



Design Principles

- Business acceleration over obstruction.
- Strategic, physically secure locations.
- Dynamic network connections.
- Zero trust environment (all ingress/egress).
- Continuous rapid change requires discovery.
- Increasing "outside" risk and shared fate.
- Control must remain cloud- and third-party-neutral.
- Automated scale — volume, velocity and variety.
- Endpoints are not secure and cannot be trusted.
- Resiliency over recovery.
- Take the shadow out of shadow IT.

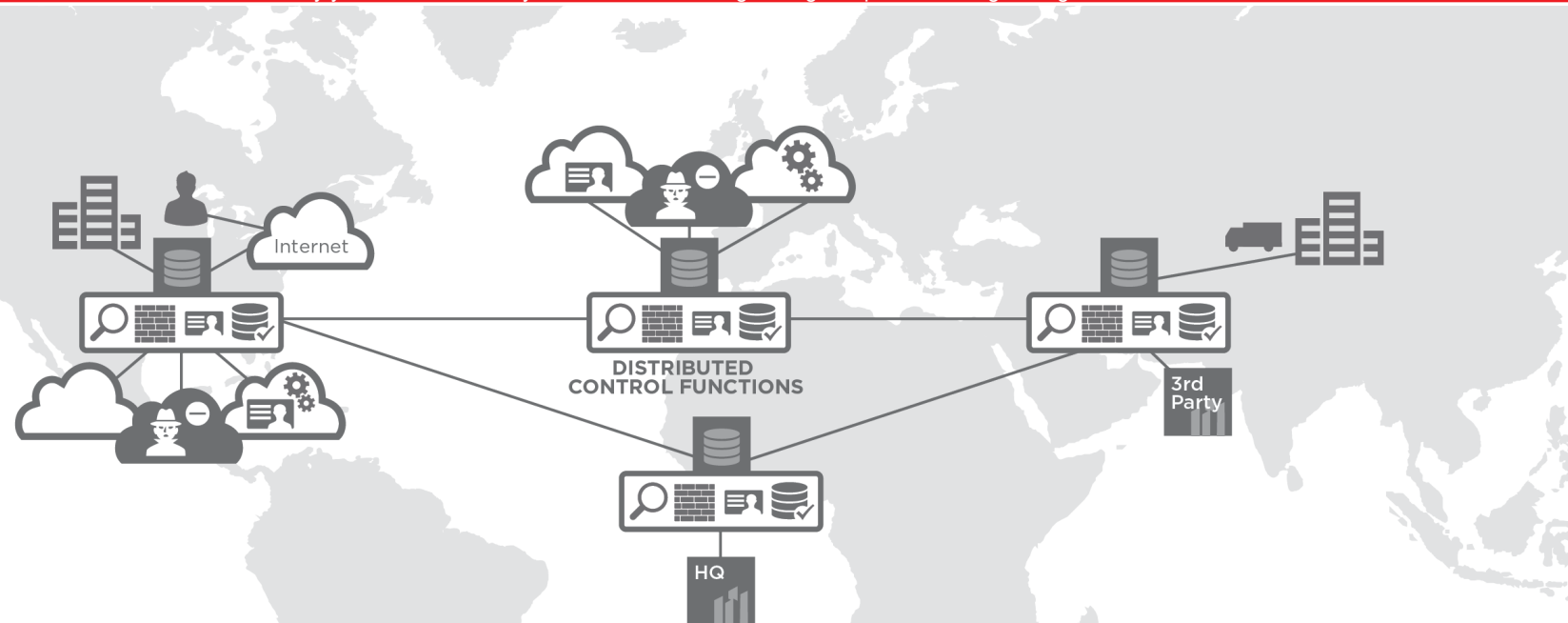
Critical Platform Elements

Global location coverage — Ability to place secure control points near customers, employees and partners for responsiveness and compliance.

Interconnection and ecosystems — Greatest choice in networks, clouds, partners and ecosystems with dynamic exchange options.

