **Security** category contains the ability to setup a policy for **Mobile Malware Protection**, and the **Access Control** category allows the definition of policy rules for **Mobile App Store Control**.

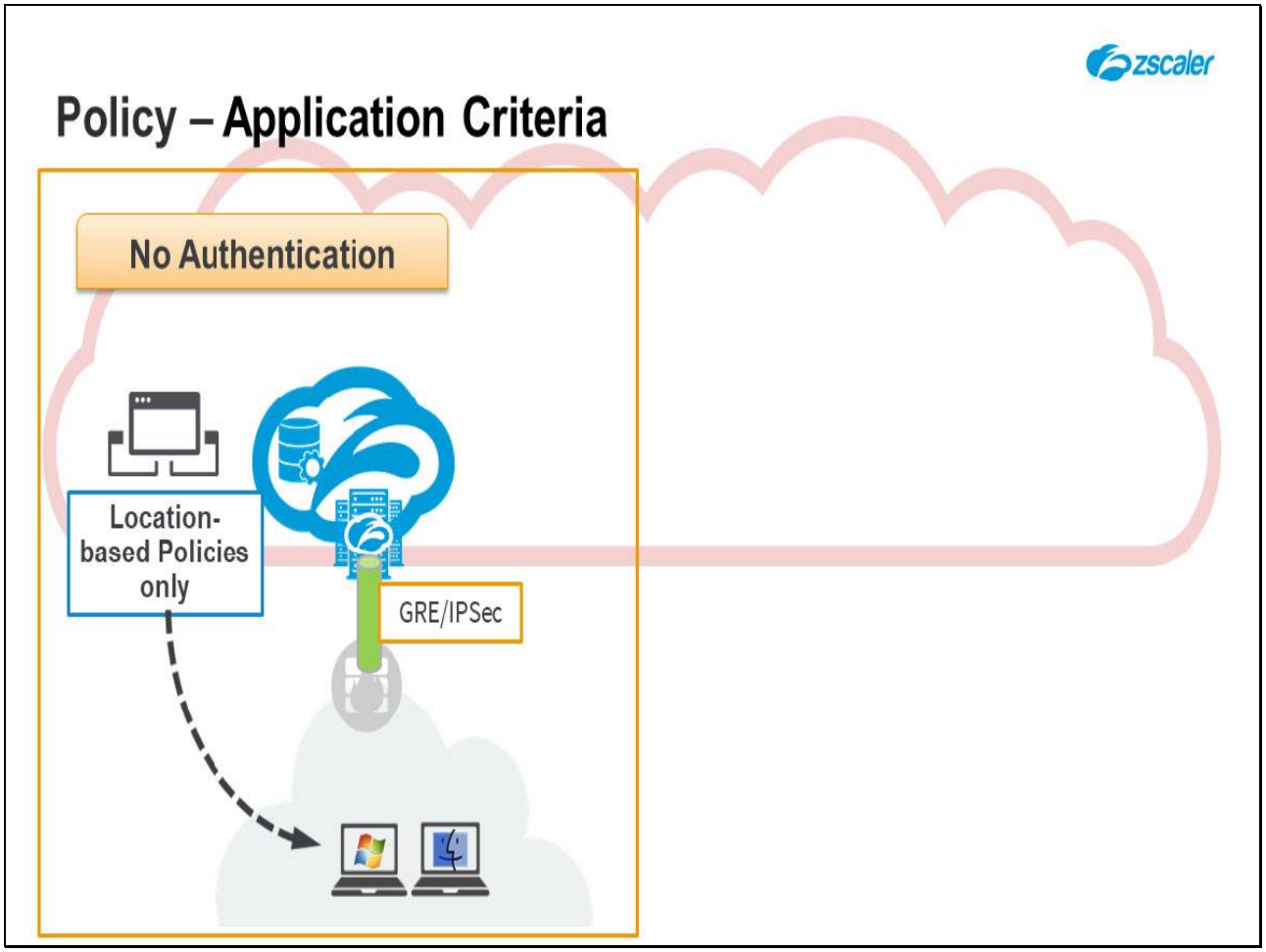
Slide 37 - Policy – Definition and Enforcement



Slide notes

TThe **Firewall** area contains **Access Control** policies allowing the configuration of **Firewall Control**, or **DNS Control** policies. Note that the **Firewall** policy configuration is for both the Basic, and Next Generation Firewall configuration, depending on your subscription.

