THE IBOSS ACADEMY

Overview

The iboss Academy provides training and certification for the iboss Zero Trust Security Service Edge (SSE). The academy takes you through a journey of implementing a Zero Trust Security Service Edge at a fictional company called The Acme Corporation. The Acme Corporation has many challenges that include protecting enterprise-owned applications, data and services that are located onsite, in cloud infrastructure and across SaaS applications. In addition, the Acme Corporation has remote workers, contractors and guests that need access to these critical resources. The goal is to protect the applications, data and services while allowing users and assets to interact with the resources securely. The Acme Corporation would like to modernize by completing a cloud transformation for connectivity and security. This will allow the Acme Corporation to leapfrog the competition and remain competitive while delivering products to the world in an environment where everything and everyone can be remote and are not bound by perimeters. The iboss Zero Trust SSE will provide connectivity and security that includes compliance, CASB, malware defense and data loss prevention to ensure Acme Corporation remains at the peak of innovation while reducing cyber-risk and greatly improving the end-user experience.

Learn more
www.iboss.com

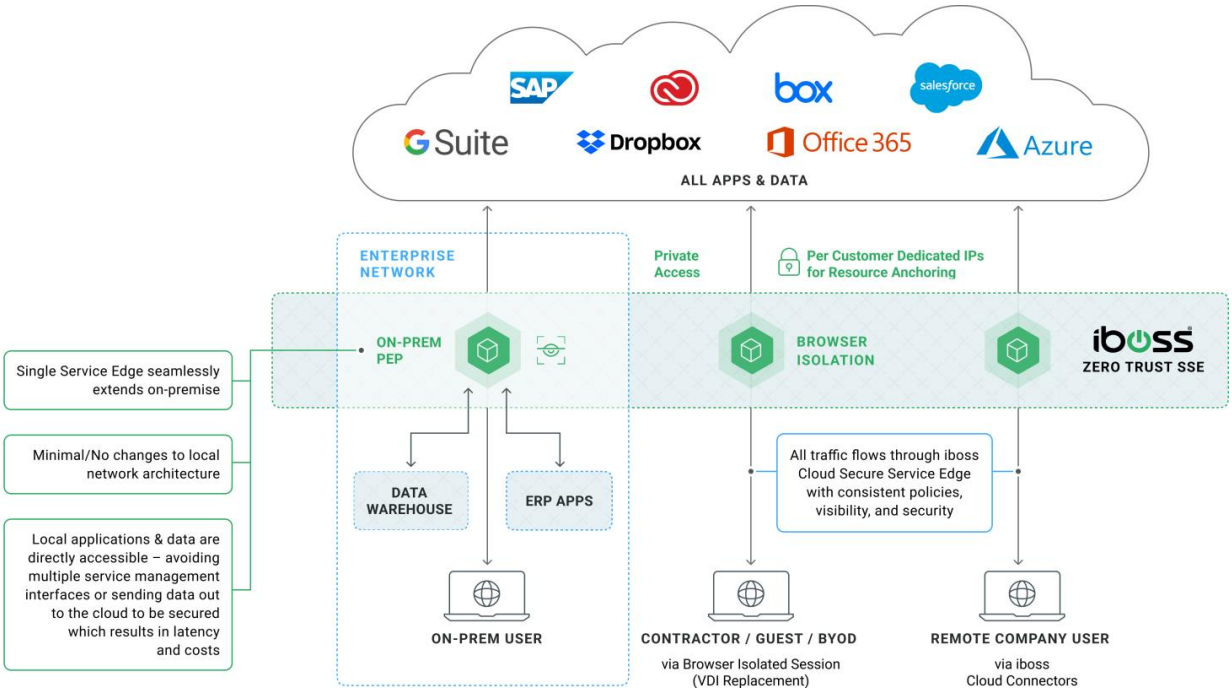

Figure 1. The iboss Zero Trust SSE will be used for the Cloud Transformation of connectivity and security at Acme Corporation

Your Mission

You have been hired by the Acme Corporation to implement the iboss Zero Trust SSE. The Acme Corporation would like to solve for all use-cases related to connecting and protecting sensitive resources, users and devices. Your job is to be the trusted professional that will design and implement the Zero Trust SSE cloud transformation. This includes connecting remote users to Acme Corporation applications that reside onsite and in the cloud. In addition, Acme Corporation would like to reduce costs by decommissioning legacy technology such as proxy security appliances that reside in the datacenter, VPNs that remote users leverage to connect to onsite resources, and Virtual Desktop Infrastructure (VDI) that is used to connect guests, contractors and high risk users to Acme Corporation sensitive data.

By leveraging the budget from legacy technology that will be replaced by the iboss Zero Trust SSE, the cloud transformation to the iboss Zero Trust SSE will not only improve security and end-user experience for Acme by ensuring that security and logging is available everywhere, it will also provide substantial cost savings from the elimination of legacy appliances, the labor required to manage it, the datacenter space required to host it and ongoing future costs that are incurred in future hardware refresh cycles.

The Certification Process

As you implement the iboss Zero Trust SSE for Acme Corporation, you will achieve iboss Zero Trust SSE certifications. The iboss Academy will provide you with hands on experience using the iboss Zero Trust SSE platform and implementing meaningful use cases that can be applied beyond the Acme Corporation.

The Acme Corporation

To manufacture the best products in the world in an agile fashion, the Acme Corporation allows users to work from the office or remotely. The goal is to ensure that end-users always have compliance, CASB, malware defense, DLP and logging applied regardless of where they work. By connecting the users and devices to the iboss Zero Trust SSE, traffic from laptops will be automatically redirected to the Security Service Edge which will perform those functions without users ever turning on a VPN. It is important to understand Acme Corporation's office and datacenter layout to determine where the sensitive applications, data and services reside as well as ensure that users have access to resources from anywhere.

Acme Corporation Org Structure

The Acme Corporation consists of several departments which includes Sales, HR, IT, call center and general employees.

