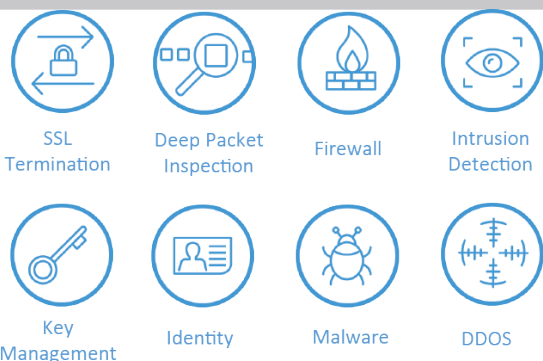




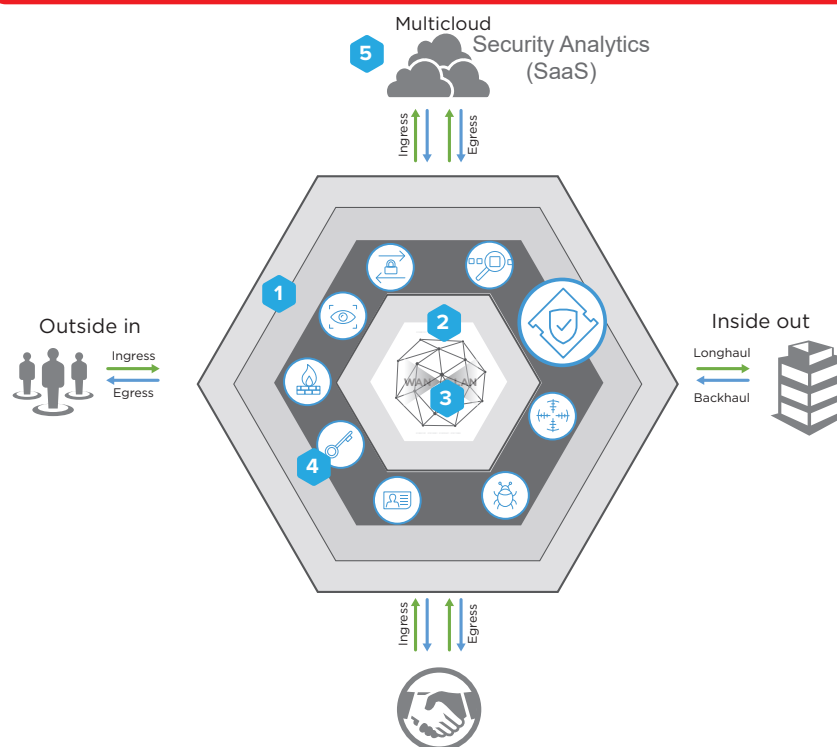
## Design Principles

- Defense in depth.
- Secure communications.
- Reluctance to trust.
- Service authentication/authorization.
- Principal propagation/authorization.
- Tamper proofing.
- Replay protection.
- Injection protection.
- Password/credential protection.
- Multifactor authentication.
- Least privilege.
- Enumeration.
- Weakest link.

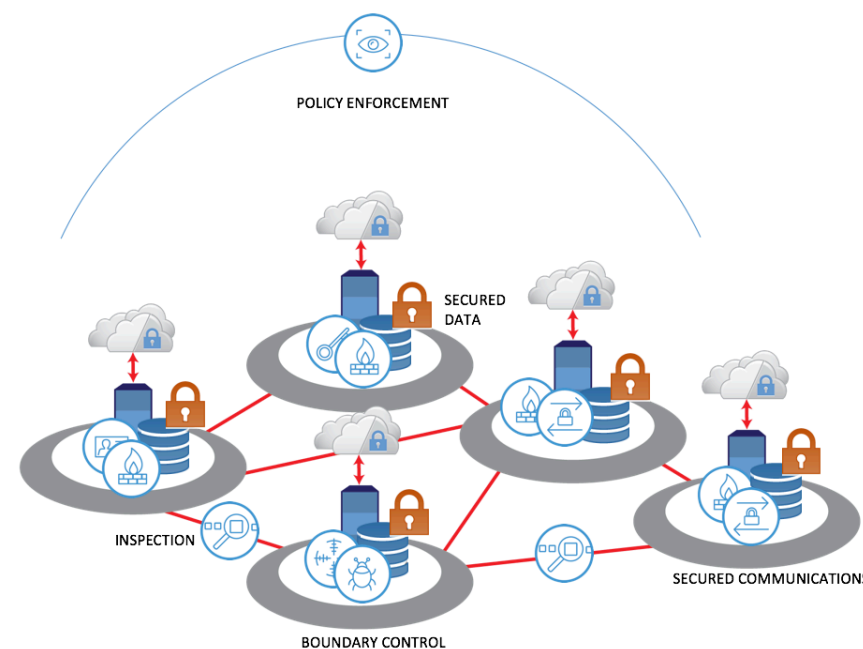
## Edge Node Components



To secure the digital edge, you need to be prepared for multicloud application and data flows, servicing people, employees and partners across multiple networks. It goes beyond a gate, or a wall; it is now more equivalent to airport security with domestic and international traffic and different classes of service. After checking identity and authorization (to even go through airport security, or to travel at all), every item is scanned and digitally interrogated regardless of destination. It is a trust-nothing model analogous to digital edge.