Integration and control — Leverage proximity and low latency to privately integrate physical and virtual services from a marketplace of leading options.

Digital is reshaping growth, driving revenue and investment out to the edge. This shift requires dynamic multicloud, multiparty integration and infrastructure change. This increases security exposure and the potential for devastating impact and reputational risk (loss of trust). Interconnection is the preferred approach to scale for digital business, and following the best practices of an Interconnection Oriented Architecture® (IOA) firms are distributing strategic control points (near customers, employees and partners) and using them as forward operating bases (in military terms). This provides a unique vantage point to control the traffic across all networks, distribute control functions where needed for scale, strategically integrate cloud services and ecosystems, and enforce data compliance. Digital edge security is not another layer in your current control framework. It's rethinking the way you architect security and control for the digital edge as part a new digital edge control framework.

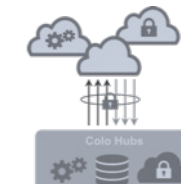


Advantages of a Digital-Ready Platform

Capabilities

- Global awareness at scale with distributed, localized and tailored fine grained control points.
- Ability to add and move capacity where needed as traffic patterns shift/change.
- Standardized way (and places) to integrate multiple cloud and partner security tools and requirements.
- Auto discover new services and business activities when they traverse a control point (and apply guardrails).
- Place sensitive data inside the control point, with multi-network/cloud access, for compliance.
- Easily incorporate new ecosystem innovation.
- Dramatically increase customer and partner interaction while significantly reducing attack surface and risk.

Virtual and Physical Stack



Leverage colocation hubs for hybrid deployment models that are fit for purpose between appliances and cloud-delivered services.

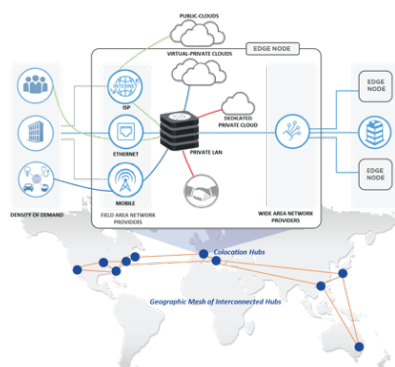
DESIGN PATTERNS

1ST Control Digital Communications

Take control of all digital communications by deploying network ingress and egress security functions in strategic interconnection control points, which act as forward operating bases, and form the foundation of a digital edge control framework.

Types of control functions involved:

- Access control and segmentation.
- Secure global DNS load balancing.
- Distributed Denial of Service.
- Transport encryption and secure access.
- Key management and tokenization.
- Global secure time.
- Security proxy.
- Advanced threat detection.
- Secure messaging and exchange.

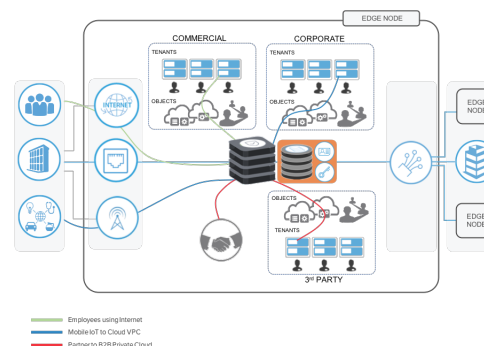


2ND Integrate Multicloud and Data Controls

Integrate multicloud control functions and data strategy. Avoid duplication and fragmentation with an end-to-end strategy that incorporates the disparate cloud environment tools and addresses associated data implications — ahead of a disaster.

Types of control functions involved:

- IAM and identity attestation.
- End point security.
- SIEM 2.0.
- Digital rights management.
- Data loss prevention.
- Data encryption across data pipeline.
- Application delivery and load balancing (API).