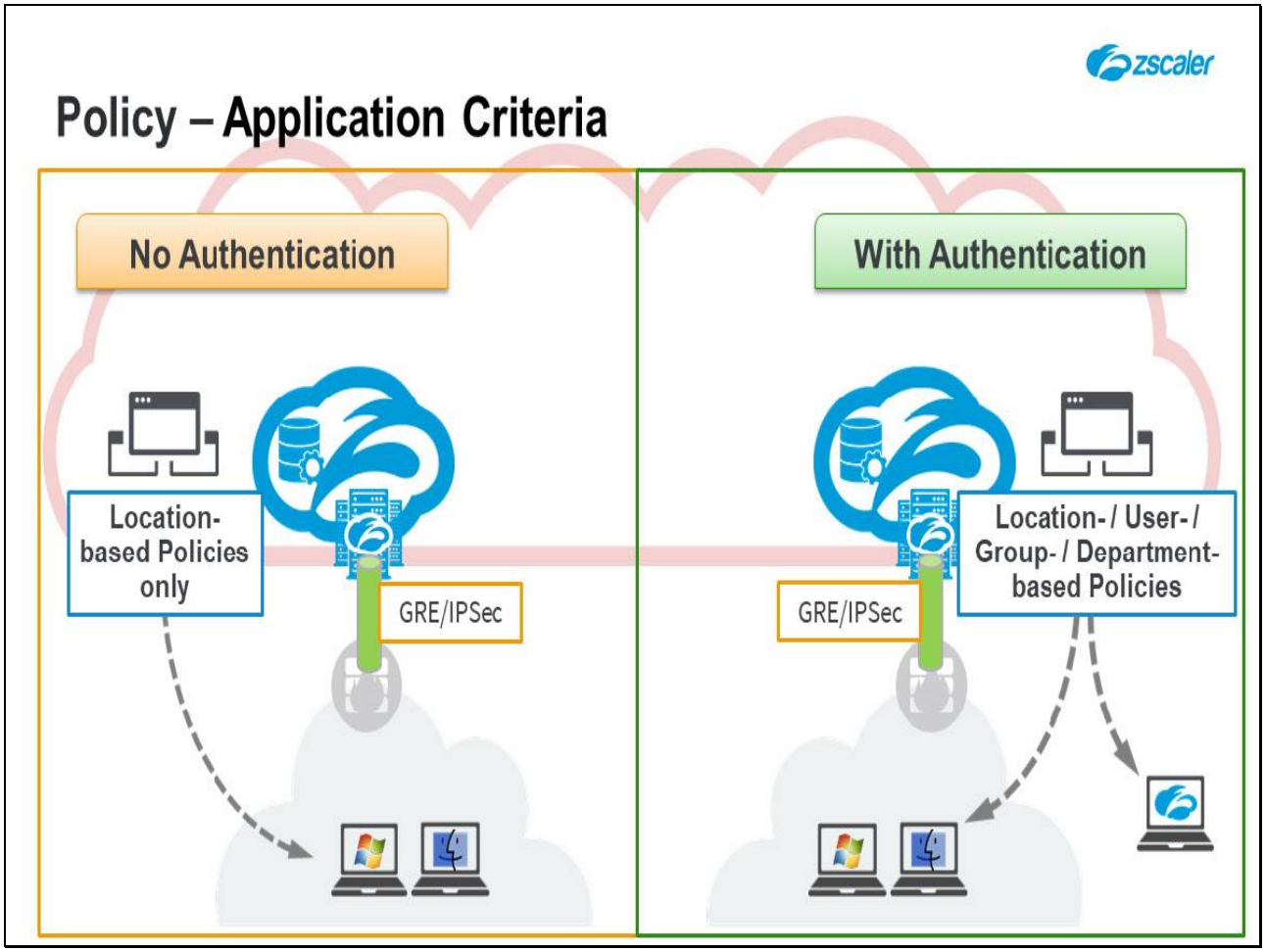
Slide 38 - Policy – Application Criteria



Slide notes

When a site is connected to Zscaler via an IPSec or GRE tunnel, we consider that a Location. You can apply Policies based on a Location, including different IP subnets of a Location without requiring individual user authentication since we know to whom the traffic belongs.