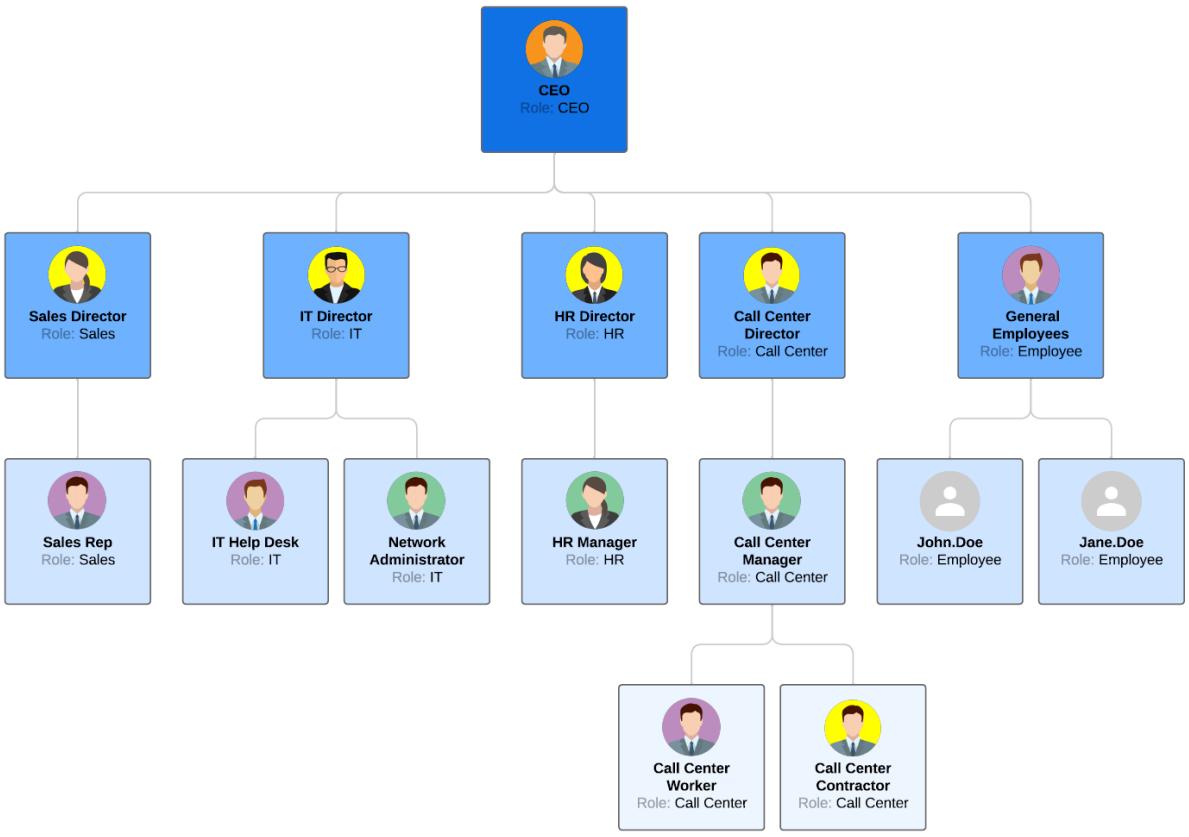

Figure 2. The Acme Org Structure

Like most companies, employees at each department have different critical business needs in order to fulfill their obligations. The differences in their roles and day to day work will require different strategies for reducing the risk from breaches and data loss. The iboss Zero Trust SSE will enable these employees to work more efficiently and be more productive while ensuring that Acme Corporation remains secure. This will enable Acme to stay at the pinnacle for the products and services that they offer.

Azure AD Org Structure

Acme has moved to Azure AD where user groups and permissions are centrally managed. Users from each department are placed into Azure AD security groups so that policies can be assigned to those users easily.

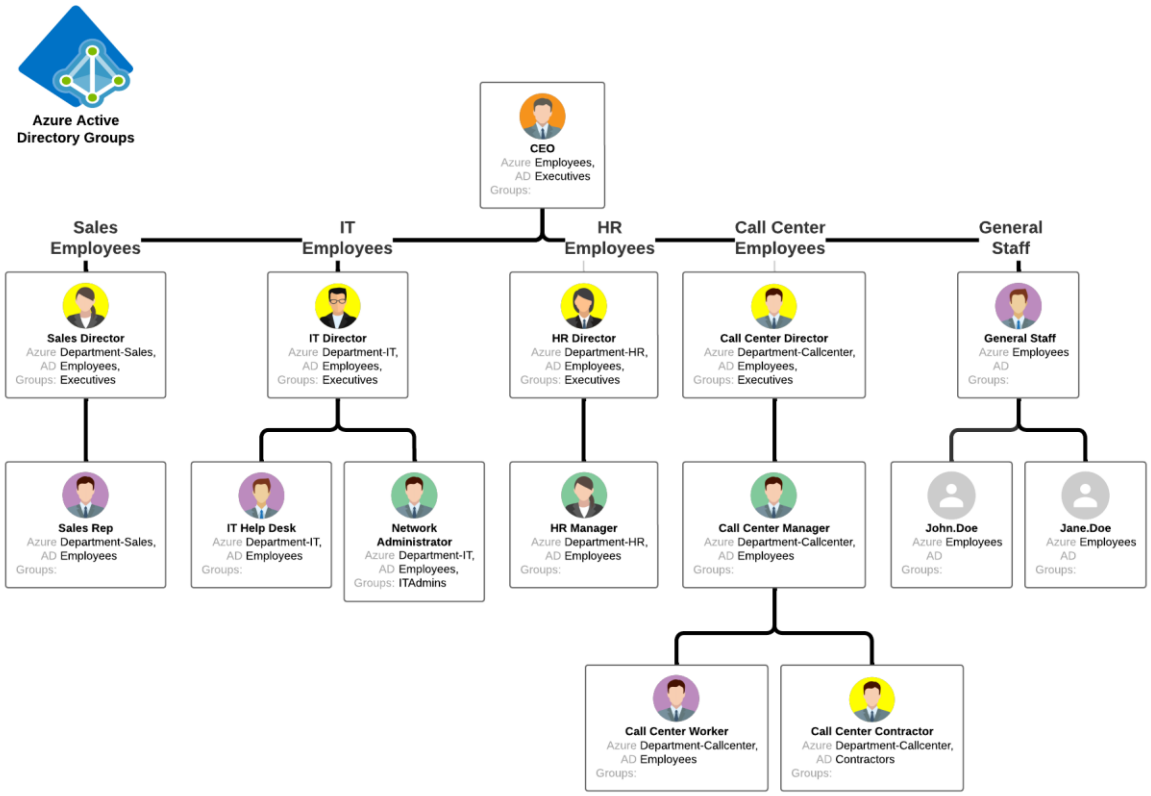

Figure 3. Azure AD Org Structure

The following table shows the Azure AD security groups and how they are assigned to each group of employees.

Employee Department	Active Directory Group
Sales Employees	Department-Sales
IT Employees	Department-IT
HR Employees	Department-HR
Call Center Employees	Department-Call Center
General Staff	No Active Directory Groups Assigned

The Azure AD groups will be leveraged within the iboss Zero Trust SSE so that access and security policies can be applied to groups of users.

Acme Corporation's Offices

The Acme Corporation has the following office and datacenter locations:

- **Corporate Datacenter** - This location contains a network for onsite servers that run various applications, such as the internal Acme Employee Portal as well as other backend services.
- **Corporate Headquarters** - This location represents the main Acme Corporation office and contains various laptops used by employees. Internet connectivity for the Corporate Headquarters is provided through the Corporate Datacenter via a private link that connects the headquarters to the datacenter.
- **Branch Office** - This is a branch office that hosts a number of employees and also has some locally hosted services, such as a web portal used for time tracking. The branch office can communicate with the datacenter via a SD-WAN connection that has been deployed. However, Internet traffic traverses directly to the Internet from the branch office via an Internet breakout from the branch office itself.