## Create Security Guardrails



## Capabilities

- Localized security and secured communications at the edge.
- Fine-grained controls in place for data and application layers.
- Control use of all cloud services and enable shadow IT without the risks.
- Ability to adapt to new business models and flows dynamically.
- Capabilities scale with cloud service augmentation in any or all regions.
- Low-latency attributes of the node design enable real-time capabilities that were otherwise impractical.
- Security and risk are business enablers, not barriers.
- Ability to leverage security innovation at the speed of digital.
- Gain visibility into unsanctioned cloud consumption and apply real-time policy controls.
- Gain deep packet inspection capability for cloud and SaaS services.
- Apply existing security tools and controls against cloud services.

## Edge Node Deployment

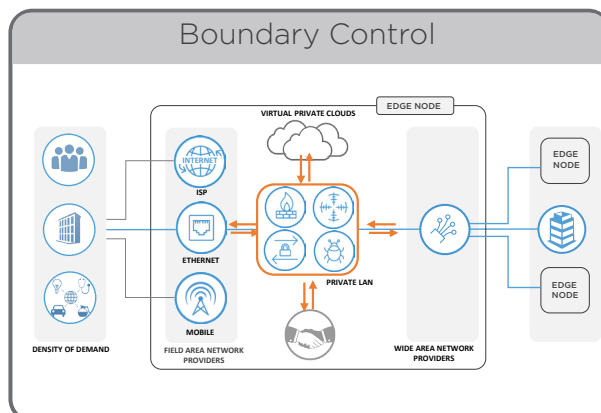


Implementation is typically a mix of physical and virtual appliances with supporting SaaS services. Plan for half a cabinet in your edge node design.

## DESIGN PATTERNS

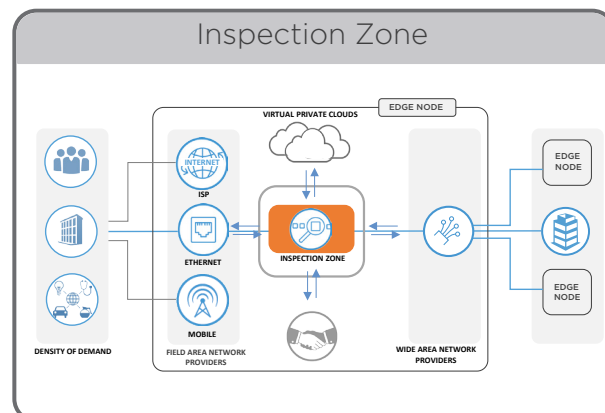
### 1 STEP 1

With the redefined edge, intersecting cloud and B2B traffic with field networks and corporate backbone, a new kind of digital border control is required.



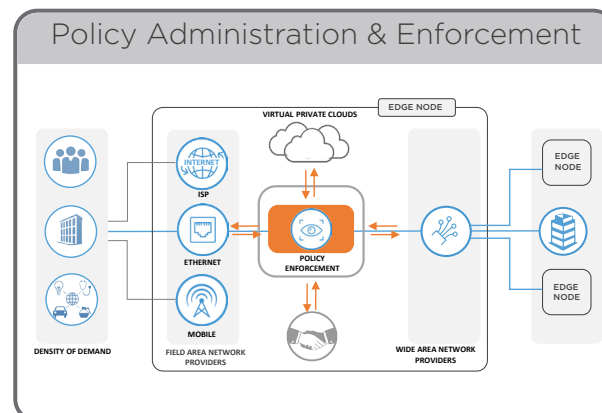
### 2 STEP 2

What was traditionally done with a perimeter DMZ now needs to be distributed to scale with each edge node. Intersection points provide a unique control point for all traffic.



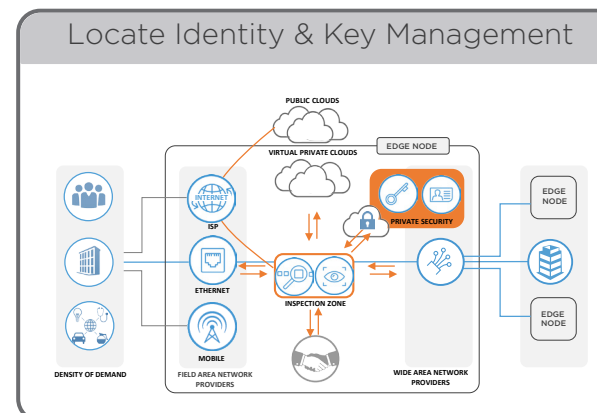
### 3 STEP 3

We segmented the traffic, but now need more fine-grained prescription on what is allowed within the flows. Services and mobile apps will be changing rapidly, requiring stronger governance.



