Zero Trust Network Solution Architecture

Practitioner Framework

Common Security challenges that are forcing the adoption of Zero Trust

Overly Permissive Access

Overly permissive access to applications either because it is unclear what the correct policy should be or mistakes in network and policy configuration, allowing attackers to get a foothold

Large Blast Radius

Internal segmentation largely unrestricted, allowing malicious users and attackers to easily move laterally once they have a foothold

Stolen Credentials Reuse

Attackers accessing sensitive applications and data using stolen credentials

Inconsistent Security

Security scanning only applied to select traffic, creates a significant risk leading to credential theft, data loss, and attackers gaining an opportunity to move laterally

Bad User Experience

End users get a highly fragmented experience based on where they're working from, and operations are overly complex for admins

Unmanaged Devices

Employees accessing sensitive applications and data from unmanaged devices results in data leaving the enterprise's security perimeter

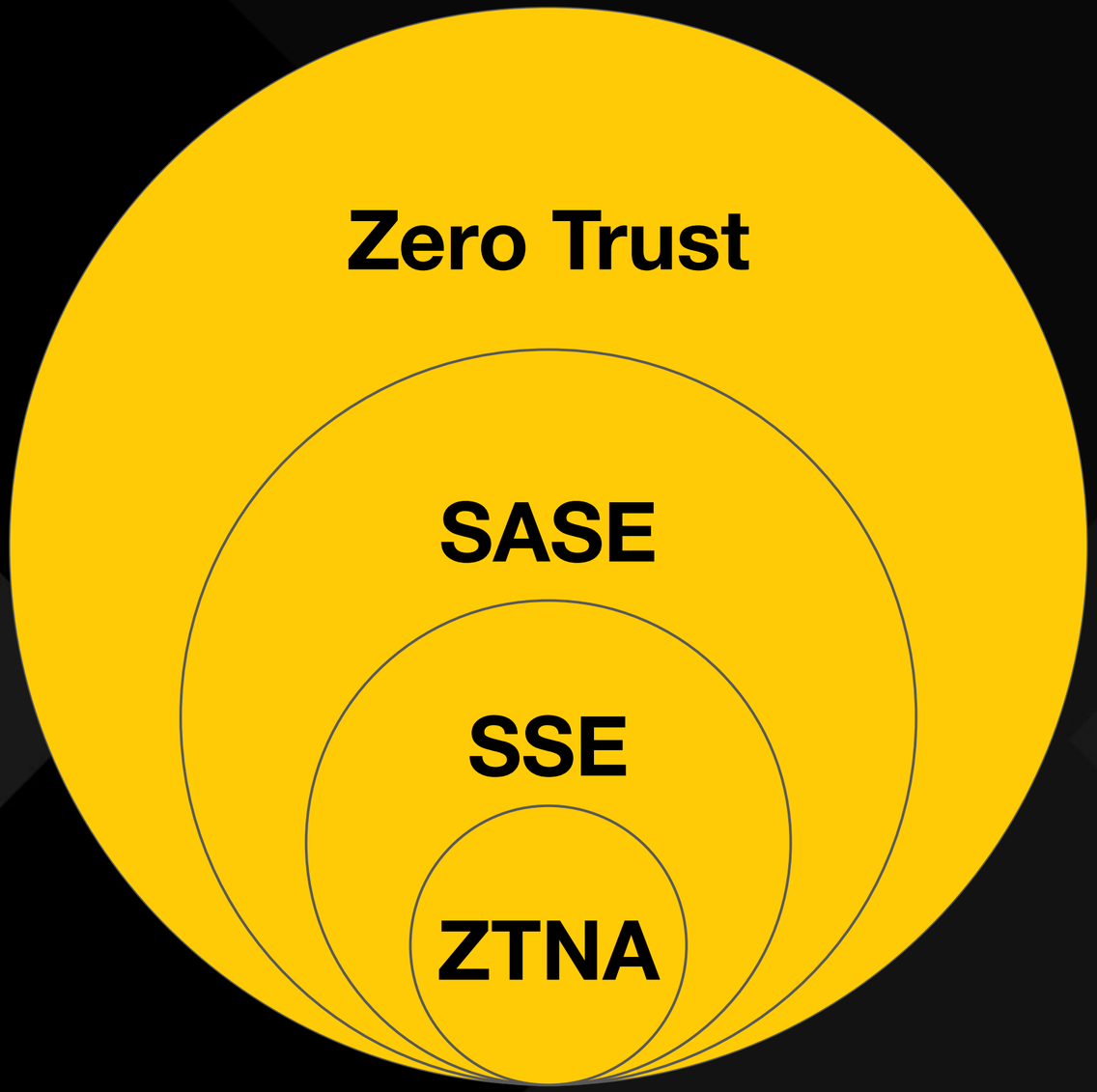
LETS GET CLEAR ON TERMINOLOGY

Zero Trust is a **strategic approach** to cybersecurity.