Slide 39 - Policy – Application Criteria

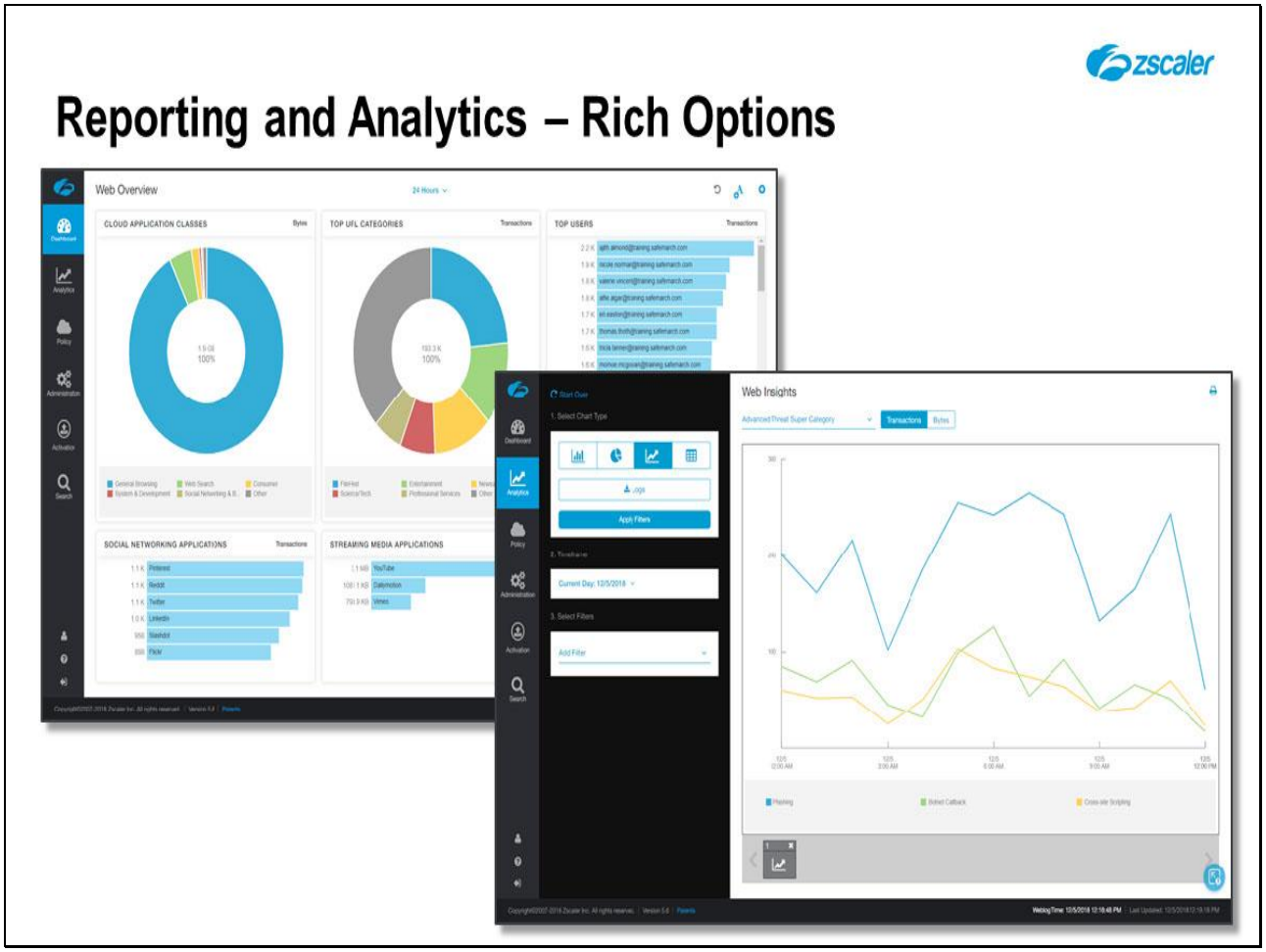


Slide notes

If you also want to apply policies based on individual users, groups, or departments, you can enable Authentication for a Location. Systems that cannot authenticate, like Internet of Things devices, will use Location-based policies. Users who are connecting to Zscaler outside of a tunnel are considered Road Warriors and must authenticate so that we can apply the correct policy to them.

You may have traffic from applications that don't support authentication or cookies, or you are not doing SSL inspection. In this scenario, you would use Surrogate IP. Once a user authenticates Zscaler temporarily maps that IP to that user for applying policy. That is why it is critical to not NAT traffic prior to sending it to Zscaler.