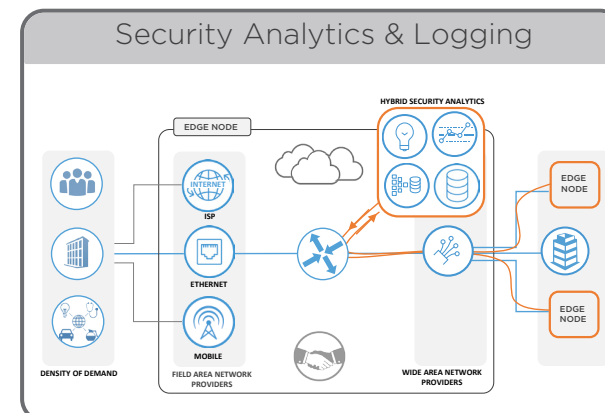
### 4 STEP 4

The node design provides extremely low latency but only if the reasons for traffic to leave are reduced. Colocate high-dependency services in the node and scale as more nodes are deployed.



### 5 STEP 5

Link all of these controls together with security (and network) analytics to not only make sure all the doors and windows are locked, but ensure that everyone is in the crowd is behaving.





**Problem**

Effective boundary control proves difficult when the edge has been redefined across mobile, cloud, B2B and traditional networks. The majority of traffic is shifting out into the untrusted side of the traditional perimeter. For some, the perimeter has ceased to exist.



**Solution**

Based on the IOA Network Blueprint\* as the foundational layer, implement new boundary control inside your geographical edge nodes at the ingress and egress points of segmented traffic flows. This is the closest point to users, clouds and business partners, and the ideal location for a standardized set of hybrid boundary services (i.e., that leverage Security SaaS, over multicloud connectivity, by design). The primary objective is to solve boundary control locally. Using airport security as an analogy, in this solution we are establishing the first checkpoint to determine if the actor has a valid reason to continue inside the security zone, with the exception that we are following a “zero-trust model” and challenging both ingress and egress. The types of things to block, or redirect, are not functionally different (if security is current); they are just now applied in distributed intersection points, with hybrid capabilities, and tailored according to what you need in each metro location (e.g., if its an IoT edge — tailor for that).



**Constraints**

1. While network defense has always been concentrated on securing "the edge," with the advent of mobile, cloud and digital ecosystems, the "edge" has been redefined.
2. For those still living with the traditional perimeter model, there effectively is no single edge anymore. There are many edges. This makes traditional protection methods increasingly ineffective yet still expensive.
3. Much of what security needs to protect against is occurring closer to the user, and so the protection also needs to be close to the user. Centralized protection is far from everyone.
4. Backhauling and converging traffic is creating bottlenecks, impacting performance and requiring very large and expensive security equipment that ultimately provides a questionable return on protection.



**Steps**

1. Determine the security policies and filters for each flow of traffic segmentation (Network Blueprint\*).
2. Next determine the local volumes and arrival rates of each flow to size the boundary services.
3. Qualify the expected latency overhead. Note, you can add more security as your starting latency was already exceptionally lower than before.
4. Size the services and review placement options. Use physical/virtual appliances in the node and/or potentially extend with Security SaaS. Overall demands are typically lower in a distributed model vs. centralized.
5. Apply the boundary stack across all network types: Field Area Networks, Internet Peering, Multicloud, Digital Ecosystems (B2B) and Metro WAN links to other hubs/corporate data centers.
6. Log everything for later pattern analysis.



**Forces**

- Cyber attacks are on the rise, and with the shift to digital business models and increased business dependency on technology, the impact of those cyber threats is also increasing.
- New forms of digital engagement with customers, employees and partners are being adopted every day and are becoming the dominate forms of business communication and processing.
- Likewise, digital services and ecosystems are connecting to transact (messaging). Applications are being assembled from a set of networked APIs from different sources. How do you know any of those have not been compromised?
- Lastly we have the advent of IoT. Millions of mobile and stationary 'things' try to report in.

