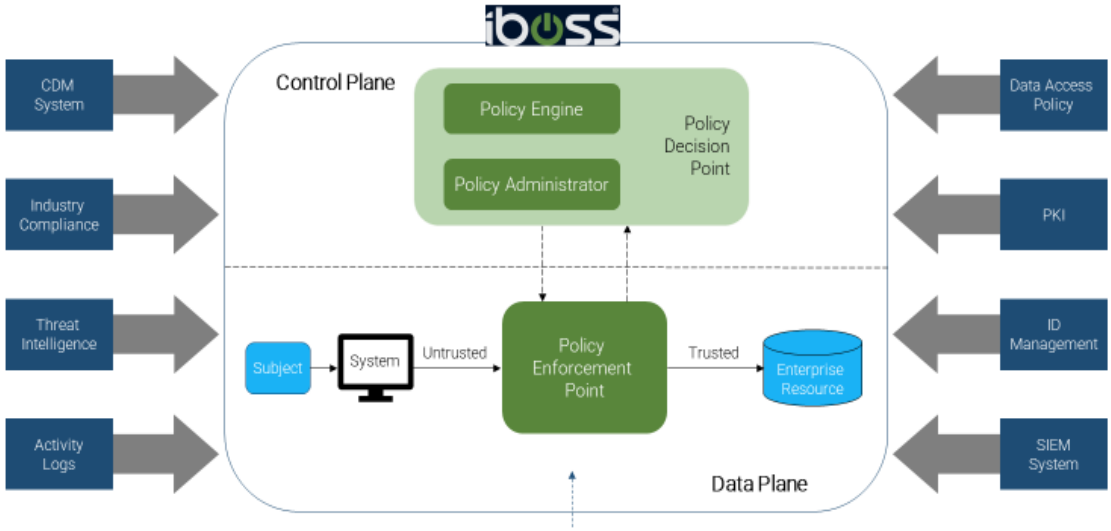
19309 Winmeade Dr. Suite 446
Leesburg, VA 20176

ATARC Zero Trust Working Group

Vendor Questionnaire

- **Is your solution/solution set comprehensive, covering all of the defined Zero Trust pillars? If not, which of the Zero Trust pillars does your solution/solution set cover? If there are gaps, do you have established relationships or partnerships with other vendors to fill those gaps?**

Logical Components of the Zero Trust Architecture from NIST SP 800-207



iboss acts as the foundational platform of the NIST 800-207 Zero Trust Architecture including the Policy Engine, Policy Administrator, Policy Decision Point and Policy Enforcement Point

5

The zero-trust security model is based on the principle of maintaining strict access controls and not trusting anyone by default, even those already inside the network perimeter. iboss acts as the core platform to meet the requirements as described in NIST S.P. 800-207, Zero Trust Architecture, by providing the policy engine, policy administration, policy decision point, and policy enforcement points, making decisions to grant or deny access to a resource. As outlined in that document

> *"Many of these TIC 3.0 security capabilities directly support ZTA (e.g., encrypted traffic, strong authentication, micro segmentation, network and system inventory, and others). TIC 3.0 defines specific use cases that describe the implementation of trust zones and security capabilities across specific applications, services, and environments. TIC 3.0 is focused on network-based security protections, whereas ZTA is a more inclusive architecture addressing application, user, and data protections."*[1]

[1] NIST S.P. 800-207, Zero Trust Architecture, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