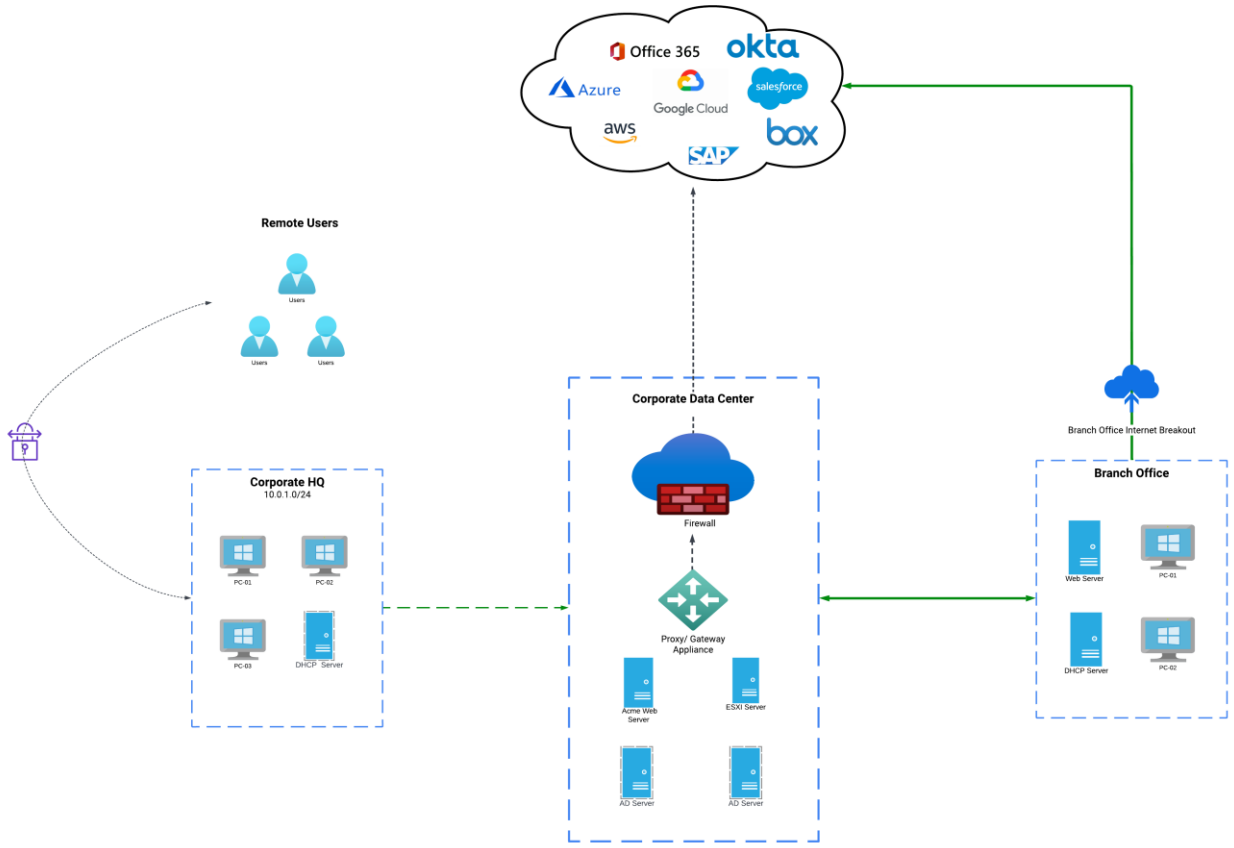

Figure 4. The Acme Corporation has three locations that include a Corporate Datacenter, Headquarters and Branch Office

Acme Corporation Network Topology

The three locations have a network topology that involves using three network subnets, one for each location. The Corporate Datacenter uses a network subnet of 10.0.0.0/24. The Corporate Headquarters uses a network subnet of 10.0.1.0/24. Finally, the branch office uses a network subnet of 10.0.2.0/24.

When users are at any of the three Acme sites, they can access resources from any other site, either through the private link that connects the Headquarters to the Datacenter or via the SD-WAN connection that connects to Datacenter to the branch office. There are two public Internet addresses Acme uses. The first public IP address is for traffic leaving the Datacenter. Since traffic from Headquarters also exits through the Datacenter, the public IP for traffic leaving Corporate Headquarters will also have the same public IP address as traffic that exits from devices at the Datacenter. The Branch Office uses its own public IP traffic headed toward the Internet as it leverages a direct Internet breakout and traffic does not need to traverse through the Datacenter.