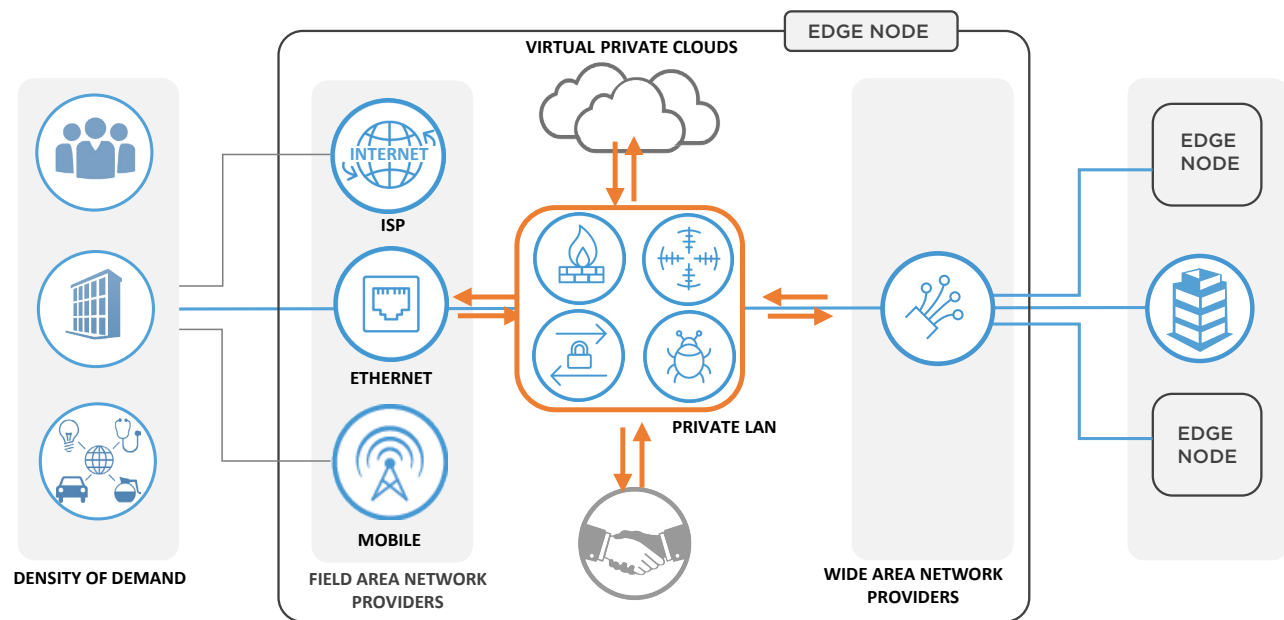


**Results**

- You have localized security controls by placing security boundaries as close to where business is executed as possible (same data center).
- Field network traffic only crosses the internet locally, and all other traffic is on private networks (dramatically reducing attack vectors).
- Capitalize on the latency advantages and implement more security, governance and controls which would have otherwise negatively impacted user experience or scale.
- The distributed edge nodes, with load-balanced traffic across the mesh, already minimize impact of attacks in any one location.
- This alleviates the impact on user experience (which is how companies usually find out they are being attacked).



**Reference View**



\* Network Blueprint — IOAKB.com



### Problem

Applications and business processes are becoming more distributed, more granular (services), more mobile and more automated. With increasing business impacts and dependencies, the need to observe interactions and flows has greatly increased, but the ability to do so has not.



### Solution

Having applied the IOA Network Blueprint\* as the foundational layer, and boundary control in the edge nodes, the solution to monitoring digital engagement and traffic is to create an inspection zone in each of the edge nodes, positioned at the intersection point of all networks, flows and traffic. This puts your controls back at the center of the network (in order to improve intrusion detection and prevention, or stop data leakage, etc.) and provides the perfect location to capture data for later analytics—not just for security, but for many analytic use cases. Extending our airport security analogy, border control allows entry into the security zone, but then what is being carried needs to be inspected before it can be allowed through (again regardless of arriving or departing in this case).



### Constraints

1. Integrating ecosystems in today's multicloud and multinet environment requires a zero-trust model that goes well beyond the capabilities of a traditional perimeter model.
2. There are various techniques to observe network traffic in order to monitor interactions and flows. However, traffic is shifting to the edge and with trends such as the consumerization of IT and direct cloud access occurring, inspection points are not available or are being bypassed.
3. Even if you could backhaul all the traffic, the volume continues to increase and centralizing that volume quickly overwhelms the inspection point.
4. As customers and employees become more mobile, security needs to be able to follow the user no matter the location or device. Traditional models are static and more limited.



### Steps

1. Determine what levels of monitoring will be applied to each segmented network flow, the amount of data captured or generated per event being processed, and what the expectation on arrival rates and projection of growth will be.
2. Size and deploy the appliances into the edge node and route authorized and authenticated traffic from boundary control into the inspection zone.
3. Apply real-time traffic analysis in this way across each of the distributed edge nodes — logging and aggregating the data for global monitoring and analysis.
4. Leverage the inspection zone to help follow the user and apply user-centric security models.



### Forces

- We are developing more complex systems, in shorter time frames, with increasing business dependence on less understood technologies, that all require greater partner and provider trust. The need for control is increasing disproportionately to the ability to control.
- More dynamic and adaptable approaches are needed to monitor traffic (which is becoming synonymous with business and commerce).
- To build advantage in the digital economy, algorithms are needed to provide insights that help decision support – like improving security, detecting intrusion, and automating efficient responses to our pace cyberbots. This starts with having useful data about traffic and interactions.