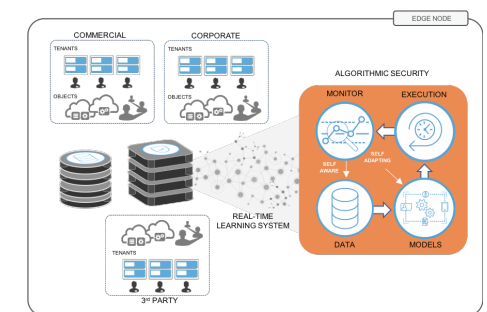


3RD Security as a Digital Business Enabler

Enable digital business by operating like a digital business. Spend less time focusing on the transitive/microthings (trending to millions) and focus on the macro relationships and how they interconnect to achieve algorithmic scale.

Types of elevated capabilities involved:

- Unify security and risk metrics across ecosystem.
- Develop user and entity behavior analytics.
- Complex event processing.
- Predictive analytics and automated response.
- Service chaining and workflow optimization.
- Leverage algorithmic modeling.
- Autonomous security bots (SecBots).





Control Digital Communications



Problem

Dispersion of processing and data, combined with increasing ingress/egress points (to internet, clouds and partners), in more locations globally, with changing regulations, and increasing attack surface and sophistication – begs the question, how do you retain control? Especially at an increasing rate of change?



Solution

What is needed is not a "perimeter", but a series of security checkpoints (a.k.a. control points). In an IOA these checkpoints are like airports, and like airport security, you challenge and inspect all traffic from multiple source and destination locations. In a zero-trust environment you are checking both inbound and outbound traffic equally. These checkpoints are geographically located where you need them, near clouds, customers, employees, etc. Together they form a distributed security mesh. By placing a control stack (or physical and virtual/SaaS functions) in each control point and routing all (important) traffic through it, you not only can control isolation, segmentation and inspection; but verify identity and enforce policy as well (who are you? where are you going? which airline or flow? what are you bringing with you? are there any red flags?). All of this happens locally and overall acts like a spider's web. As a result, when new cloud environments or partner connections are created, the new endpoints and traffic are discovered (auto update and verify), and base controls/policies are automatically applied. These permissions can be elevated or the traffic is quarantined. With this approach you can effectively track and govern all digital communications.



Constraints

1. It's difficult to establish, let alone enforce, a global standard set of controls across disparate networks, clouds, partners and endpoints — especially in a way that cannot be circumvented and is able to keep up with dynamic change.
2. Backhauling all digital communication traffic to a traditional centralized security stack is impractical with the exponential growth of traffic, and data and response time and performance impacts are too high. Bypassing the security stack would be the preferred choice.
3. Storing security information like identity and key management in multiple cloud locations alleviates the backhaul problems but creates new kinds of risk. If one is compromised, they could all be compromised, and any keys or data that get caught up in a government action may expose your data as well (and you wouldn't be notified).



Steps

1. Deploy strategic fortified control points: Select colocation hubs that meet security, availability and regulatory compliance requirements. Ensure that the networks, clouds and partners that you need to interconnect with are available.
2. Apply zero-trust boundary with dynamic interconnection: Isolate networks (e.g., corporate, commercial and third party), define primary traffic flows and interconnect the counterparties, internet circuits and SD-WAN to each.
3. Localize traffic management and transport security: Deploy global secure dynamic DNS with load balancing for planned use with multiple public/private network address spaces, including clouds. Deploy key management for encryption/certificates and global secure uptime.
4. Segment network access with inspection zones: Segment traffic flows into security zones and rules. Place device, actor, role, location — access controls and DDoS.
5. Position threat detection and policy enforcement: With guardrails that correct for insecure services (e.g., instead of blocking insecure actions, contact their APIs and secure 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.
- As companies adopt dozens of cloud services, users are being confronted with new apps. SSO integrates that, but it's both a blessing and a curse. It only takes one fake SaaS site to capture an employee's SSO credentials, and they would have access to all that employee's SSO-based SaaS apps. That entire scenario is out of your control.