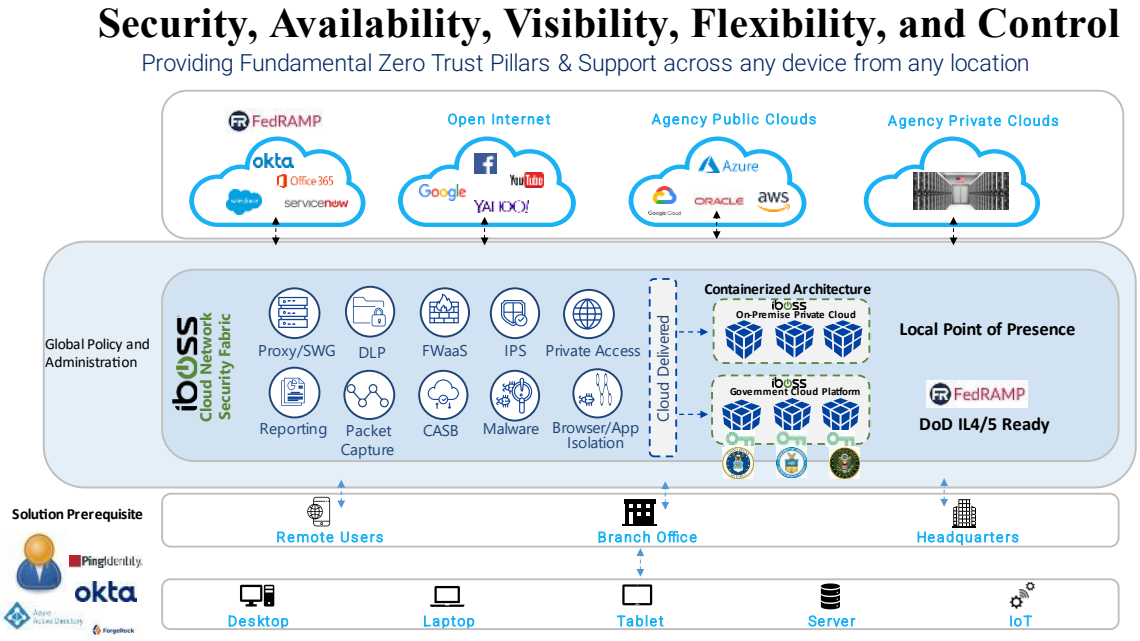
Within the IGCP, the Policy Engine (PE) is responsible for making the decision to grant or deny access to a resource for a given subject. The PE uses enterprise FAA policies in addition to input from external sources (e.g., Identity information, threat intelligence services, etc.) as inputs into the trust algorithm to grant, deny, or revoke access to the resource. The PE is paired with the Policy Administrator (PA) component; the policy engine makes and logs the decision (as approved, or denied), and the PA executes the decision. The Policy Administrator (PA) is responsible for establishing and/or shutting down the communication path between a subject and a resource (via commands to relevant PEPs) and generates any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. The PA is closely tied to the PE and relies on its decision to ultimately allow or deny a session. If the session is authorized and the request authenticated, the PA configures the Policy Enforcement Point (PEP) to allow the session to start. If the session is denied, the PA signals to the PEP to shut down the connection. The Policy Enforcement point (PEP) is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PA to forward requests and receive policy updates from the PA. Although this is a single logical component in ZTA, it may be broken into two different components: the client (e.g., an agent) and resource side (e.g., a gateway component in front of resource that controls access) or a single portal component that acts as a gatekeeper for communication paths (e.g. for non-enterprise managed devices or for IOT systems that cannot utilize an agent).

As outlined in the below graphic, a Zero Trust Architecture can't be instantiated, by deploying a single technology such as user identity, remote user access, or even micro-segmentation, rather Zero Trust is a foundational strategy to build from. Built on an open, API driven platform, iboss has both native and commercial integrations with leading vendor technologies within the Zero Trust ecosystem; although there are many capabilities required to effectively deploy a true ZTA, iboss believes following these core tenets are key steps to an Federal organization successfully implementing a Zero Trust Architecture:

1. **Zero Trust Access via IP Restrictions:** iboss provides organizations with unique IP addressing (or organizations can "bring their own IP space"); using the dedicated IP space preserves connections to private back-office providers and easily integrates with third-party technology providers that require dedicated IP addresses. It also ensures that organizations do NOT need to whitelist all cloud vendor IP addresses egressing back into their network (an operations & management quagmire) OR setup Source IP based Anchoring (which requires backhauling remote traffic through the TIC and increases the attack surface as it requires virtual hardware to be deployed in an Agency's DMZ). The non-shared Dedicated Source IPs allow all public applications to become private (via IP restrictions/ACLs) which ensure connections are only granted based on user identity. This allows access to public SaaS platforms (Salesforce, ServiceNow, etc.) by only connecting sessions coming from that agency's IP space, essentially turning a "public" application "private."
2. **Terminate Connections to Ensure Policy Enforcement:** Built on a single-pass inspection proxy architecture, iboss inspects all traffic at line speed (including decrypted traffic), interrogating the request against the requisite policies prior to connecting to the requested resource. Technologies such as firewalls, simultaneously inspect the traffic in conjunction with delivering the traffic to its destination. If a file containing PII is accidentally sent or perhaps a malicious file is detected via download, while alerts can be sent, the file has already reached its destination (external to the organization or on an internal endpoint, which is too late.
3. **Policy Granularity to Protect Data Based on Contextual Information:** iboss leverages integrations with identity platforms and performs device posture to verify access rights of the entity

requesting access to the resource, and it uses granular business policies based upon context, including user, device, the application being requested, as well as the type of content. Policies are adaptive, which means that as context changes, such as the user's location or device, the user access privileges are continually reassessed.

4. **Minimize the Attack Surface:** iboss connects users directly to the resource they are requesting, not to the network, like a VPN. This direct connection eliminates the risk of lateral movement by preventing a compromised device from infecting other network resources. With iboss, users and applications are invisible to the internet, so they can't be seen, and therefore cannot be attacked.