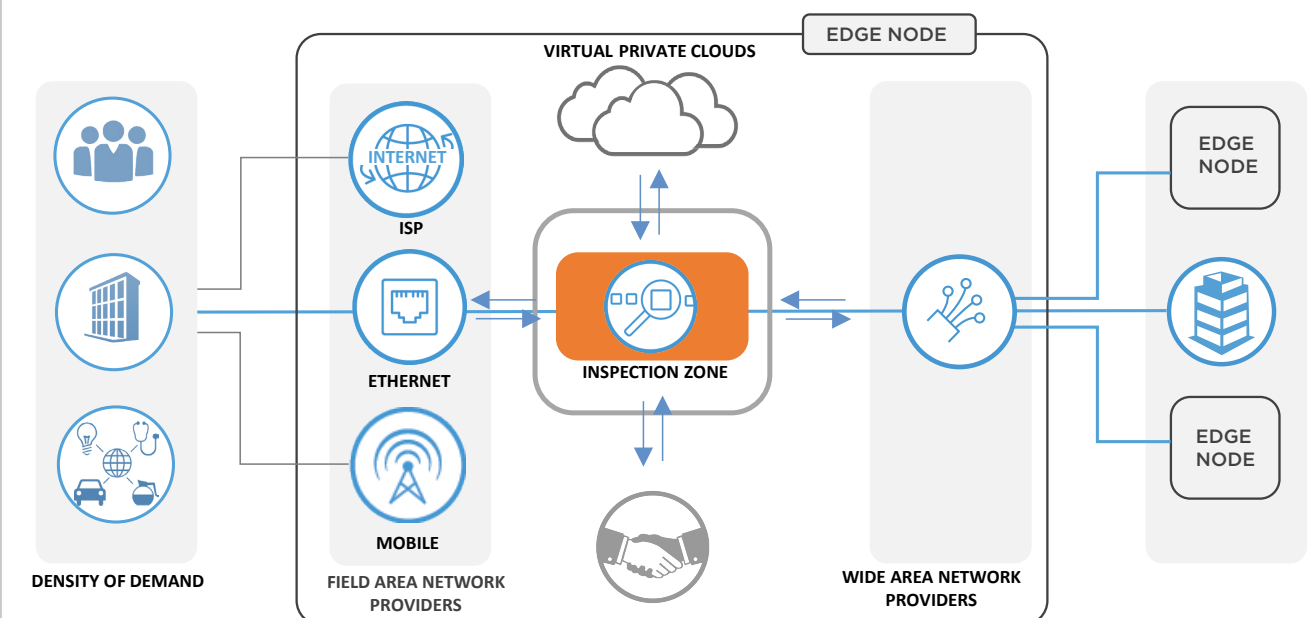


### Results

- Now all traffic and interactions across network segments can be monitored and logged.
- Distributed inspection zones at high-bandwidth and lowest-latency intersection points allows this service to efficiently scale.
- The ability to leverage cloud ecosystems (and security service innovation) with a low-latency cross connect presents opportunity.
- As new cloud services are added, they can automatically be monitored. In addition, interactions between cloud services can be routed through the inspection zone (even from the internet).



### Reference View



\* Network Blueprint — IOAKB.com





## Problem

More complex systems are being assembled, in shorter time frames, with increasing business dependence on less understood technologies. New guardrails are needed to protect people and the company from mistakes or unsanctioned behavior.



## Solution

As the third Security step with the Network Blueprint\* layer as a foundation, policy enforcement can also be deployed and applied in edge nodes for improving boundary controls and preventing mistakes or malicious actions within the inspection zone. Leveraging monitoring capabilities, event processing can detect and take action in real time for a variety of scenarios that would otherwise not be possible. A developer accidentally runs a test against a production database, an employee tries to send a file link but sends access to the folder (containing competitor information) — since all business traffic traverses the edge nodes, distributed control points operate at every intersection point.



## Constraints

1. The ability to establish policies is mostly unlimited within any organization, yet most organizations do not have the ability to enforce policies.
2. In order to enforce policies, you need to implement in a way that cannot be circumvented. Doing so is generally difficult to achieve.
3. Many of the activities to which firms need to apply policies are outside their boundaries (perimeter) and not visible. It may be known that it is occurring, but there is no broad enforcement capability (other than manual processes).
4. Without basic event processing and monitoring, determining what policies are needed is difficult.
5. You cannot manage an automated environment without automated controls. As a result, governance and risk management are severely limited.



## Steps

1. Establish which flows require what kinds of policies. In doing so, determine what is available in your security ecosystem that can be leveraged in your edge node.
2. Install the interception appliance and configure it to be part of the flow with a dedicated path to SaaS services.
3. Consider a SaaS service that maintains policies and registries of already prescribed and mature execution/remediation steps.
4. Monitor and log policy actions as another source of data for later analytics.
5. Tailor the policies over time for the most effective coverage.



## Forces

- The digital economy is driving exponential increases in types and sources of requests that require policy approval (e.g., APIs, mobile apps, partner and ecosystem connections).
- Policy enforcement decisions are real-time in nature, and as such, user experience and scale are driving enforcement decisions closer to the edge.
- Automated businesses need equally capable guardrails in place to mitigate risk and protect boundaries and employees from mistakes amid the automated chaos.
- Through software-defined infrastructure (technology APIs) and digital services (business APIs) come tremendous power and capability. You didn't hear about millions of people's private information being lost, or leaked, 10 years ago.