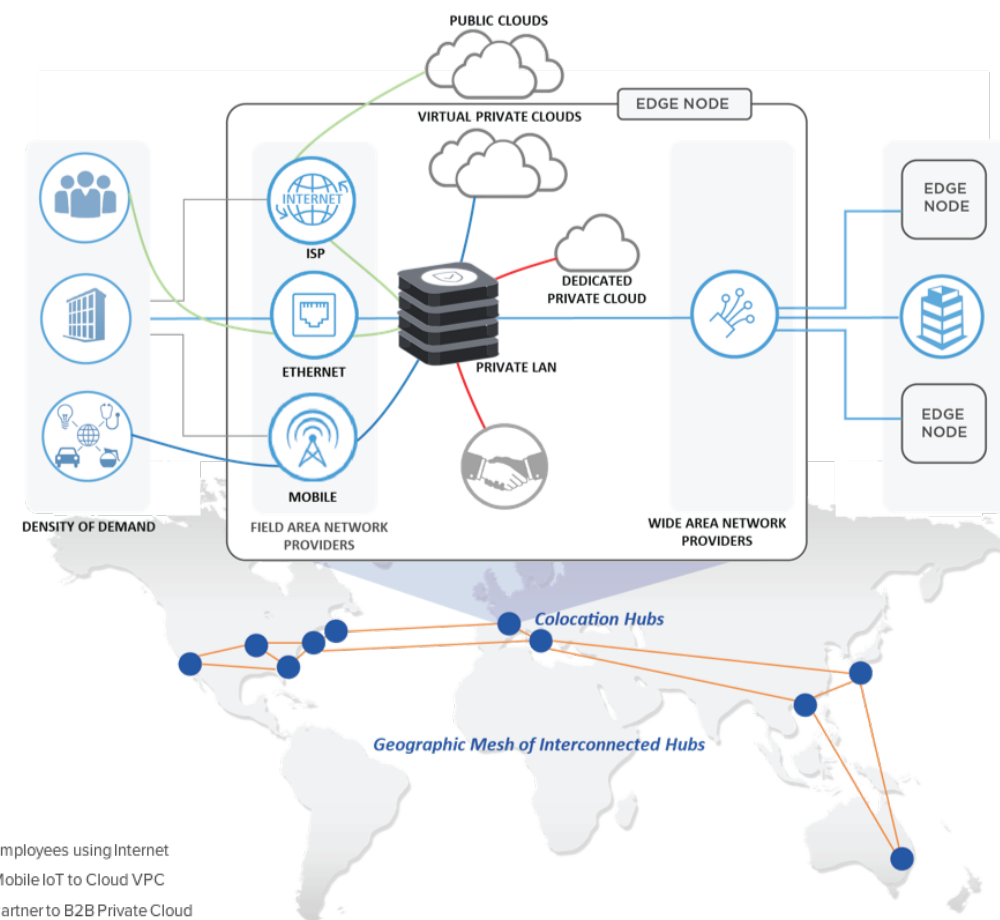


Results

- You now have distributed critical infrastructure services near customers, clouds and ecosystems — in some of the most secure, resilient and compliant facilities in the world.
- Your security stack is now colocated in ideal locations—the intersection points of networks, clouds, partners and ecosystems with the highest security and bandwidth and lowest latency.
- The majority of business traffic crosses private dedicated links and typically stays within the colocation facility and metro area.
- Because of the huge performance gains and low latency, a much greater level of security can be applied and all traffic can be routed through the stack with minimal penalty (limiting lateral attacks). Your security stack will actually be the preferred route to alternatives.
- Gain bidirectional visibility and control over all mobile, IoT, cloud, partner and data center communications — including shadow IT.

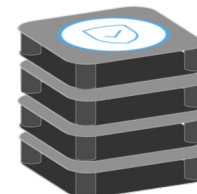


Reference View



Controls

- Access control and segmentation.
- Secure global DNS load balancing.
- Distributed Denial of Service.
- Transport encryption and secure access.
- Key management and tokenization.
- Security proxy.
- Advanced threat detection.
- Secure messaging and exchange.
- Global secure time.