8

Salient Characteristics:

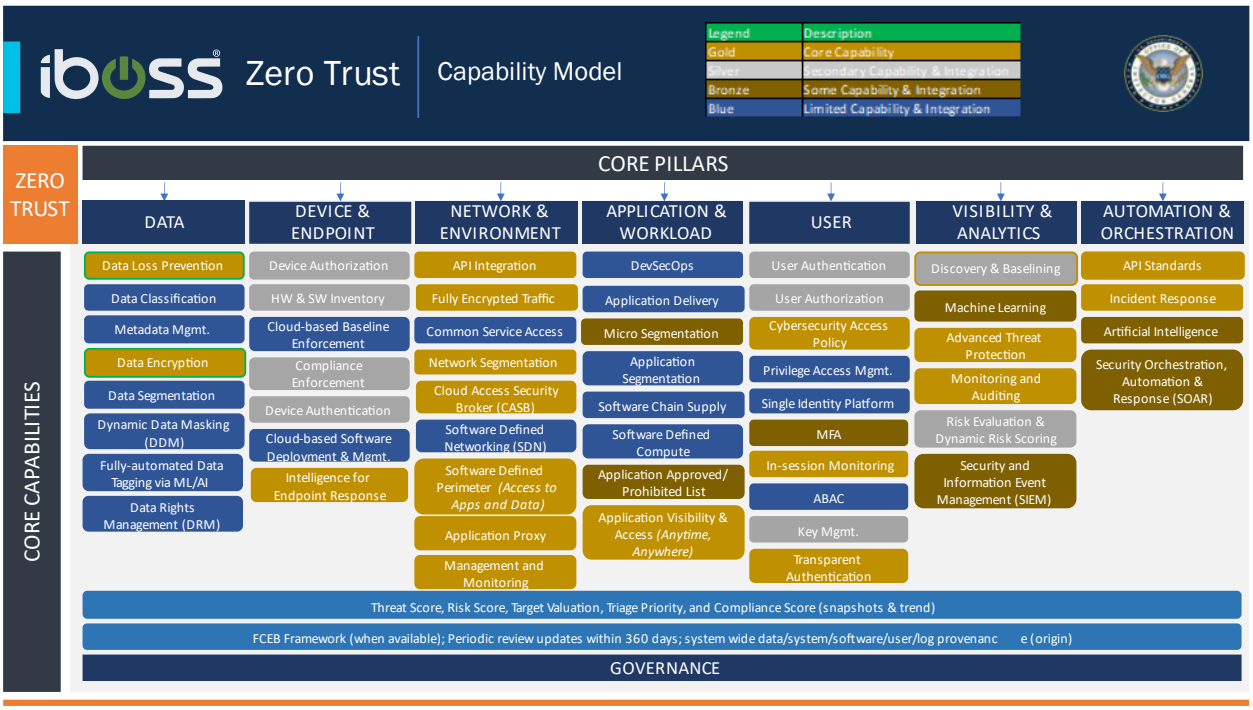
iboss' proprietary, containerized multi-tenant functionality ensures that Federal Departments and Agencies will have complete, consistent visibility and control over their network traffic while meeting the demands of the "work from anywhere" user community; each tenant in the IGCP is provisioned into their own environment, ensuring data remains separated and availability isn't impacted. This architecture provides the following benefits to organizations from a security and performance perspective:

- Unlike platforms that operate a shared gateway model where ALL government customer traffic is mixed and encryption keys are stored at the shared, enterprise gateway level, the IGCP's encryption keys remain at the individual tenant level. The iboss architecture eliminates the chance that encryption keys compromised in one tenant can impact another or lateral movement can occur between tenants within the cloud service.
- The iboss proprietary containerized architecture secures Internet access from anywhere, including in and out of the physical network perimeter. Containerization dedicates resources (gateways) for each organization in the service, delivering high availability and low latency while isolating customer traffic through their dedicated instance. This architecture also enables

horizontal scaling by adding additional resources to each tenant when needed (versus provisioning more bandwidth across the global environment).

- The iboss multi-tenant, containerized architecture also provides unique IP addressing; using the dedicated IP space preserves connections to private back-office providers and easily integrates with third-party technology providers that require dedicated IP addresses. It also ensures that organizations do NOT need to whitelist all cloud vendor IP addresses egressing back into their network OR setup Source IP based Anchoring, required by other SASE vendors. The non-shared Dedicated Source IPs allow all public applications to become private (via IP restrictions/ACLs) which ensure connections are only granted based on user identity. This allows access to public SaaS platforms (Salesforce, ServiceNow, etc.) by only connecting sessions coming from that agency's IP space.
- Because all tenant traffic is isolated in the IGCP, network administrators can easily understand where any network bottlenecks are occurring with the ability to pull PCAP data instantly, supporting the need for consistent visibility and control over the network environment. In a shared gateway model, customers are often required to contact the SASE provider's support organization to get complete visibility of routing for troubleshooting purposes and for simple network packet captures.
- iboss can extend its cloud architecture into agency private clouds (current TIC locations) with feature parity, enabling organizations to replace legacy proxy capabilities and providing global policy and administration delivered from the cloud.
- iboss provides native IPv6 addressing in support of OMB M-21-07, enabling D/As to address IPv6 requirements while moving to a Zero Trust Architecture, as required by EO 14028.
- The IGCP is comprised of one cloud-native platform, providing single pass decryption and inspection across each of the security microservices.
- The separation of data ensures that accidental data spillage across tenants will never happen, while traffic is mixed in a shared gateway model, increasing the risk that an accidental cross-contamination of data could occur.
- Agencies can run penetration tests or Red Team exercises against their IGCP environment without impacting the service of other tenants. As Federal organizations continue to move applications from the legacy data center to the cloud, being able to perform these critical security exercises on their cloud service providers will ensure D/As remain security diligent.