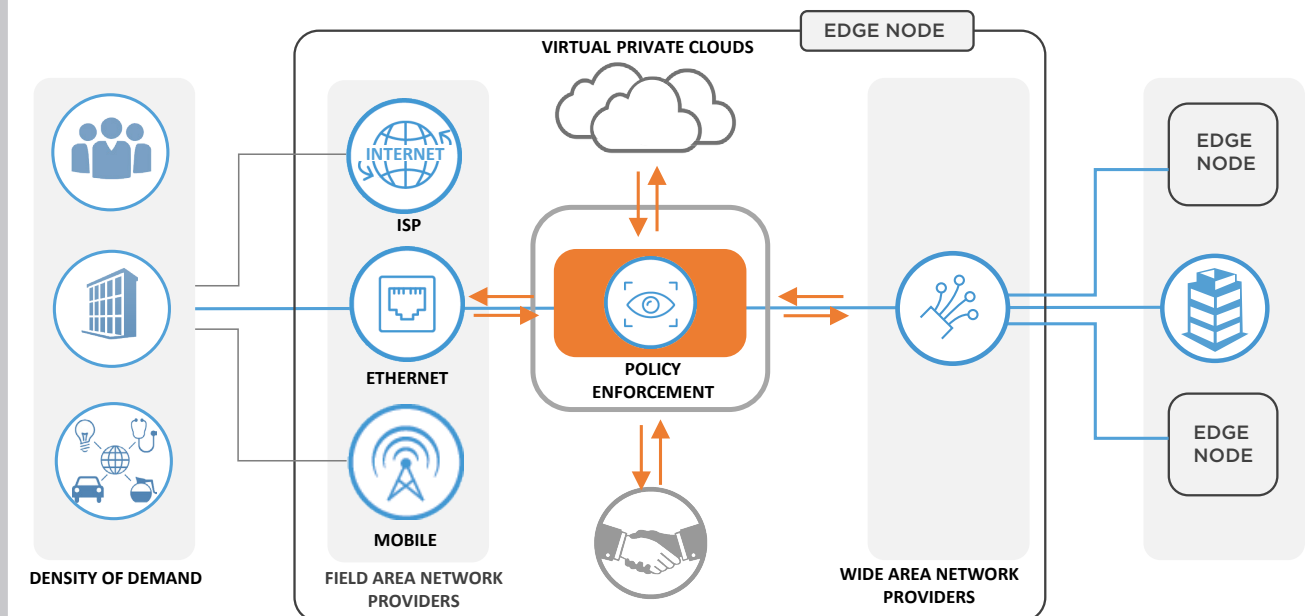


## Results

- Know that firm policies, like cloud usage, are being adhered to.
- Avoid the most common mistakes and an ecosystem full of lessons learned (the hard way) with subscription(s) to security services.
- Another hybrid design allows offloading into clouds to shifting to cloud-delivered, from cloud-assisted.
- Capitalize on the latency advantages and implement more security, governance and controls, which would have otherwise negatively impacted user experience or scale.



## Reference View



\* Network Blueprint — IOAKB.com



## Problem

Tracking the bidirectional flow of users and services and requiring those services to constantly fetch credentials and decryption keys causes latency delays if those services are not colocated. However, in a multicloud environment, that can cause a proliferation of copies, which increases complexity and may be compromised.



## Solution

Place critical infrastructure services in the edge nodes. These services should be both latency sensitive and risk sensitive (like security services such as identity and key management). They typically have high traffic volumes – and can be placed in proximity to clouds, digital ecosystems and user population centers in the edge nodes. This provides a federated service within the trusted security infrastructure. This way your company retains full control over the services, and if any of the clouds and/or partners become compromised, it is not a "shared fate" scenario (they don't even have the data). Likewise, even within your firm, access to these systems must traverse the inspection zone, and policy enforcement points ensure attempts to steal or leak security data are detected and prevented. Not only does this simplify management and improve security, the results are far more efficient and beneficial.



## Constraints

1. Having the security information stores like key management and identity services centrally located (HQ data center) forces all edge requests to backhaul and longhaul over the WAN. Whenever traffic does that, user experience and application performance suffer.
2. Likewise, security information has traditionally been centralized due to a natural resistance to proliferate sensitive data that, if compromised, could cripple the firm.
3. Cloud providers offer these services to alleviate the need for backhaul, and they get used because there are no viable alternatives.
4. If a multicloud environment is compromised or caught up in a government action (does cloud have a nationality?), as a shared infrastructure tenant your company's data could be involved.



## Steps

1. Deploy security appliances (usually dedicated hardware appliances) and apply proxy/load balancing as needed.
2. Configure boundary roles and inspection zone policies to further protect access.
3. Leverage network segmentation to provide an isolated service replication/synchronization channel (closed circuit) across the edge node fabric.
4. Encrypt security service data with a separate mechanism and break-glass procedures.

Note: Public internet apps can also use the services over the ISP link. In addition, for services that are already established in a cloud, you can extend hosted service(s) to other clouds with a path through the edge node rather than duplicate them.