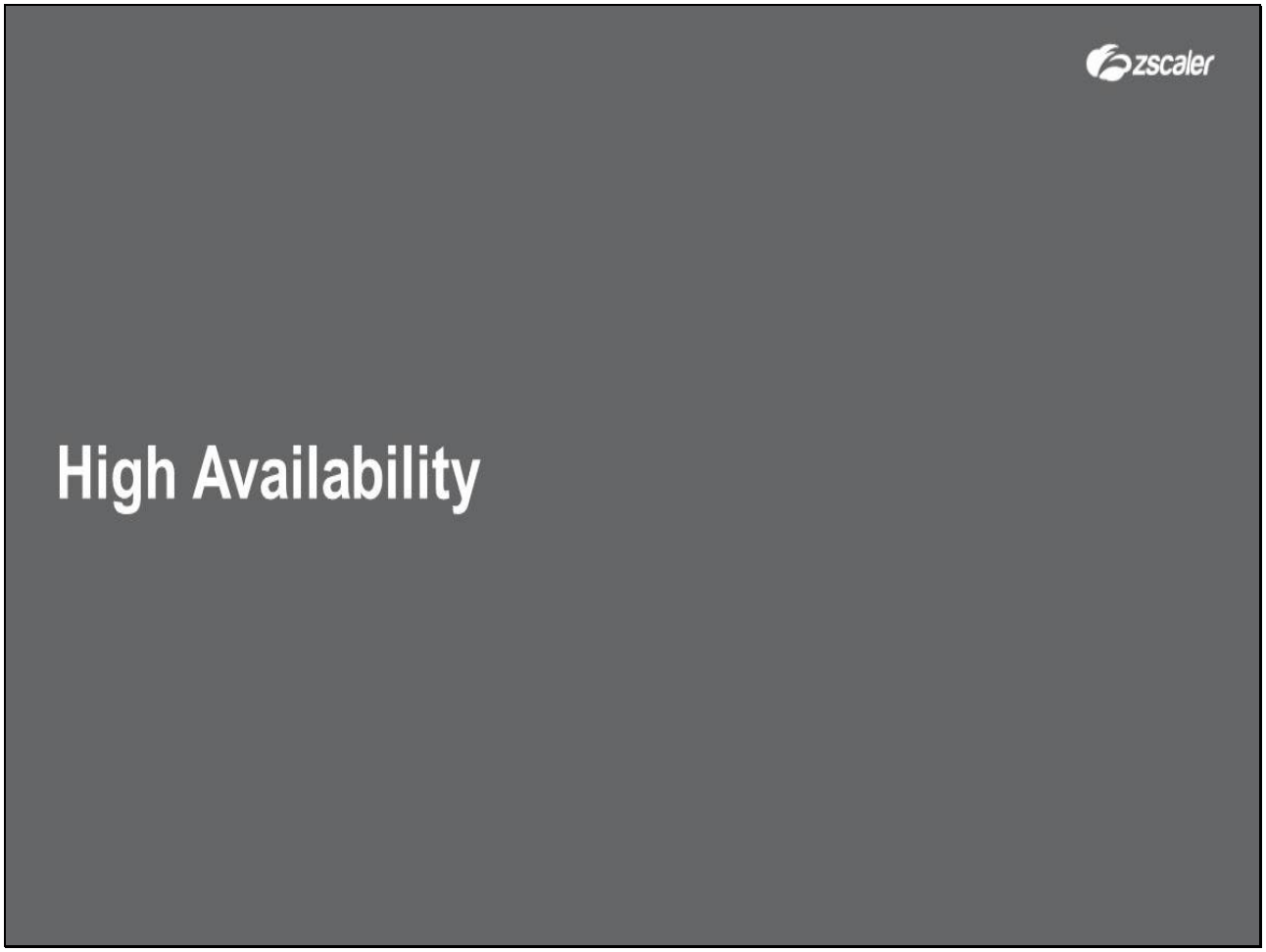
Slide 40 - Reporting and Analytics – Rich Options