- **Describe (in detail) how your solution addressed each of the covered pillars.**



Shown in the graphic above, iboss provides different areas of coverage and capabilities across each of the Zero Trust pillars. The iboss, proprietary, containerized multi-tenant functionality delivered via the IGCP ensures that Federal Agencies will have complete, consistent, visibility, security and control over their network traffic while meeting the demands of the new, "work from anywhere" Federal community and satisfy the network requirements outlined in Executive Order 14208. Built on a containerized cloud architecture providing the foundation of the zero trust principles for secure connectivity outlined in NIST S.P. 800-207, the iboss Government Cloud Platform (IGCP) provides a multitude of security capabilities delivered via a cloud-native platform to allow Government organizations move to a Zero Trust Architecture as required by the recent Executive Order on Improving the Nation's Cybersecurity: Zero Trust Network Access, Secure Web Gateway, Malware Defense, Remote Browser Isolation, Cloud Access Security Broker and Data Loss Prevention to all connections, via the cloud, instantaneously and at scale. Containerization allows iboss to enable agencies to give users secure access to applications from anywhere, all while maintaining a completely isolated and controlled network data path, complete with horizontal scaling to ensure the fastest connections while minimizing latency. In addition, the unique architecture allows for natural hybrid-cloud deployments, stretching the cloud service, so proxy and firewall security capabilities can be delivered within the government network, providing global policy enforcement throughout the enterprise. With over 4,000 customers, iboss has the experience needed to help Federal organizations transition from protecting in-office workers to protecting their modern "work-from-anywhere" workforce while providing fast, secure and direct connections to any resource, from any device, under a true, zero-trust framework. A Gartner Magic Quadrant "Visionary", and backed by 230+ issued and pending patents, iboss processes and secures over 150 billion daily network transactions globally and is in process to be authorized at the FedRAMP Moderate level by the first quarter of 2022.

DATA

- Data Loss Prevention: DLP is a core service within the IGCP. The Data Loss Prevention (DLP) service is native to the IGCP, providing rich functionality and rulesets for both Data in Motion as well as Data at Rest. Additionally, the iboss DLP service enforces policy on AIP labels of sensitive O365 documents to prevent data loss transfers to personal cloud environments (e.g. a user accidentally saving a sensitive document to their personal Dropbox account).
- Data Classification: iboss does not perform any Data Classification
- Metadata Management: iboss does not perform Metadata Management
- Data Encryption: iboss performs single pass encryption & decryption of network packets as they traverse through the IGCP service. The majority of nation-state attacks, including recent ransomware attacks attributed to nation-state aligned actors, are hidden in encrypted traffic. Subscribing to the IGCP will enable Federal agencies to achieve visibility quickly and easily into encrypted traffic vs. updating legacy security tools
- Dynamic Data Masking (DDM): iboss doesn't provide DDM functionality
- Fully Automated Data Tagging via ML/AI: The IGCP does not provide Data Tagging
- Data Rights Management: iboss doesn't perform Data Rights Management actions

DEVICE & ENDPOINT

- Device Authorization: Device Authorization in the iboss platform is performed using security groups and policies. Varying on the method of connectivity into the iboss platform (Cloud Connector, IPsec, GRE, Explicit, or even on prem). Iboss can assign users to a group defining access and control specifically defined by but limited to: IP destinations, categories, SaaS applications, TCP ports, Protocols, Domains, etc.
- Hardware & Software Inventory: iboss can work in conjunction with a CDM system containing HWAM/SWAM info to allow for Agencies to establish conditional access policies.
- Cloud-Based Baseline Enforcement: iboss does not provide cloud-based baseline enforcement for devices or endpoints
- Compliance Enforcement: The iboss cloud connector (CC) client gathers telemetry around various configurations on the endpoint that is leveraged by the trust algorithm, such as the presence of a client certificate or a current antivirus engine. If the policy conditions are not met, the connection can be denied, or it can be assigned to a security group with controlled access. If the connection is allowed, all subsequent content will be scrutinized and if certain thresholds are met, additional actions can be taken.
- Device Authentication: The iboss platform supports Active Directory authentication for single sign-on, including identity providers using SAML, Azure AD, ADFS, OpenID, and other iDP's for gateway authentication scheme.
- Cloud-Based SW Deployment & Management: iboss doesn't deploy or manage devices or endpoints, it works in conjunction with them through an open API. The iboss cloud connector is installed manually via an .msi or pushed through a deployment tool such as SCCM, Intune etc. An agent policy

in the iboss platform presents the ability to perform an Auto-update for the installed cloud connector on the end points as new versions become available, and totally transparent to the user.