## Forces

- The balance between "trust-no one" security and reasonable performance is very hard to achieve with remote critical infrastructure services—but the risks need to be mitigated.
- Business is becoming heavily dependent on IT services and the impact of outages—especially for what is sometimes termed critical infrastructure (DNS, Directory, Identity, Key Management or even Network) equates to \$/second in downtime and reputational damage.
- When private information is compromised, data is leaked, and/or worst case, slowly corrupted over time, the impact can take months to be fully understood and typically costs the firm hundreds of millions in remediation.

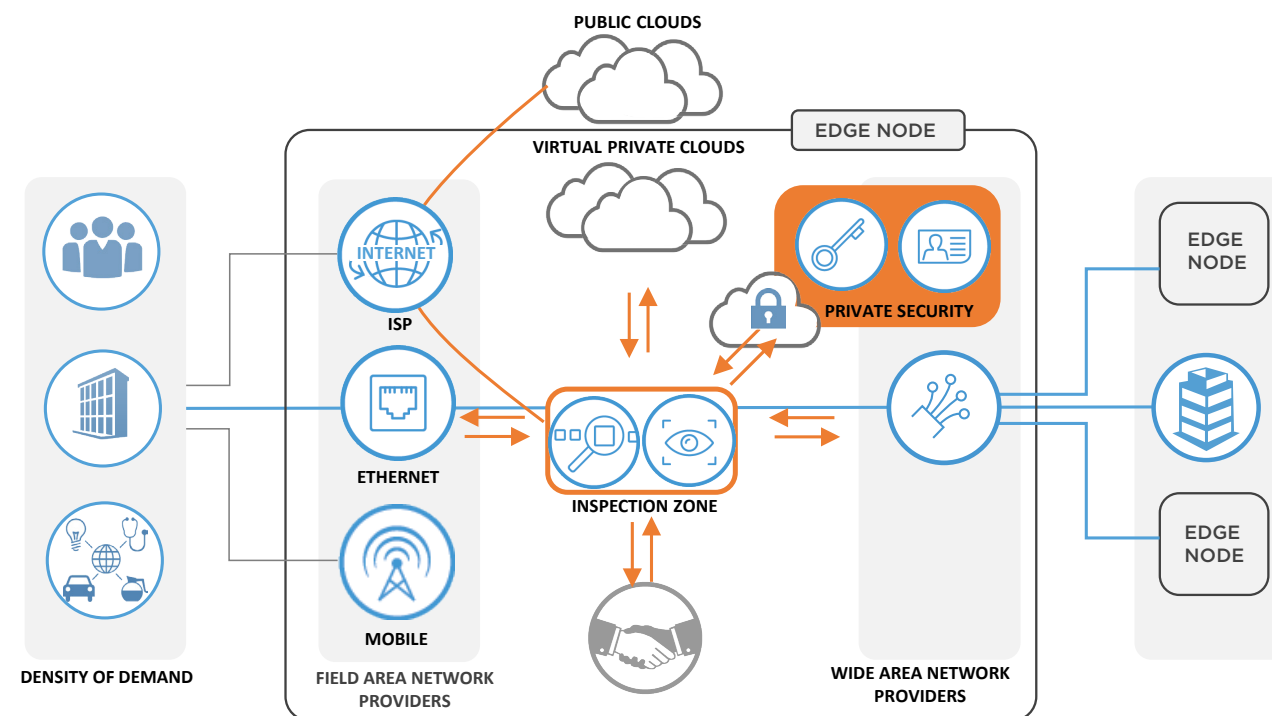


## Results

- Security services remain in control of the firm at all times regardless of changes to cloud services' use.
- Multitenant service attacks (hypervisor core dumps) will not yield services or security data, as the information doesn't exist there.
- Capitalize on the latency advantages and implement more security, governance and controls, which would have otherwise negatively impacted user experience or scale.
- Overall performance and resiliency is improved with services federated across edge nodes and intersection points.
- Any disruptive event in a cloud or partner environments will not be a "shared fate" scenario.



## Reference View





## Problem

The need to handle an increasing volume and variety of millions of security information points (assuming you have the ability to capture those). The overall level of security intelligence required today goes well beyond the capabilities of yesterday's infrastructure.



## Solution

By implementing the preceding steps in this blueprint and the foundational Network Blueprint\* layer, you are able to scale analytical capabilities with the help of the security ecosystem (and SaaS), control and move large volumes of data across low-latency direct connections, and observe all localized interactions between all parties in a distributed and scalable manner. You can incrementally improve your inspection capabilities through all levels of the OSI stack while applying evolving models and analytical intelligence. More importantly, you have the control to act on, or respond to, the delivered insights. Improve your policies (enforced globally at all intersection points – therefore, across all clouds and partners) and further compartmentalize risk over time. Adapt to changes in business processes and technology from a position of governance. Provide real-time risk positions and trend analysis as decision support for the security roadmap, backed by data to prove the return on security posture. Likewise, stop investing in ineffective practices.