Slide notes

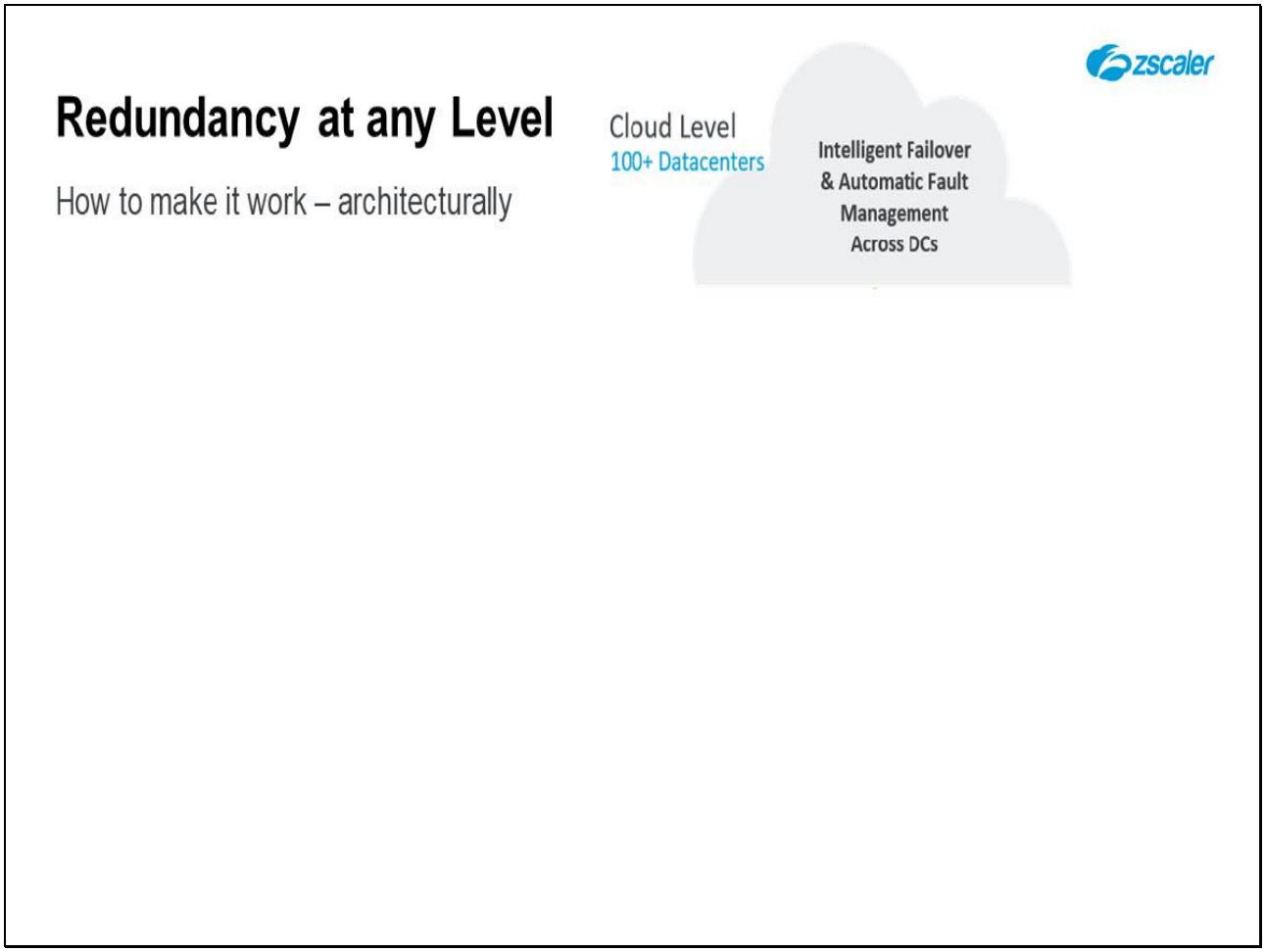
The Zscaler Admin Portal provides customizable Dashboards for real-time monitoring of the company's security, users, application, and traffic status. It also provides advanced Analytics engines to allow reporting and forensic analysis of security incidents.