- Intelligence for Endpoint Response: As the source of information for all network activity, the IGCP provides all critical network telemetry on every session, ensuring Incident Responders have complete network visibility to correlate with information that they've seen at the endpoint.

NETWORK & ENVIRONMENT

- API Integration: iboss has a RESTful API offering access to data, resources, and processing routines to integrate with any internal security stack, SIEM, EDR, and threat intel platform
- Fully Encrypted Traffic: A core capability of the IGCP is full encryption and decryption of network traffic
- Common Service Access: iboss does not support Common Service Access.
- Network Segmentation: iboss presents network segmentation through either our cloud or on-premise offering. Iboss' unique containerization architecture establishes granular network separation.
- Cloud Access Security Broker (CASB): CASB is a core capability of the iboss SASE platform. The IGCP's CASB microservice can additionally support integration with Microsoft Cloud Application Security (MCAS) from a log sharing and visibility perspective; with any application signature that Microsoft receives, iboss automatically applies that signature to all apps, extending the MCAS capability to non-Microsoft SaaS applications. The CASB capability provides complete visibility into any cloud-based application or custom definition for remote or on-premise personnel would possibly access through a secure portal.
- Software Defined Networking (SDN): iboss does not perform SDN functions
- Software Defined Perimeter (Access to Apps & Data): iboss' recognizes Software Defined Perimeter as access to resources using a zero-trust model. the iboss Private Access feature includes a foundation to control access to private or public resources granted by tightly coupled SAML integration. The iboss platform is based on containerization architecture supporting a customer dedicated and unique source IP addresses, that identifies only those subscribed users to establish connectivity to their SASE service using a zero-trust model.
- Application Proxy: The iboss platform offers application proxy capability for any TCP based protocol (such as HTTP, HTTPS etc), with the ability to perform SSL Decrypt traffic, observe and parse the clear text payload, then re-encrypt the traffic to the destination.

APPLICATION & WORKLOAD

- DevSecOps: iboss does not perform DevSecOps functions
- Application Delivery: iboss doesn't provide Application Delivery capabilities.
- Micro Segmentation: iboss doesn't provide micro segmentation.
- Application Segmentation: iboss works in conjunction with other platforms or tools focused on application segmentation to deliver identity based micro-segmentation capabilities.
- Software Supply Chain: iboss doesn't monitor the software supply chain
- Software Defined Compute: the IGCP does not provide SDC capabilities
- Application Approved/Prohibited List: The iboss CASB microservice monitors and reports on discovered user to application traffic to common SaaS applications. Application controls can be enabled to prohibit application access while approving others. Additional features enable one to configured for evasive protocol control (such as TOR, FTP etc), port control (TCP/UDP and direction),

Custom CASB definitions can be defined by the administrator to identify and control user defined applications.

- Application Visibility & Access (Anytime, Anywhere): iboss proxies traffic to applications, providing visibility and access for users and contains detailed reporting info to understand what users accessed which applications for how long and from what location.

USER

- User Authentication: The iboss platform supports Active Directory authentication for single sign-on, including identity providers using SAML, Azure AD, ADFS, OpenID, and other iDP's for gateway authentication scheme.
- User Authorization: Authorization policies are applied to the system via Dynamic Linking. Authorized users' movement, control movement are enforced and can be applied to policies associated with Allow/Block lists, Private Access, DLP, Malware Enforcement, and Bandwidth shaping just to name a few.
- Cybersecurity Access Policy: Using the iboss platform, one can create cybersecurity access policies and be associated to users and/or groups, which can comply uniquely to an acceptable use policy, or deny access to a destination(s), but also protect against malicious downloads or even exfiltrating sensitive data from the client.
- Privilege Access Management: iboss does not provide PAM capabilities
- Single Identity Platform: iboss is not a single identity platform
- Multi-Factor Authentication (MFA): iboss can work in conjunction with MFA platforms
- In-Session Monitoring: User in-session monitor is performed in real time as a user advance through the iboss platform. Events are creating mapping individual users' movement which include time/date, IP address, usernames, user agents, URI's, category matching, ports used, user agents, bytes, just to name a few. With the power of the containerized architecture, iboss enables administrators to perform PCAP's of user traffic for assisting in client troubleshooting. Registration or Cloud Connector monitor presents additional monitoring to paint a picture of what policies a user is matching on, capturing their geographic location, operating system, MAC address, local IP / public IP address with the ability to revoke their access.
- Attribute Based Access Control (ABAC): Not applicable, iboss doesn't provide ABAC for Users
- Key Management: Key Management is supported with HSM integration in iboss' IGCP FedRAMP environment.
- Transport Authentication: iboss supports Transport Authentication where a user-agent authenticates to an origin server while guaranteeing freshness and without the need for the server to transmit a separate authentication session with the user agent.