## Constraints

1. Low visibility into activity at the edge limits the security data collected.
2. Building infrastructure required to conduct large scale and deep analytics on the data can surpass skillsets.
3. Building out analytics inside a single cloud is like locking a single room in the house. The larger picture across mobile and business ecosystems is not being accounted for.
4. Centralizing analytics means reduced reaction times to geographically dispersed threats.
5. Each region has different threat vectors, regulations and profiles that can require different analysis and response. It's not one size fits all.
6. Defense in depth requires analytics at all levels of the environment, which can be siloed and therefore ineffective.



## Steps

1. Plan where data will be aggregated and how it will be accessed (Data Blueprint\*).
2. Inventory real-time event processing and data sources/logs that are planned or currently available (e.g., boundary, inspection, end-point).
3. For each of the network segmentation classes of traffic, plan the initial behavioral analytics models and process for tuning them.
4. Apply hybrid infrastructure services in the isolated, closed-circuit environment. Logging repositories should be immutable, but false logs should not be possible either.
5. Observe the known good state to learn normal behavior for anomaly detection.
6. Run your own penetration, vulnerability and behavioral tests to tune the models.
7. Integrate policy enforcement for real-time response to attacks.



## Forces

- Cybercrime is growing at the same pace and sophistication as digital business.
- Zero-day vulnerabilities are increasing as the pace of technology change increases and maturity and understanding decrease.
- Recent advice from authorities and industry experts is to assume your environment is already compromised and has been for quite some time. You just don't know it yet.
- Infiltration is driving the need to observe all kinds of behavior in order to detect subtle patterns, not just the obvious threats.
- In the rapidly changing world of digital business, it will become increasingly difficult to understand risk profiles without established analytical models.

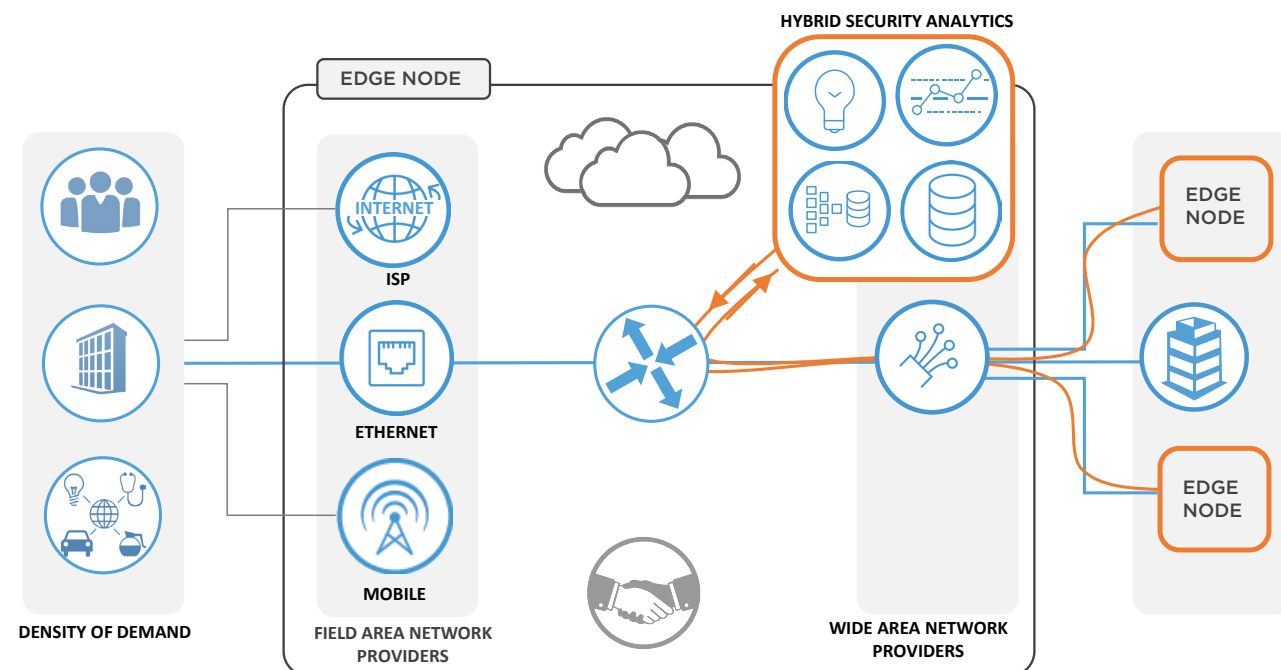


## Results

- The security position for the firm is not only well understood, but is observable and policy controlled—with machine learning.
- Capacity issues are buffered by expansion into cloud services, and can in the future can be mitigated in real time as models and policies learn that behavior.
- Achieve an optimal mix of real-time event processing and situational analysis.
- Skillsets and innovation can be easily sourced from an ecosystem of security services.
- New business models and cloud services can be activated seamlessly with full protection.
- Security and risk management are now enablers of digital business, not barriers or detractors.



## Reference View



\* Network and Data Blueprints — IOAKB.com