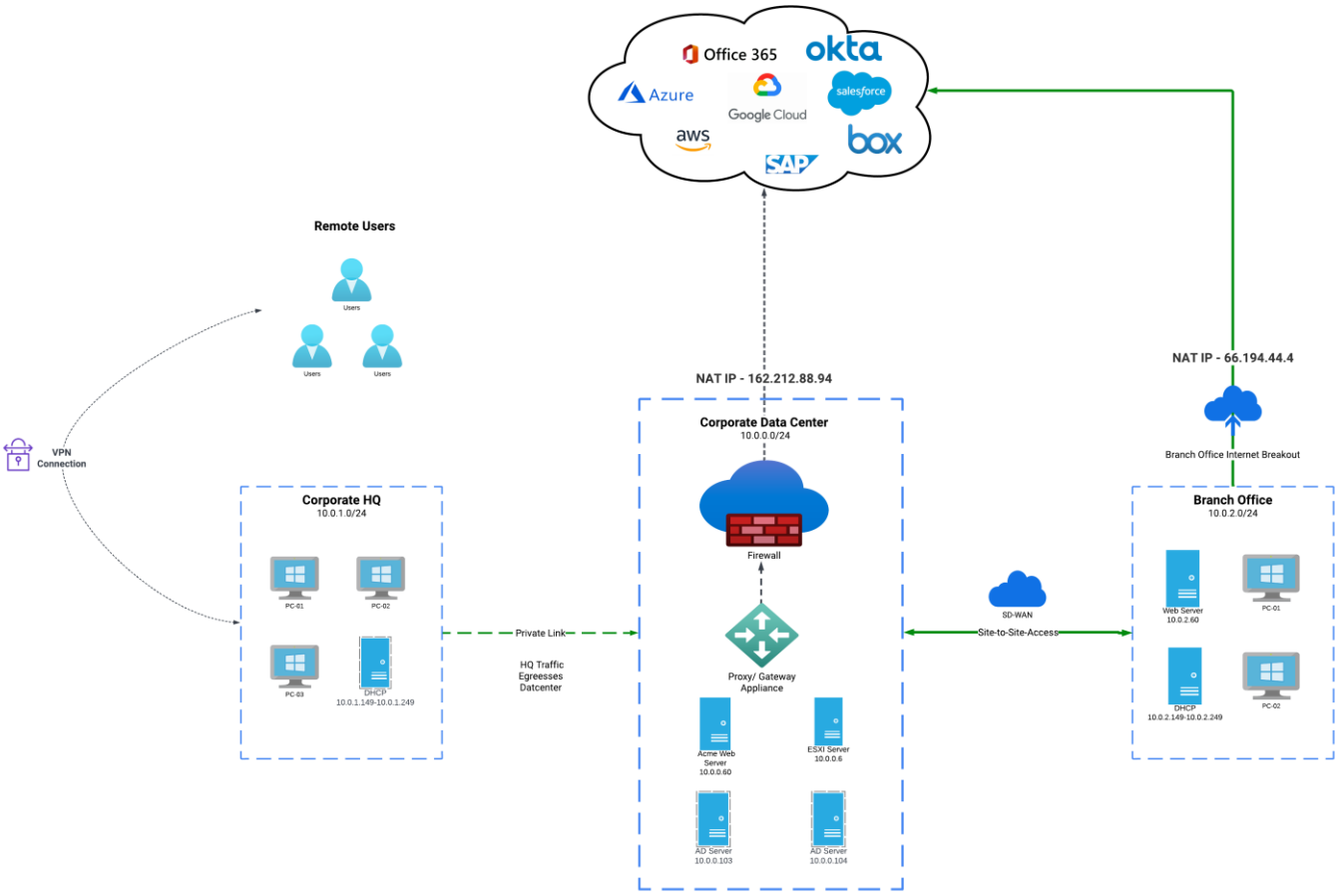

Figure 5. Acme Corporation's Network Topology

Challenges with Current Network Layout

There are several challenges Acme wants to solve related to their current environment. Because the Corporate Datacenter provides Internet connectivity for the Corporate Headquarters, there is a large volume of bandwidth traversing the datacenter which is resulting in latency for users at the Headquarters and leading to high costs due to the private link that must be maintained between the two locations. Prices for the private link keep increasing which is resulting in higher costs for Acme. To make things worse, the network security appliances that are hosted at the Datacenter to provide protection for the Headquarters is also getting very expensive and Acme has just learned that a hardware refresh will be required which will result in a lot of labor and even higher costs. Because Acme is moving all of the applications to the cloud, the long term goal is to decommission the datacenter and eliminate the dependency of users within Headquarters to have to connect through the Datacenter for Internet access. This will greatly reduce bandwidth and datacenter costs as well as greatly reduce management overhead.

Finally, the branch office has a direct Internet breakout. Traffic leaving the branch office does not traverse the Datacenter which means there is no security (CASB, malware defense and DLP) being applied to that traffic. There is also a lack of visibility as there is no logging being generated for connections to the Internet from devices in the branch office. Acme would like to get a consistent level of security and visibility across all locations, including remote workers.

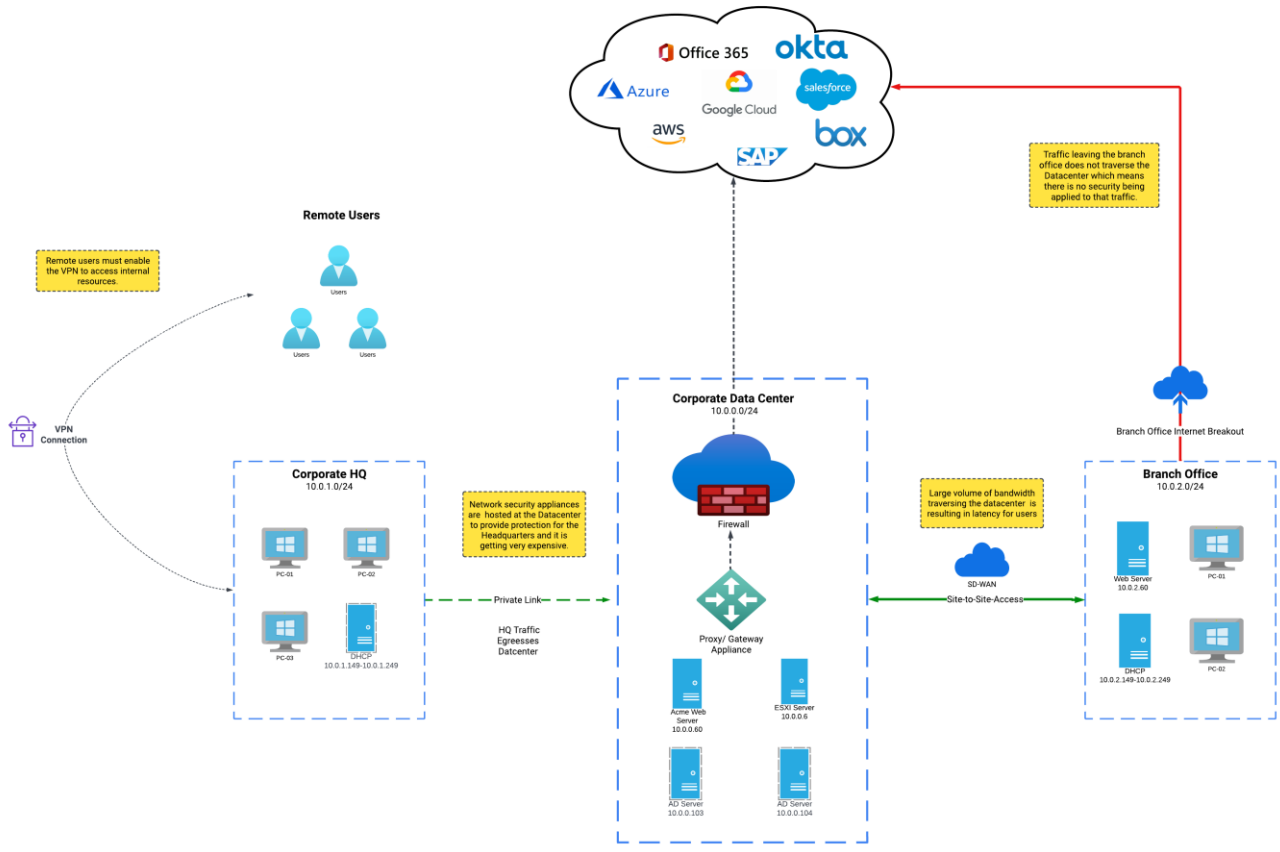

Figure 6. Challenges with Current Network Layout

iboss Zero Trust SSE Overview

The iboss Zero Trust Security Service Edge is a platform that combines connectivity, such as ZTNA, and security capabilities such as CASB, malware defense, DLP and logging, into a single platform that automatically connects users and devices to all enterprise owned resources and the public Internet. It automatically encrypts all network traffic, including DNS, at all times regardless of location and redirects the traffic to the global Security Service Edge which provides connectivity and security capabilities. The iboss Zero Trust SSE platform will be used at Acme Corporation to perform the complete cloud transformation for connectivity and security.