VISIBILITY & ANALYTICS

- Discovery & Baselining: iboss demonstrates network discovery using our CASB service to detect and report access to cloud applications. The iboss API-based CASB feature also enables out-of-band malware and DLP scanning of files and data stored within enterprise cloud services, such as Box, Microsoft 365, and Google. Iboss also integrates with Microsoft Cloud App Security extending data at rest within DropBox, Box and other popular cloud applications. Signatures are automatically

synchronized with iboss to ensure data is protect while in motion (between users and the cloud) and at rest (e.g. within Sharepoint). Baselining is presently being reviewed as a viable platform feature.

- Machine Learning: iboss does not provide a customer front facing ML interface, however, performs backend classification that utilizes Dynamic Page Content Inspection for uncategorized sites. Utilizing the hybrid cloud classification engine, when a site is updated on any iboss solution, that classification is pushed in real time to all iboss solutions connected to the gateways. This ensures the latest threats are classified and defended against.
- Advanced Threat Protection: iboss' Threat Intelligence Protection allows integration with continuous security feeds from over 50 best of breed anti-malware engines including iboss' network and threat intelligence to mitigate malicious threats delivered to the end user. Through the cloud-native architecture, updates from each of these engines are in continuous synchronization, eliminating the static updates of engines, which creates breach exposure windows. Engines include C&C, IP reputation, signatures, heuristics, phishing defense, and AI.
- Monitoring & Auditing: The IGCP provides detailed monitoring and auditing information across each of the security microservices featuring event logging and reporting and establishing alerting thresholds and actions which can be configured to automatically alert when certain actions are detected. Email alerting for critical
  events and high-risk behavior are built into iboss cloud throughout the platform. Real time alerting can be setup for things such as evasive behavior, keywords and search terms, high risk category monitoring, URL exceptions, scheduled reporting, Malware sandboxing and malicious high-risk browsing activities. iboss also provides an Incident Response Dashboard which provides complete historical information as to who, what, when and history against the user/device causing the alert and why it was triggered.
- Risk Evaluation & Dynamic Risk Scoring: The IGCP provides risk analysis by identifying potentially compromised sites that have not yet been classified by reputation or signature-based malware engines. This capability analyzes various aspects of a request, including the URL, HTTP headers, and site content. Based on that score, the page is either blocked or allowed depending on the thresholds for Low Risk, Medium Risk, and High Risk, providing users with visibility and context.
- Security Information & Event Management (SIEM): The IGCP integrates with industry leading commercial off the shelf (COTS) SIEM tools, such as Splunk, MS Defender, IBM Q-Radar, and others. Logs can be automatically forwarded from the IGCP to SIEMs, either on-premise or in the cloud tools and no additional licensing or software is required.

AUTOMATION & ORCHESTRATION

- API Standards: The documented and detailed RESTful API of iboss offers access to data, resources, and processing routines to integrate with Security Orchestration, Automation, and Response (SOAR) platforms to expedite the incident response process.
- Incident Response: Incident Response Center monitoring component provides single-pane-of-glass reporting on infected devices on a customers' network, giving instant visibility into a wealth of information for IR needs, including: compromised machines, infection type, user, Command and Control (C&C) Callbacks, the average dwell time of infections (i.e. how long since discovery the infection became active on the network), and the total amount of malware that has been blocked trying to enter the network.

- Artificial Intelligence: As noted above, the IGCP contains multiple security feeds and engines, as the IGCP receives new information, the AI/ML utilities can help automate the incident response process, through explicit policies or through behavioral analytics and integration with SOAR platforms.
- Security Orchestration, Automation, and Response: The IGCP can integrate with SOAR platforms through the API

- **Does your solution/solution set allow for non-traditional assets (i.e. IoT devices)? If so, please detail the specifics.**

Yes, the IGCP includes a Reverse Web Proxy (RWP) service, a Guest Access service, and a Cloud Application Isolation service that enables the security controls in the platform to be applied to non-traditional IT assets, such as IOT devices, many which can't have an agent installed on them. The flexible architecture supports each of the four notional architectures in SP 800-207, allowing for the PEP to be delivered through the FedRAMP cloud service (IGCP) or as an on-premise gateway, or in any combination, while enabling global policy management.