Slide 41 - High Availability



Slide notes

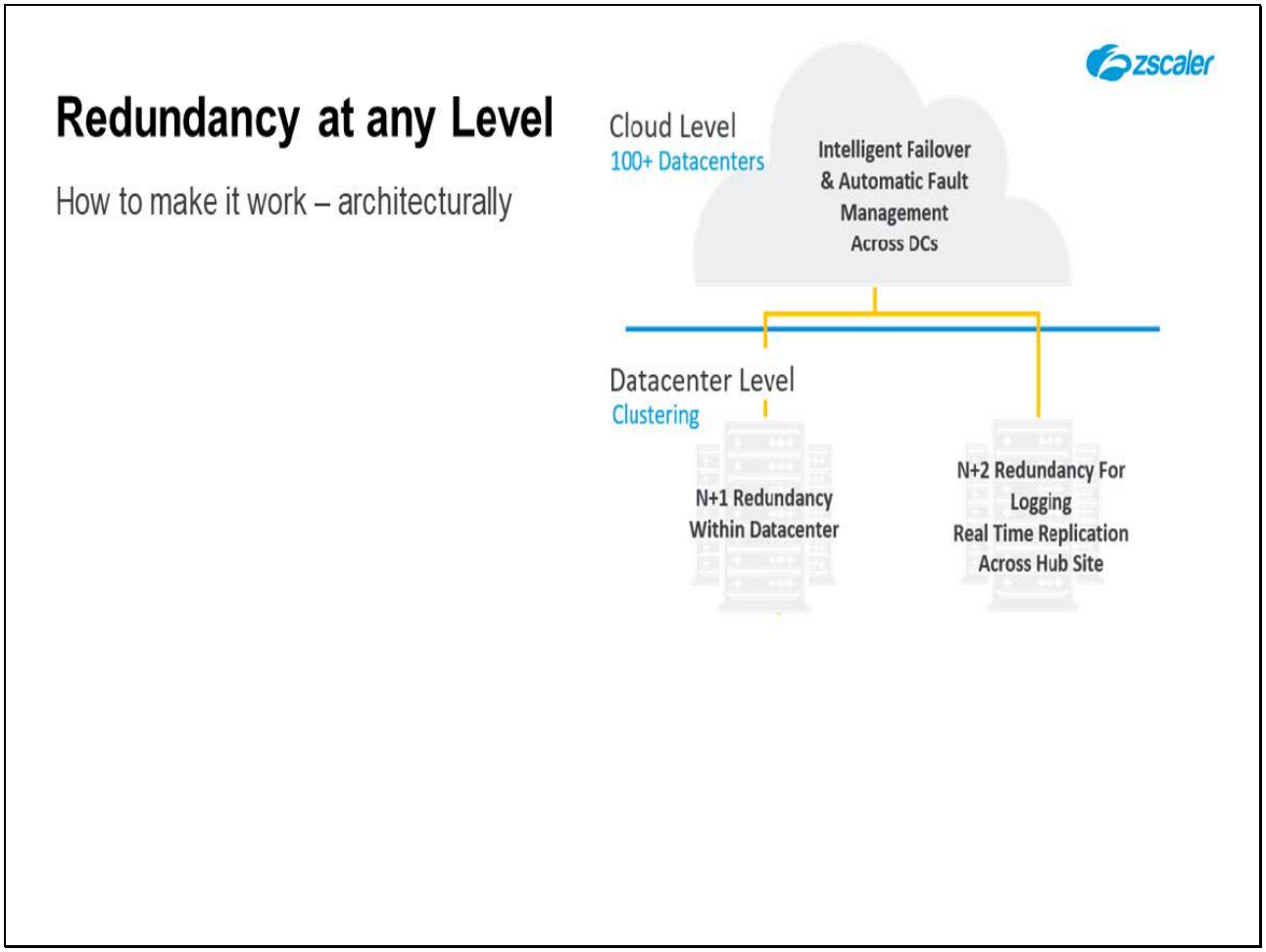
Slide 42 - Redundancy at any Level



Slide notes

We'll end with a bit about High Availability. Zscaler's architecture is built to be Highly Available from the ground up. Every component of the platform was built with that in mind. It starts with having cloud-level failover with Datacenters all over the world. It's the peering, exchanges, and all of that to ensure that we can reroute traffic and stay up.