Integrate Multicloud and Data Controls



Problem

Distributing services to clouds creates new operational silos, fragmenting IT's view of their infrastructure. It's easy to adopt these decoupled systems without realizing that you're losing sight of that larger-scale flow integration (e.g., services integration, network implications, requirements on placement, encryption and access of data).



Solution

Place cloud-neutral control functions in the distributed control points and develop the end-to-end security, encryption and data strategy. Leverage connectors and API gateways to plug-in cloud and SaaS infrastructure, configure IaaS, PaaS and SaaS to route all traffic through the security fabric (where necessary, place slave instances inside clouds) and retain federated control over all objects, identities, keys and data access. First establish identity groups to match the network isolation groups (in previous pattern – Control Digital Communications) e.g., at corporate, commercial and third-party level. Create top-level controls that apply to all networks (the tide that raises all ships). Then for each isolation group (which inherits location, device, role and actor segmentation from boundary), create a federated object repository that supports numerous tenants (or identity groups) to segment business groups, application families and provider type (legacy, private, public — cloud/SaaS providers). Establishing a zero-trust multinet, multicloud, multitenant identity space. Since the components that make up this strategy can be sourced and service chained locally over private, low-latency interconnection, the problems that would otherwise make this counter intuitive no longer apply. Further, malicious software or users cannot laterally move through your environment or cross zones. Likewise, sensitive data in this architecture is not stored in the cloud or with third parties at all, but within the control point on private storage (especially useful in cases relating to data sovereignty). Where sensitive data is required to reside in one or more clouds, they use your cloud-neutral key management controls. In all cases you still govern how those clouds encrypt the data and who can access the data.



Constraints

1. To successfully address real-time attacks, the time difference between detection and response needs to be near zero. However, as the environment becomes more distributed and diverse, across multiple services, response time is increasing—and was already too high. Tighter integration with clouds and business partners can fragment controls, increasing or transferring risk (their risk is now yours), which is a primary barrier to cloud adoption.
2. While many services come with connectors to help re-integrate flows, if the latency between these components in the service chain is not low, the workflow will not be able to scale with automation and volumes of alerts/events.
3. Keeping the data in the centralized data center can impact performance (and business), driving risk waivers for distributed copies of data out to the edge. If you don't control that data or access to it, your firm is at extreme risk.



Steps

1. Multicloud identity management: Natively integrate cloud/SaaS identity and access controls with your federated critical infrastructure (or synchronize push updates). Avoid users directly accessing cloud accounts and other configurations that prevent moving apps/data between clouds. Leverage additional data points to detect stolen SSO credentials (wrong device, wrong location, outside normal behavior).
2. Cloud-neutral encryption and key management: Leverage your cloud-neutral key management through your distributed control points to natively integrate cloud connectors and APIs. Prevent clouds or third parties from having access to your data and keys.
3. Private data repositories and compliance: Data that determines compliance, security, audit and reputational risk should not be distributed outside your private control. Place in off-premise, physically secure and compliant facilities. Establish data services interfaces to all data for both internal and third-party access controls (with immutability as needed).
4. Application infrastructure(s): Integrate security with application and PaaS infrastructures. Provisioned and configured services use the control points natively.
5. Development and API services: Integrate source libraries, application services and gateways.



Forces

- Digital is driving an increasing rate of change with diminishing time to fully understand change implications.
- Breaches are driving regulation changes, like GDPR, which have some firms re-thinking where they put data, and re-thinking their existing cloud architectures entirely.
- There is an increasing need for trust between customer and partner/providers. Both need to be convinced that you are not the weakest link in the ecosystem.