- **Are there existing, operational implementations of your solution in either government or industry? Can you provide customer references?**

Yes / Yes. iboss has over 4,000 customers across Government and industry. Customer references can be provided after interested parties execute a Non-Disclosure Agreement (NDA). Customer success and supporting our customers is key tenant in the iboss company philosophy; iboss scored 4.7 out of 5 overall & 4.7 out of 5 for support, in the recent Gartner Peer Insights Survey https://www.iboss.com/blog/iboss-named-a-2021-gartner-peer-insights-voice-of-customer-swg/ . Our proprietary cloud architecture allows our SLA to provide our FedRAMP customers with 99.999% guaranteed uptime while providing Mission Critical level support. The iboss CNOC (Cloud Network

Operations Center) monitors the IGCP service 24x7x365, working with Technical Account Managers and key client personnel to collaboratively resolve any service issues.

- **The government will not transition to a Zero Trust environment by flicking a switch. State how your solution will co-exist with legacy approaches during a transition.**

The IGCP's adaptable architecture and licensing model facilitates Agency modernization strategies by integrating with legacy technologies and allowing Agencies to leverage existing assets as they move toward a Zero Trust environment over time. According to Gartner, "To protect anywhere, anytime access to digital capabilities, security must become software-defined and cloud-delivered, forcing changes in security architecture and vendor selection. SASE is a pragmatic and compelling model that can be partially or fully implemented today." (Gartner, Strategic Roadmap to SASE Convergence, March 2021) However, as individual agencies are in different stages of IT maturity, moving toward a Zero Trust Architecture as part of their digital transformation is a journey specific to each organization. For example, a "cloud-forward" agency that has many of their applications already in the cloud could choose to implement the IGCP to replace their legacy TIC/Data Center security tools on day one. Another agency could want to leverage the IGCP to replace their legacy VPN and CASB solutions in FY 2022, then look to implement DLP, SWG, and other functions in 2023. The majority of Federal customers are creating a multi-year, multi-stage plan for modernization, easily supported and facilitated by the IGCP's hybrid architecture, open API driven platform, and flexible licensing model.

- **How does your solution detect, identify, and handle failures, suspect activity, possible exploits, etc.?**

This is a difficult question to answer as it covers a broad scope. The IGCP can identify the following types failures: failed DNS queries for iboss proxy requests on behalf of the client, failed proxy access for iboss proxy requests on behalf of the client to their intended destination, all remaining proxy errors for iboss proxy requests on behalf of the client, and PAC Script Download Failures (including syntax and registration failures), etc. Regarding suspect activity identifying/exploits, The Incident Response Center monitoring component provides single-pane-of-glass reporting on infected devices on a customers' network, giving instant visibility into a wealth of information for IR needs, including: compromised machines, infection type, user, Command and Control (C&C) Callbacks, the average dwell time of infections (i.e. how long since discovery the infection became active on the network), and the total amount of malware that has been blocked trying to enter the network. The High-Risk Machines section of the Incident Response Center is designed to show machines within the organization where a high-risk connection occurred or where 50 connections or greater were made to domains hosting malware. This gives the administrator a quick and easy way to see the overall machines exhibiting high-risk behavior, whether the machine is still infected, the type of behavior triggered the high-risk, and the last date of communication for the connection or malware. The Recently Cleared Machines area of the Incident Response Center is an audit log of machines that were once infected but have been cleared by the administrator. When iboss sees an infection communicating on the network, it flags that machine as infected. The administrator can then clean the infection on the machine and mark it as clean within iboss. Exploits can also be prevented through the implementation of iboss SSL Decrypt and administration capabilities, Malware Detection/Prevention, implementing a firm and effective policy to block older vulnerable operating systems & browsers, and to include a content filtering policy for users destined for websites that are malicious in nature or unknown by the iboss threat defense platform

- **An on-premise end-user device is compromised by an outside party. How does your solution contain the impact of this exploit?**

As outlined in the above answer, the Incident Response Center monitoring component within the IGCP provides detailed visibility into compromised devices; depending on the device type, exploit type, and policy, the impact could be contained through various courses of action. Once a user is identified as compromised, their status can be revoked disabling their to the customers instance. Furthermore, integration with an EDR platform could result in another type of containment action using the iboss API.

- **How does your solution prevent the impact of insider threat?**

Iboss helps prevent the impact of insider threat through granular Role-Based Access Control (RBAC) capabilities based on least privilege principals, ensuring users can view, access, and modify only information they are entitled to per agency policy. The IGCP has visibility into all traffic that traverses the platform, providing visibility into users, devices, and application connections, outlining what people are connecting to and the actions they are taking. From
an iboss perspective, a rich audit trail provides information outlining the specific areas of the platform that have been accessed by users, enabling agency auditors/investigators to identify potential anomalous behavior. Additionally, detailed log information can be automatically sent from the IGCP to other agency tools to perform more in-depth analysis if desired.