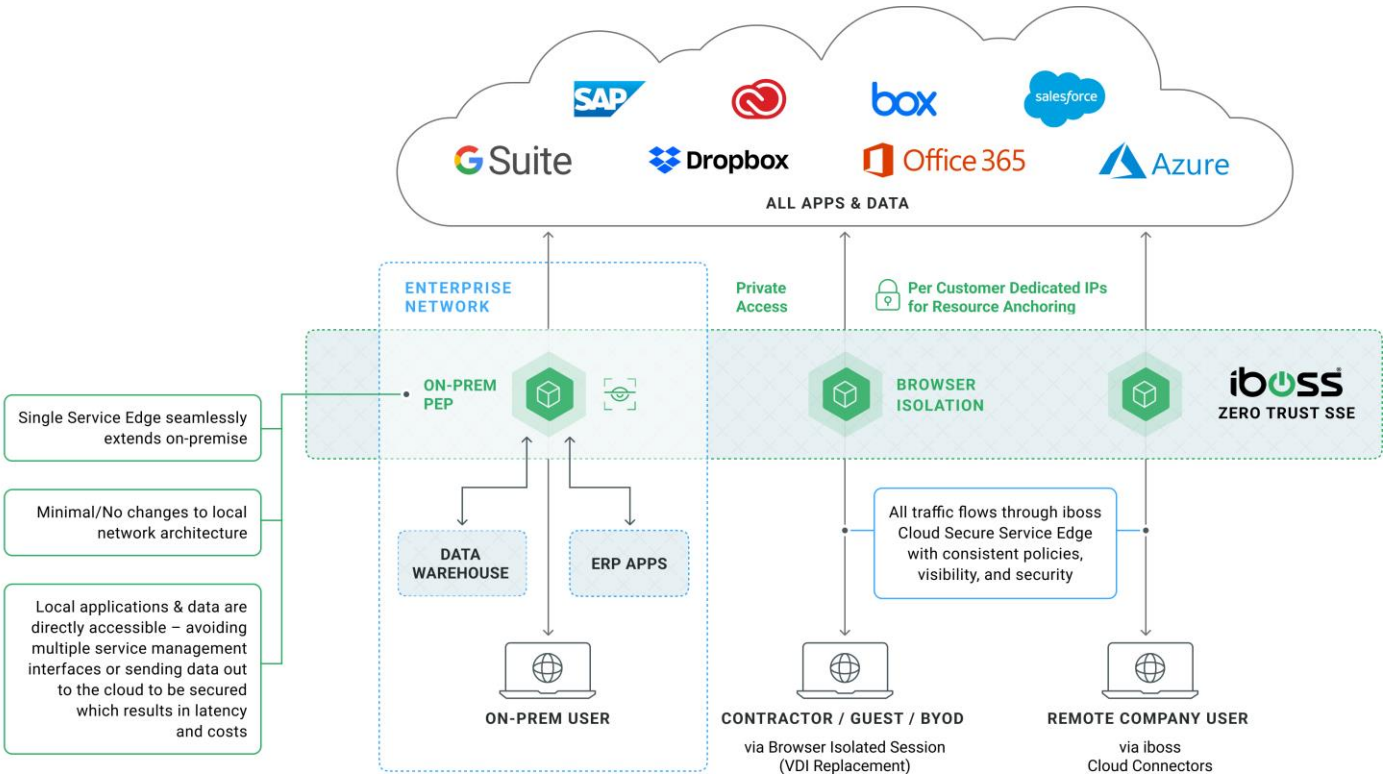

Figure 7. Figure 7. The iboss Zero Trust SSE will be used for the Cloud Transformation of connectivity and security at Acme Corporation

With the iboss Zero Trust SSE, users and devices from Acme Corporation will be able to connect to commodity internet at any location with the assurance that security and logging will always be in place. This is because the network traffic from their devices will always be fully encrypted and and sent to the service which will provide connectivity to all resources and security such as CASB, Malware Defense, DLP and logging. This will substantially increase security for Acme Corporation while greatly reducing the costs related to complex network security infrastructure at Acme offices and datacenters.

The iboss Zero Trust Security Service Edge (SSE) prevents breaches and data loss by targeting the root cause of the top initial infection vectors for ransomware, which is unauthorized resource access. According to the Cybersecurity and Infrastructure Security Agency (CISA) and in conjunction with the United Kingdom, Australia and other world governments and agencies, the top three initial infection vectors for ransomware breaches was unauthorized access to networks via phishing, stolen credentials or brute force and exploiting vulnerabilities.

2021 Trends Show Increased Globalized Threat of Ransomware | CISA

CISA Alert (AA22-040A) - Trends Show Increased Globalized Threat of Ransomware

Understanding this root cause analysis of ransomware breaches is critically important. Acme Corporation has sensitive applications, data and services which will remain secure if unauthorized access to those resources by attackers is prevented. For example, with the many hundreds of applications that Acme uses, at one point one of those applications will have a vulnerability due to software flaws. If that application is exposed and accessible by attackers, the attackers will take advantage of that vulnerability immediately to breach the service resulting in financial and data loss. The goal of the iboss Zero Trust SSE is to make all Acme enterprise-owned resources private and only accessible by approved and authorized Acme users. By leveraging this concept, even if an application becomes vulnerable, it is still protected because the attackers cannot gain access to the service. In addition, the iboss Zero Trust SSE combines Zero Trust access concepts with a complete deep content security stack that includes CASB, malware defense, DLP and browser isolation so that all interactions to sensitive resources are protected with the highest level of protection.

The iboss Zero Trust SSE is aligned directly to the NIST 800-207 Special Publication titled Zero Trust Architecture and meets all of the tenets as well as network requirements for a proper Zero Trust Architecture, or ZTA, implementation.

The service implements the concepts in the NIST 800-207 and the iboss Zero Trust SSE is a technical implementation of the centerpiece of this model. Acme Corporation wishes to implement Zero Trust according to the NIST 800-207 Zero Trust Architecture principles and we'll use the iboss Zero Trust Security Service Edge to do so as it forms the technology foundation of this architecture. The NIST 800-207 model provides a strong and clear foundation for Acme Corporation to implement Zero Trust which greatly reduces cyber risk, breaches and data loss.

In addition, the NIST 800-207 is part of the NIST Risk Management Framework (RMF) which Acme Corporation leverages as a cybersecurity framework to reduce risk.

NIST Risk Management Framework Overview

There are three core security objectives that implementing the iboss Zero Trust SSE is designed to achieve which is modeled after NIST FIPS 199.

1. **Preventing Data loss** – Referred to as ***Confidentiality*** in FIPS 199
2. **Preventing Data Destruction** – Referred to as ***Integrity*** in FIPS 199
3. **Ensuring access to Enterprise critical resources** – Referred to as ***Availability*** in FIPS 199

The NIST FIPS 199 guidelines describe these security objectives and how to assign security impact levels to each of these objectives.

In addition to these core security objectives, the iboss Zero Trust SSE is designed to meet additional Acme Corporation objectives such as ensuring compliance with regulatory guidelines and laws.

Implementing the NIST 800-207 Zero Trust architecture requires technology, processes and people. The iboss Zero Trust SSE is designed to provide the technology needed to implement this framework. It also simplifies running the required processes and organizing the people to create a robust Zero Trust strategy.

Implementation Strategy

Core Zero Trust SSE Concepts

Before starting with any configuration, it is important to understand a core concept that is used for the foundation of any policies created within Zero Trust SSE framework. The Zero Trust journey is anchored around understanding clearly what is being protected. Zero Trust is anchored around three core variables:

1. **The Resource**
2. **The Subject** (i.e. User)
3. **The Asset** (i.e. Device)

These are the three key components that are interacting with each other and the foundation for the risk that is to be mitigated.