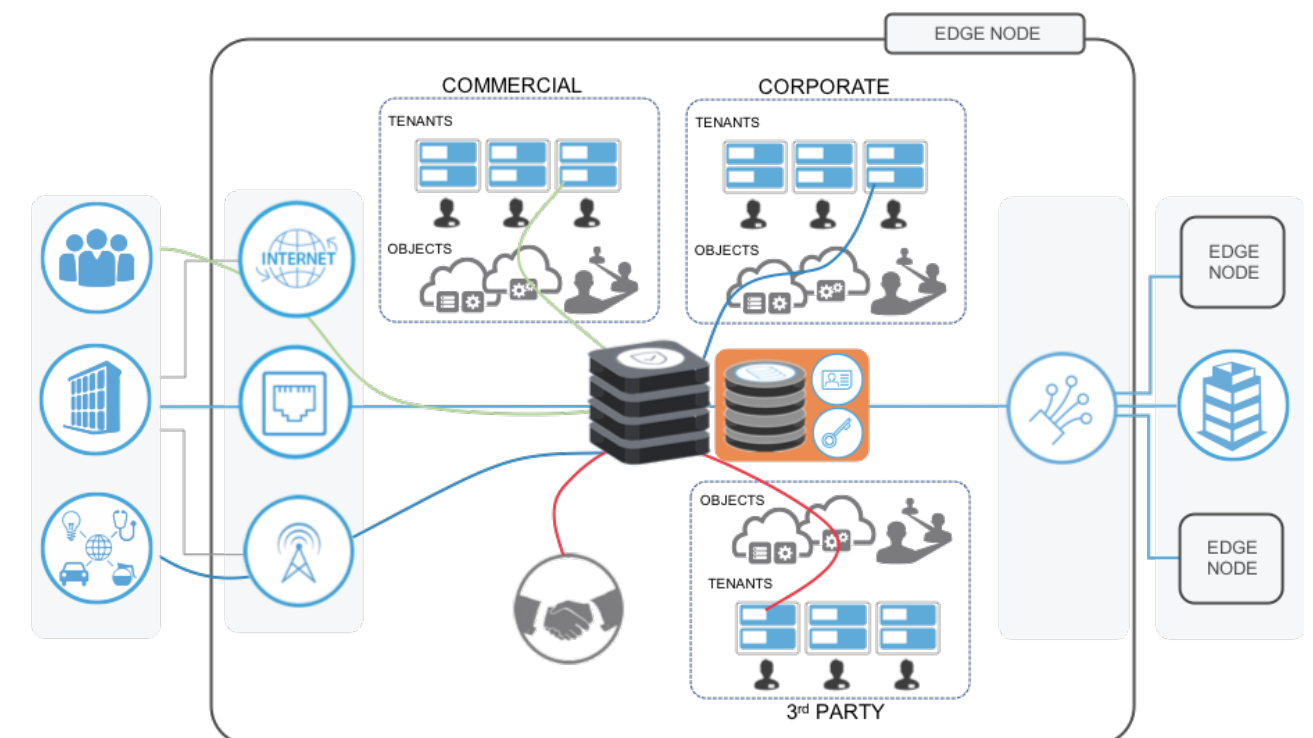


Results

- Capitalize on the latency advantages by implementing more security, governance and controls that would have otherwise negatively impacted user experience or processing scale.
- Security services remain in control of the firm at all times regardless of changes to cloud services' use, and security traffic is private.
- Multitenant service attacks (e.g., hypervisor core dumps) will not yield services or security data as the information doesn't exist there.
- Any exploit, or government action, in a cloud or partner environment will not be a "shared fate" scenario. You are protected, as only you have the keys.
- Natively integrating security with cloud, PaaS and development means doing the right thing is actually preferred by everyone. Dynamically enable new services with proactive entitlement.



Reference View



Controls

- IAM and identity attestation.
- Cloud Access Security Brokers.
- End point security.
- SIEM 2.0.
- Data loss prevention.
- Data encryption across data pipeline.
- Digital rights management.
- Application delivery & load balancing (API).





Security as a Digital Business Enabler



Problem

Security teams are seeing exponential change and increasing complexity, and have less time to balance the risk. Attacks, across more technologies, are getting more sophisticated, and the impact is now significantly higher (loss of trust can put you out of business). Security has to slow things down to protect the firm, but the business needs growth at speed to survive.