Slide 43 - Redundancy at any Level

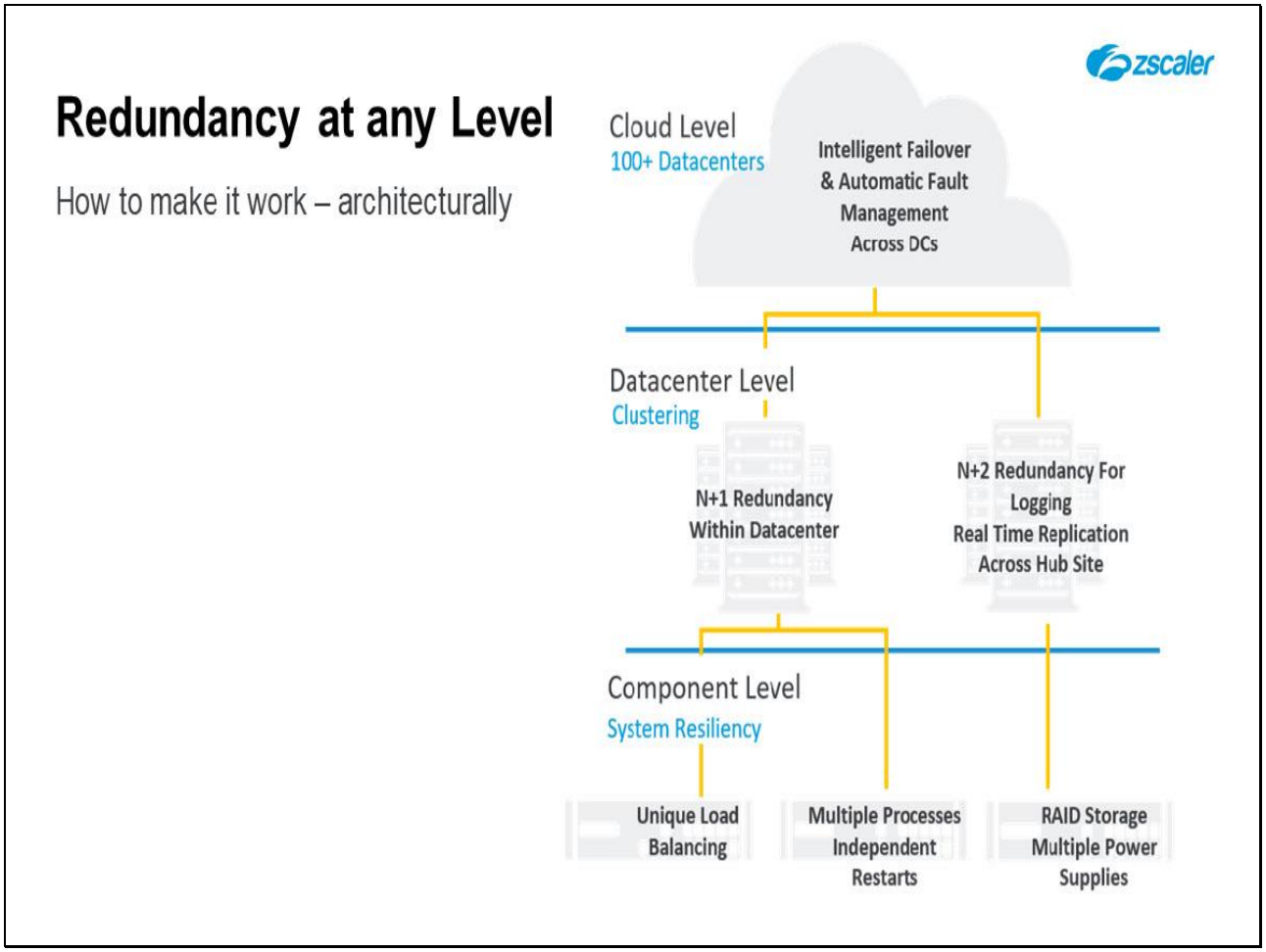


Slide notes

Beyond that within a single Datacenter everything is N+1 or N+2. All our traffic forwarding when it comes to us goes to a Virtual IP that load balances N+1 into a redundant architecture. So even if we took out one or 2 instances it isn't going to affect anything because the IP remains the same and traffic continues to flow. If that fails and the entire Virtual IP goes down, then we fail DC-DC. For logging and reporting we do N+2 to be extra careful.

This means all logs are written in triplicate so no matter if we have a major disaster on both coasts, we'll still have a way to keep logging and reporting going because that is the primary data that we are dealing with.