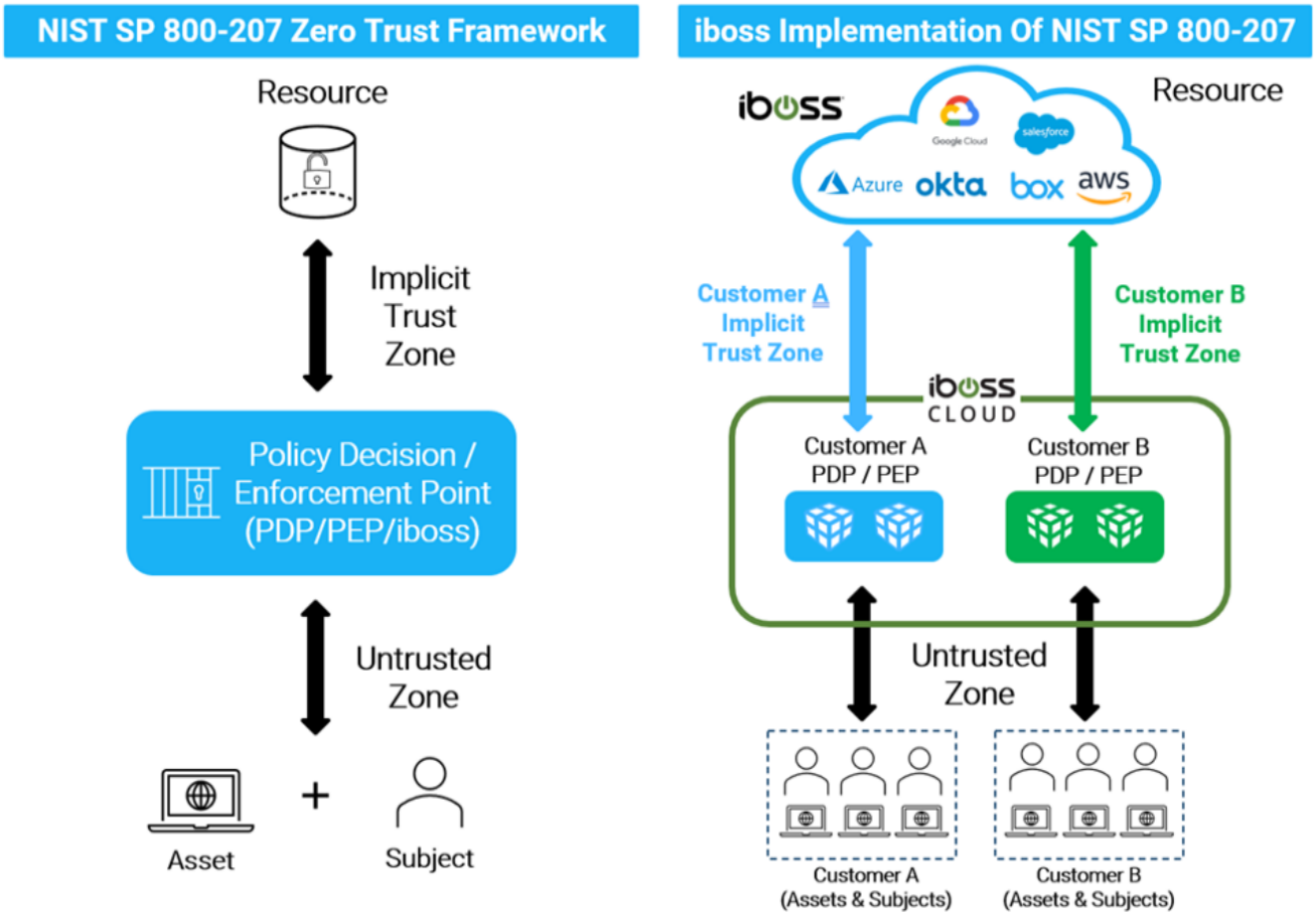

Figure 8. Zero Trust is anchored around the Resource, Subject and Asset

The iboss Zero Trust SSE will catalog all three actors and allow policies to be created that determine how users and assets interact with resources. The first step in the Zero Trust journey is to start with classifying and connecting enterprise-owned resources. Enterprise-owned resources are the most important in terms of risk, as they contain the sensitive data and provide the critical services to Acme Corporation. This is an important concept to understand. The goal is to classify Acme enterprise-owned resources. This allows a clear distinction between where data should reside and where data should not reside. For example, by clearly knowing all enterprise-owned resources, any application or service outside of that list should be untrusted and should never have Acme data placed within that application as that would result in data loss.

> ⓘ Zero Trust starts by clearly cataloging enterprise-owned resources so that there is a clear boundary for protecting data between enterprise-owned applications and non-enterprise owned applications in order to prevent breaches and data loss.

The iboss Zero Trust Security Service Edge delivers a global unified service to automatically connect all users and devices to any destination with CASB, malware defense, DLP and logging applied to every transaction.