Solution

For many industries, the shift to digital business already happened. IOA has been developed (over years) from studying that shift and capturing architecturally what others did and are doing. Innovation is not invention, but more the application of an existing solution in a new context. With that in mind, take algorithmic (algo) trading as a precedent. It exhibits many of the same challenges as those facing IT security. There are very large volumes of data that must be captured, analyzed and then acted upon in real time. The market shifts continuously, and machines are programmed to act autonomously based on that change. The impact of failure is business threatening, and the compliance and legislative requirements are extremely fine-grained, strict and uncompromising. To solve, many companies needed to re-architect, starting with IOA and controlling all digital communications (pattern 1). Instead of clouds, in this case, they integrated with market exchanges and counterparties (pattern 2), and to scale they applied autonomous machines and artificial intelligence. AI is not that new in the security space; however, there is a difference. They didn't apply AI to their existing architecture to help them manage the "things" which leads to having too much data and unhelpful 'business intelligence'. AI was incorporated into the new architecture to deeply analyze the "communication between the things" and understand and control what was happening in real time. To expand on that analogy, it's the use of CEP that presents real-time data (state) to a series of models (AI), which triggers bots (autonomous engines) to go take action. This informs a master monitor that updates, adapts and improves the system. Self-aware means self documenting. Self-adapting means at the speed of the attack. Security is a digital business enabler, with guardrails.



Constraints

1. IT security teams are unable to effectively transform at the same pace at which the threat they face is evolving. This leaves them trying to deal with the threat using the technology that they already know and have installed — which was not designed for the challenges of digital.
2. Segmentation has not necessarily been used as a corporate means to compartmentalize problems, and as such, all activities feel like boiling the ocean.
3. If a human is involved, the time to respond goes up by at least an hour. An automated autonomous attack can laterally compromise more than a thousand machines in a fraction of that time (in a large-scale flat network).
4. Teams are overwhelmed by multiple data sources that do not contain the relevant context and correlations to quickly detect, hunt and react to attack. This means data has to be constantly transformed, compared and verified.



Steps

1. Aggregate events with complex event processing: Analyze all cross-tenant communication to inform CEP models for each isolated network. All other incidents and alerts should be handled at security zone/tenant level.
2. Share intelligence with partners and customers: The cornerstone of digital business is multiparty business engagement, so reach out socially to your counterparts and share your architecture. Exchange incident data directly with real-time feeds. Security data equates to experience; your models become exponentially smarter.
3. Apply end-to-end behavioral analytics: UEBA (user and entity behavioral analytics) can educate your models on what normal looks like (self-aware and self-updating). Use CEP (step 1) to simplify UEBA and avoid the multisystem mashup of disparate data. With CEP feeding UEBA, this can be automated.
4. Develop algorithmic models: Start simple, have the system record a month of activity, learn from that history and deploy models in shadow mode. Set to being live when false alarms, or necessary interventions, reach near zero.
5. Pre-emptively respond: Define independent automated workflows for each response type. Multiple workflows can be triggered to scale the real-time (parallel) response.



Forces

- Technology life cycles are shrinking, toward being throwaway. Managing the "things" is becoming pointless.
- The number of devices (IoT) and endpoints (with micro services) is headed toward millions.
- The average time for a breached company to perform a forensic assessment (on what happened) is six weeks and getting longer.
- The need to understand critical relationships (on the network) is becoming paramount.