- **Using the recent Solar Winds event(s) as a backdrop, how does your solution address supply chain issues?**

iboss doesn't address supply chain compromises like the Solar Winds recent attack, which was extremely difficult to identify; these types of attacks can be amongst the most difficult to unearth. However, utilizing a defense in depth approach gives the greatest chance for detection. The IGCP's full traffic decryption gives us the ability to examine data as it passes through the IGCP to Federal networks, this leads to much higher detection rates. iboss utilizes a combination of feeds, signature, and heuristic based detection technologies that are constantly being updated to ensure that Federal Agencies are protected against the latest threats. In addition, our DLP engine technology assists in detecting and blocking data exfiltration attempts.

- **Describe interoperability with other vendors' solutions.**

As mentioned above, the documented and detailed RESTful API of the IGCP offers access to data, resources, and processing routines to integrate with a variety of complimentary vendor solutions, such as IDP, EDR, SIEM, and SOAR platforms, allowing Agencies to architect a Zero Trust platform covering each of the pillars.

- **Most agencies will have a mix of cloud and traditional data center environments. Describe how your solution works in hybrid environments (legacy and cloud).**

The iboss SASE platform provides network security as a service that can be delivered from the IGCP, an on-premise data center, via Microsoft Azure, or in a hybrid fashion encompassing any of the above, providing flexibility to agencies as they modernize their environment and move towards a Zero Trust architecture. The containerized architecture of the iboss service allows gateways to stretch into private points of presence at any desired location (agency data center, branch office, etc.), extending the reach of the cloud service into desired locations. As a cloud-native platform leveraging a multi-tenant architecture built on the concept of containers and microservices, the data plane is separate from the control plane, allowing organizations to centralize the management & policy enforcement across the enterprise, regardless of the architecture.

- **How can agencies leverage existing investments in your solution (cost is one of the main concerns we've been hearing from the working group, so this is an important aspect of the overall solution).**

The flexibility that iboss provides from both an architecture and licensing perspective enables Federal agencies to capitalize on their existing investments and utilize their available funding as they modernize their architecture to comply with Executive Order 14028.

- Architecture: as outlined previously, iboss is the only SASE vendor that provides a complete, hybrid model, allowing agencies to utilize either the IGCP, deploy in an on-premise fashion, or in combination – extending the security edge of their perimeter from the cloud to their private cloud (agency data center) applications for a consolidated approach to Zero Trust for secure connectivity.
- Licensing: iboss provides unlimited licensing for Government customers, enabling them to structure a licensing model aligned to their deployment needs. This flexibility allows agencies to align their resources and funding appropriately as they modernize their architectures in a predictable, efficient manner.

For example, an Agency could have a multi-year project where the first step is to eliminate VPN usage and implementing TIC 3.0 policies for their remote users, allowing personnel to go direct to the internet. The second phase could be allowing personnel to access FedRAMP SaaS applications, and the third phase could be to retire their legacy TIC-based Secure Web Gateway appliance/s. The unlimited licensing model

allows the Agency to onboard into the IGCP in conjunction with the project rollout and funding, maximizing the Agency efficiency of the budget while providing the services when the agencies require them.

- **How will the vendor integrate with a trust algorithm? Will this be something that the vendor would like to provide or something they expect agencies to create in house? (This is in reference to NIST 800-207)**

The global policy engine within iboss governs the entire platform, built on "least privilege" principles and through integrations with identity platforms and other asset databases, iboss provides the "trust algorithm" outlined in NIST 800-207, as previously noted, making the critical decision to grant or deny access to an enterprise resource.

Access request: iboss proxies the request from the subject (via an encompassing the resource requested and the primary information from the requester via the IDP. This can include OS version, software used (e.g., does the requesting application appear on a list of approved applications?), and patch level. Depending on these factors and the asset security posture, access to assets might be restricted or denied.

Subject database: iboss works in conjunction with the Identity platform to allow for a collection of privileges to govern access to applications. The iboss global policy engine is built on "least privilege" principles to enable very specific roles and access to be granted to subjects in the enterprise depending on use-case and business or mission need.

Asset database (and observable status): The iboss global policy engine works in conjunction with this database that contains the known status of each enterprise-owned (or BYOD) asset. This is compared to the observable status of the asset making the request to iboss and can include attributes such as: OS version, software present (e.g., antivirus), location (network location and geolocation), and patch level. iboss can restrict or deny access depending on the asset state and policy.

Resource requirements: This set of policies that complement the user ID and attributes database defines the minimal requirements for access to the resource. Requirements may include authenticator assurance levels, such as MFA network location (e.g., deny access from overseas IP addresses), data sensitivity, and requests for asset configuration that would drive the policy creation in iboss.

Threat intelligence: As noted previously, iboss provides threat intelligence from 50 different sources as part of the IGCP service about general threats and active malware operating on the internet. iboss also provides specific information about communication seen from devices that may be suspect, such as queries for possible malware command and control nodes, which is available in the incident response dashboard.