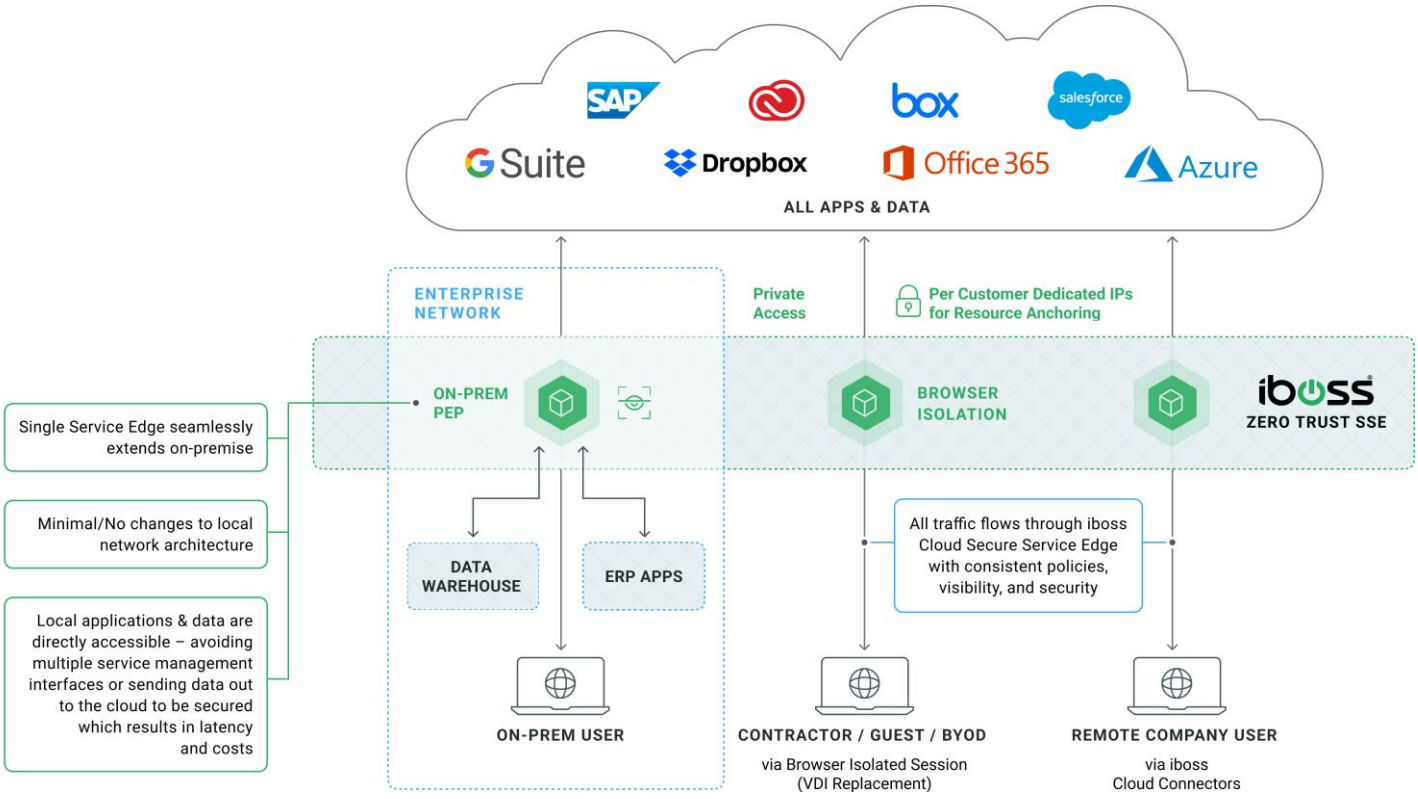

Figure 9. The iboss Zero Trust Security Service Edge combines connectivity, such as ZTNA, and security capabilities such as CASB, malware defense, DLP and logging, to automatically connect Acme users and devices to all enterprise owned resources and the public Internet

Strategy for Connecting Users & Devices to the iboss Zero Trust SSE

The NIST 800-207 describes four deployment strategies for Zero Trust implementations.

1. **Device Agent/Gateway Based Model** - This model includes deploying agents on Acme devices that will perform device posture checks, such as ensuring anti-malware is running, as well as redirecting traffic to the iboss Zero Trust SSE at all times and from any location. The iboss Zero Trust SSE provides Cloud Connector agents for this purpose. We will leverage this model for all Acme owned devices.
2. **Enclave Based Model** - This model still includes the install of Cloud Connector agents but also includes placing iboss gateways, or Policy Enforcement Points, onsite.
3. **Resource Portal Based Model** - This model includes connecting users through a VDI-like interface with no agent installation required. This is particularly required for guests, contractors and high risk users where Acme data must not touch personal or high risk devices. The NIST 800-207 suggests Browser Isolation as a way to implement this model and the iboss Zero Trust SSE includes Browser Isolation capabilities. We'll use this for the Acme call center employees as well as contractors.
4. **Device Sandbox Model** - This model includes pushing an agent into a device sandbox for Operating Systems that support this functionality in which only data from the sandbox is redirected to the iboss Zero Trust SSE.

For our implementation, we'll use the "Device Agent/Gateway" based model for all Acme owned devices. We'll use the resource portal based model, using iboss Browser Isolation, for contractors and call center agents so that users from within those groups can interact with applications but the data from those applications will never touch the high risk and non-enterprise owned devices.

Strategy for Connecting Acme Resources to the iboss Zero Trust SSE

Acme Corporation has resources that are located at the datacenter, HQ and the branch office. In addition, Acme Corporation has SaaS applications that need to be connected to the iboss Zero Trust SSE as well. This will allow the iboss Zero Trust SSE to protect these resources with compliance, CASB, malware defense and Data loss Prevention in addition to providing logging for every transaction to sensitive applications, services and data. Once the resources are connected to the iboss Zero Trust SSE, Acme users and devices that are authorized will be able to connect to them from any location.

To connect resources within Acme datacenters and offices, we'll leverage the iboss Network Connector which automatically creates tunnels to the iboss Zero Trust SSE so that the iboss service can communicate to onsite resources.

Deployment Strategy Summary

What is being Connected	Deployment Strategy
Resources onsite within Acme Corp datacenter and offices	We will use the iboss Network Connector which will create tunnels to the iboss Zero Trust SSE an provide access to onsite resources.
Acme owned devices	We will use the iboss Cloud Connector agent which will connect these devices to the iboss Zer Trust SSE from any location.
Contractors & Guests	We will use iboss Browser Isolation which will provide a VDI-like interface using the end user's browser which will prevent data from touching no Acme owned devices to prevent data loss.
Acme Call Center employees	We will use iboss Browser Isolation to prevent cal center employees from having direct access to da within Acme sensitive applications.

Certification Course Overview

The certification course will take you through deploying the iboss Zero Trust SSE at Acme Corporation. As the hired trusted IT and security consultant responsible for the design and implementation, you will gain a detailed understanding of the iboss Zero Trust SSE including how to create appropriate policies for connectivity and security.

What's Needed for the Course

Requirement	Description
Acme Corp Virtual Windows Desktop	Acme Corp will provide you a virtual desktop environment that you will use during the course. You can connect to this desktop using a RDP client. This desktop will be used throughout the course which will represent an Acme owned asse This desktop will be connected to the iboss Zero Trust SSE using the Cloud Connector agent. You will receive the credentials for the remote desktop before you start the course.
iboss Zero Trust SSE account	You will need an iboss Zero Trust SSE account which will represent the service that Acme Corporation will be connected to for security. The account should have Browser Isolation enabled f the guest, contractor and call center portions of the Acme deployment.
Access to the Identity Provider Azure AD	This will be used to configure authentication to Acme resources using the iboss Zero Trust SSE. Access to the Acme Corporation's Azure AD account will be provided.
Access to the Acme Corporation Office Environment	This is a simulated environment that is provided by iboss and represents the Acme Datacenter, HQ and Office.
Access to the VMWare ESX environment within the Acme datacenter which will run the iboss Network Connector	The iboss Network Connector creates tunnels from the Acme datacenter to the iboss Zero Trust SSE so that users can access Acme resources that sit onsite within the datacenter, HQ and branch office The iboss Network Connector is a virtual appliance that is installed in the Acme datacenter within the VMWare ESX server sitting in that datacenter.

The simulated Acme Corporation Office Environment and Okta is provided by the iboss Academy. Details for logging into these environments is provided separately.

Course Outline Overview

The iboss Zero Trust SSE certification course will be a journey of implementing iboss at Acme with the following steps.

1. The course will begin by providing a fundamental understanding of what the iboss Zero Trust Security Service Edge is and its overall architecture. This will be important as it will set the foundation for the deployment strategy as well as the business and security outcomes that will be achieved during Acme's cloud transformation.
2. Acme resources are then connected to the iboss Zero Trust SSE. Connecting Acme SaaS applications will be covered first.
3. Next, a fundamental understanding of what resource policies are and how they are used to protect Acme resources is provided. This will include creating and managing iboss Zero Trust SSE resource policies.
4. Acme owned devices are then connected to the iboss Zero Trust SSE using the iboss Cloud Connector agent. For this portion of the course, your laptop will be connected to the iboss Zero Trust SSE which will represent an Acme owned laptop.
5. The Acme Identity Provider (Azure AD) is then connected to provide modern authentication and MFA when accessing Acme resources.
6. This is followed by connecting Acme resources within the Acme datacenter, HQ and the branch office. This is accomplished by deploying the iboss Network Connector within the datacenter which will create tunnels to the iboss Zero Trust SSE that will be used to access onsite resources.
7. Security and compliance policies are configured to protect resources with compliance policies, CASB, malware defense and Data Loss Prevention.
8. Advanced continuous adaptive access policies are created using iboss Trust Algorithms to provide dynamic protection to Acme resources based on user and asset risk.
9. The Application & Service discovery dashboard is leveraged to discover resources within Acme for classification and cataloging.
10. iboss Browser Isolation is then used to connect call center agents through a VDI-like interface to critical Acme resources.
11. Guests are then connected using iboss Browser Isolation guest sessions.