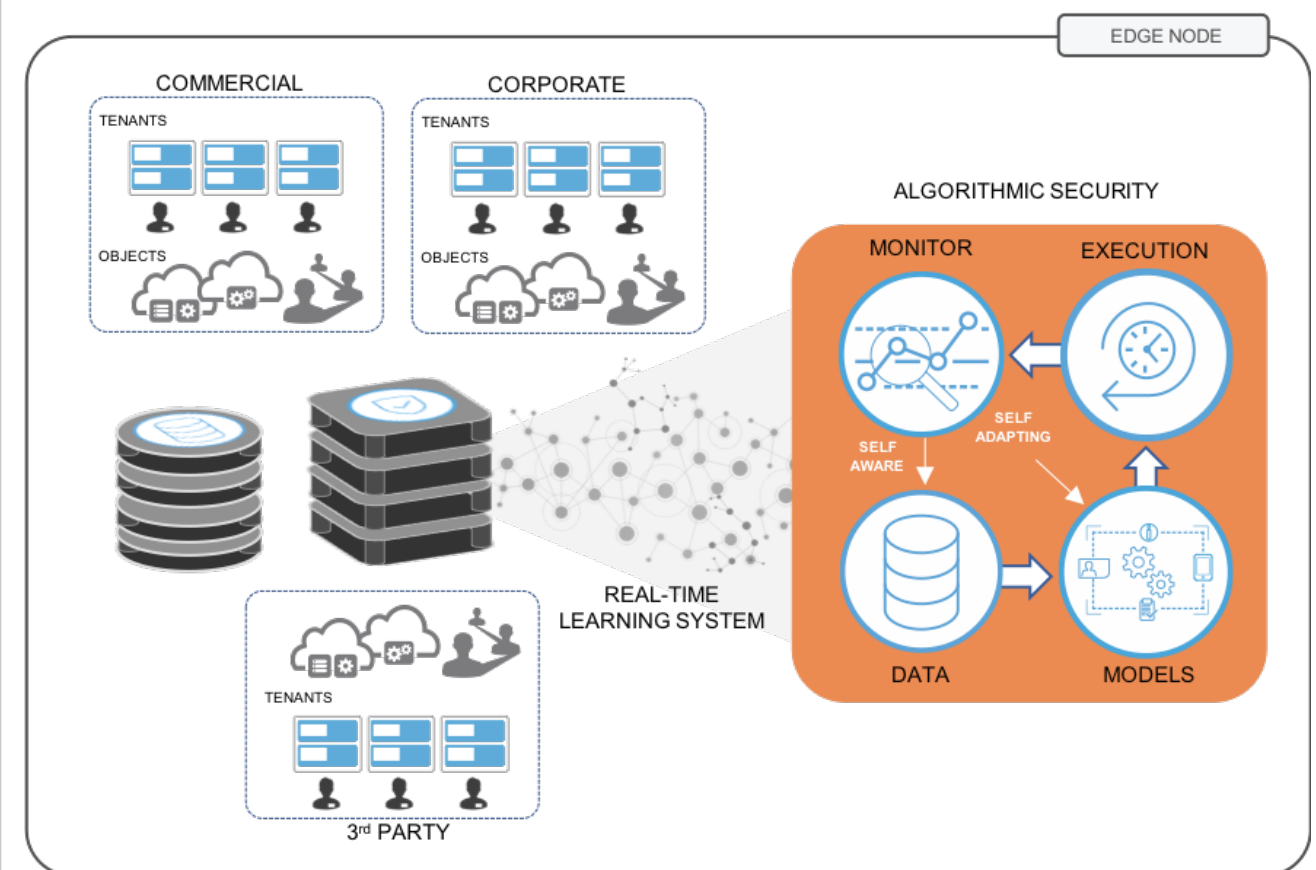


Results

- Complexity is reduced (abstracted). Security is not about chasing patches on endpoints, but rather securing tenants (zones). Thus tenants can be on different clouds and handle changes locally. Security can focus on CEP.
- Attacks or incidents can be isolated and targeted at scale.
- Security is constantly learning, not just from direct experience, but from information shared with partners and customers.
- Sharing this architecture builds trust and can improve your counterparties' security – which further reduces your own risk as well.
- In this architecture you can approve non-sensitive and low-risk changes/activities automatically (get out of the way), with guardrails.
- IT security is no longer a detractor, but a strategic advantage.



Reference View



Controls

- Unify security and risk metrics across ecosystem.
- Develop user and entity behavior analytics.
- Complex event processing.
- Predictive analytics and automated response.
- Service chaining and workflow optimization.
- Leverage algorithmic modeling.
- Autonomous security bots (SecBots).