Slide 44 - Redundancy at any Level



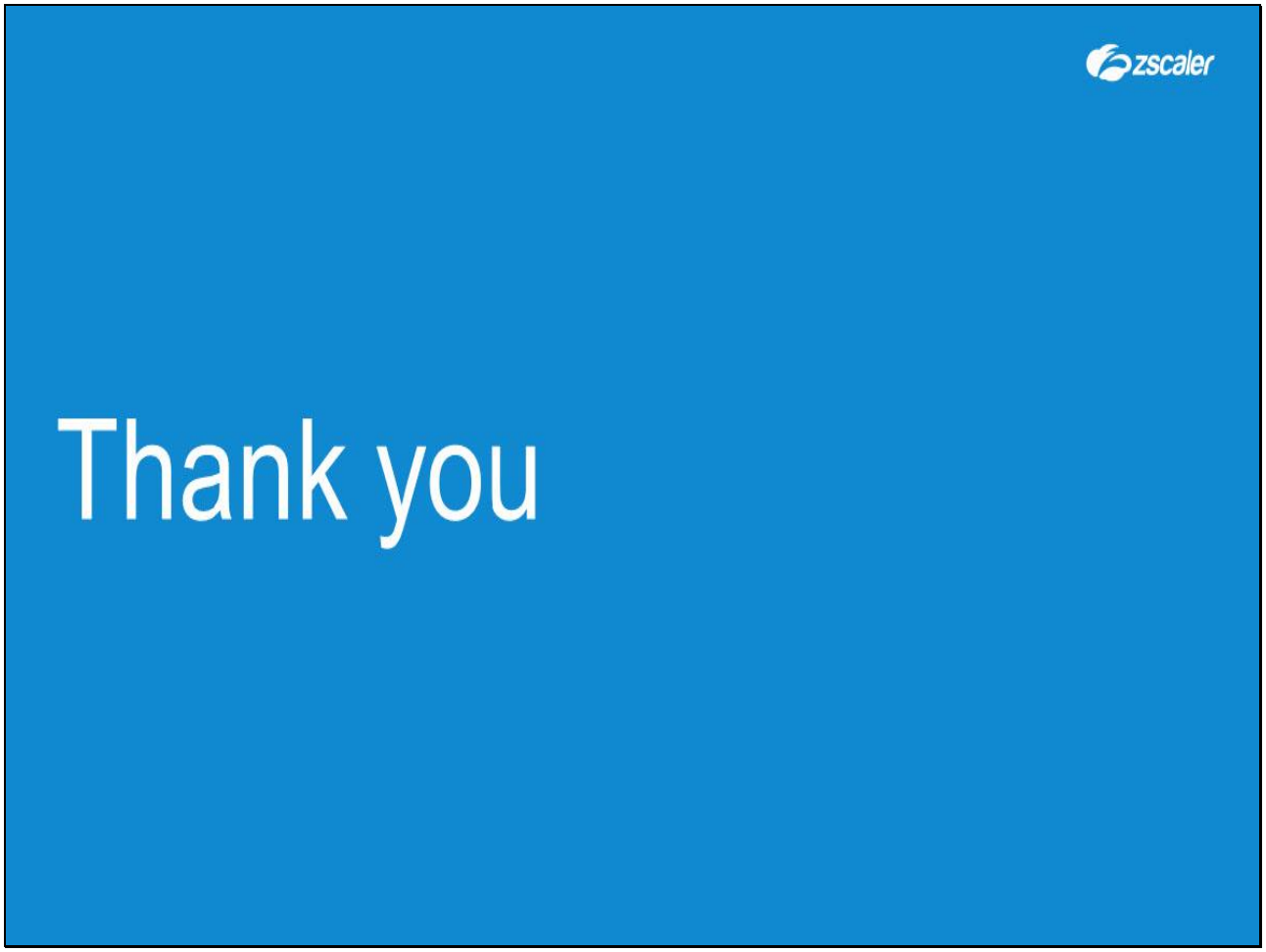
Slide notes

Lastly within each component within a single box we have redundancy and resilience. We have a unique load balancing architecture because it's a purely software defined infrastructure.

We spin up many instances of the software within a single box and load balance across them. So if an instance has a failure just that instance restarts and the box never has to reboot. Most of our boxes have not been rebooted for years now. So there is resilience within the software within the box and we have multiple processes that can independently restart without touching anything else.

The reason we can offer you a 5 9's SLA is because at every level we have HA built in from component level to Datacenter level to cloud level.

Slide 45 - Thank you



Slide notes

This concludes the Zscaler Architecture module. We hope this module has been useful to you and thank you for your time.

To close this module, click the **X** in the upper right. Don't forget to take the quiz to receive credit for the module.