From this certification course, you will form a strong foundation of concepts related to iboss Zero Trust SSE connectivity and security.

Course Syllabus

iboss Zero Trust SSE Overview

Goal

Learn about what the iboss Zero Trust SSE is and its overall architecture. This will provide the knowledge needed to create a successful deployment strategy for Acme as well as understand the security and business outcomes that will be achieved.

Objectives

- Understand what Zero Trust and Security Service Edge (SSE) is
- Understand how the iboss Zero Trust SSE is leveraged to reduce breaches and data loss
- Understand what legacy technologies are replaced with the iboss Zero Trust SSE to reduce costs and provide a better and more secure end user experience
- Understand the differences between the legacy and new approach that will be used for connectivity and security which will be important to successfully complete a cloud transformation
- Understand how users and devices are connected to the iboss Zero Trust SSE
- Understand overall data flows through the iboss Zero Trust SSE as users access resources

Connecting SaaS Resources to the iboss Zero Trust SSE

Goal

Connect Acme SaaS resources to the iboss Zero Trust SSE for protection and visibility.

Objectives

- Gain an understanding of the iboss Resource Database used to catalog resources
- Differences between Enterprise Owned and Non-Enterprise Owned Resources
- Learn about resource tagging including configuring security impact levels for resources
- Create resources including resources from the App Library and custom resources
- Learn how to test connections between the iboss Zero Trust SSE and protected resources
- Adding resources to Resource Policies for protection

Understanding Resource Policies

Goal

Learn how to create policies to protect Acme owned resources and prevent the leakage of sensitive data to public and unsanctioned applications.

Objectives

- Understand the differences between Enterprise Owned and Non-Enterprise Owned Policies
- Learn about the different types of Resource Policies, including Resource List and Category-based Resource Policies
- Learn how Resource Policies are dynamically selected and applied to resource requests
- Learn how to creating and manage Resource Policies
- Gain a high level understanding of Resource Policy security settings
- Create Catch-All Resource Policies to ensure protection across all transactions

Connecting Devices to the iboss Zero Trust SSE Using Cloud Connector Agents

Goal

Connect an Acme owned laptop to the iboss Zero Trust SSE with the iboss Cloud Connector.

Objectives

- Gain a high level understanding of the iboss Cloud Connector agents
- Learn how to install the Windows Cloud Connector agent
- Learn how to centrally manage Cloud Connector settings using Connector Policies

Identity and Authentication

Goal

Connect the Acme Identity Provider to the iboss Zero Trust SSE so that modern authentication can be required to access sensitive applications, services and data.

Objectives

- Understand the benefits of leveraging an Identity Provider in Resource Policies
- Overview of Federated Identity Provider Integration
- Configure Azure AD for User SSO
- Applying Resource Policies to user transactions based on Identity Provider group membership
- Requiring step-up authentication to access sensitive resources

Connecting Private Onsite Resources to the iboss Zero Trust SSE

Goal

Connect Acme onsite resources to the iboss Zero Trust SSE, including resources within the Acme datacenter, HQ and branch office.

Objectives

- Learn how to define locations within the iboss Zero Trust SSE
- Connect onsite resources to the iboss Zero Trust SSE using the iboss Network Connector
- Learn how to define and configure private onsite resources within the Resource Database
- Learn to test connectivity between the iboss Zero Trust SSE and onsite resources
- Assign onsite resources to Resource Policies for protection

CASB, Malware Defense & Data Loss Prevention

Goal

Learn how to configure CASB, malware defense and Data Loss Prevention to protect Acme resources from breaches and data loss.

Objectives

- Learn to configure CASB controls for resources
- Learn to apply Malware protection to resources using Resource Policies
- Apply Data Loss Prevention protection using resource policies
- Troubleshooting policies using Policy Tracing

Configuring Continuous Adaptive Access to Dynamically Protect Resources

Goal

Dynamically protect Acme resources by applying continuous adaptive access policies based on asset and user risk.

Objectives

- Gain an understanding of iboss Trust Algorithms used for continuous adaptive access
- Learn how to configure and take action based on user, asset and resource signals
- Assign Trust Algorithms to Resource Policies to protect resources with adaptive access
- Learn about Trust scoring and how scores are applied to each transaction
- Learn how log events are scored using Policy Tracing

Identify Resources Using the Application & Service Discovery Dashboard

Goal

Find hidden sensitive Acme resources using the Application & Service Discovery Dashboard.

Objectives

- Discover hidden SaaS, Cloud Infrastructure & Onsite Resources
- Understand discovered resource risk by leveraging cloud app scores
- View resource risk details and learn how to override scores and risk findings
- Learn how to catalog automatically discovered resources into the Resource Database

Leverage Browser Isolation for VDI-like Resource Access

Goal

Leverage Browser Isolation to replace VDI access at Acme for call center users and contractors.

Objectives

- Use iboss Browser Isolation to grant call center users access to sensitive applications through a pane of glass to provide data separation
- Applying Browser Isolation to BYOD, Guest or Contractors
- Provide agentless access to sensitive resources to guests and contractors through Browser Isolation guest sessions
- Provide shell access to contractors while requiring modern authentication using Browser Isolation

SOLUTION BRIEF

ABOUT IBOSS

iboss is a cloud security company that enables organizations to reduce cyber risk by delivering a Zero Trust Security Service Edge platform designed to protect resources and users in the modern distributed world. Applications, data and services have moved to the cloud and are located everywhere while users needing access to those resources are working from anywhere. The iboss platform replaces legacy VPN, Proxies and VDI with a consolidated service that improves security, increases the end user experience, consolidates technology and substantially reduces costs. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, Browser Isolation, CASB and Data Loss Prevention to protect all resources, via the cloud, instantaneously and at scale. The iboss platform includes ZTNA to replace legacy VPN, Security Service Edge to replace legacy Proxies and Browser Isolation to replace legacy VDI. This shifts the focus from protecting buildings to protecting people and resources wherever they are located. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking 4 billion threats per day. More than 4,000 global enterprises trust the iboss platform to support their modern workforces, including a large number of Fortune 50 companies. iboss was named one of the Top 25 Cybersecurity Companies by The Software Report, one of the 25 highest-rated Private Cloud Computing Companies to work for by Battery Ventures, and CRN's top 20 Coolest Cloud Security Companies of 2022.

To learn more, visit **www.iboss.com**.

+1 877.742.6832
sales@iboss.com

101 Federal St
Boston MA 02110

www.iboss.com