Goal: **Eliminate implicit trust** and **continuously validate** every stage of a digital interaction.

paloalto NETWORKS

LETS GET CLEAR ON TERMINOLOGY



Gartner *defined* technology market segments like **SASE, SSE, and ZTNA.**

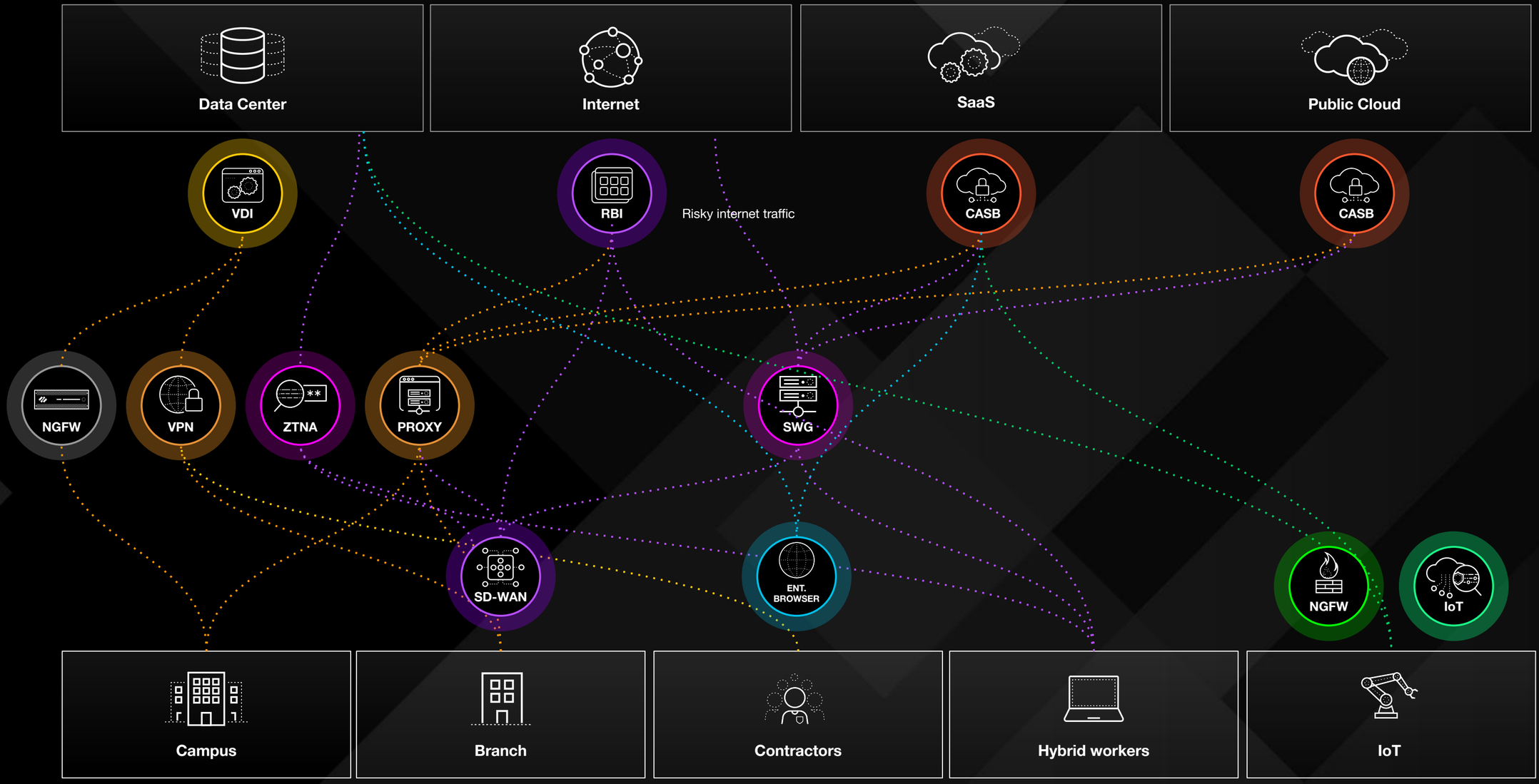
ZTNA implementations have largely been **defined** by the **vendor community.**

paloalto NETWORKS

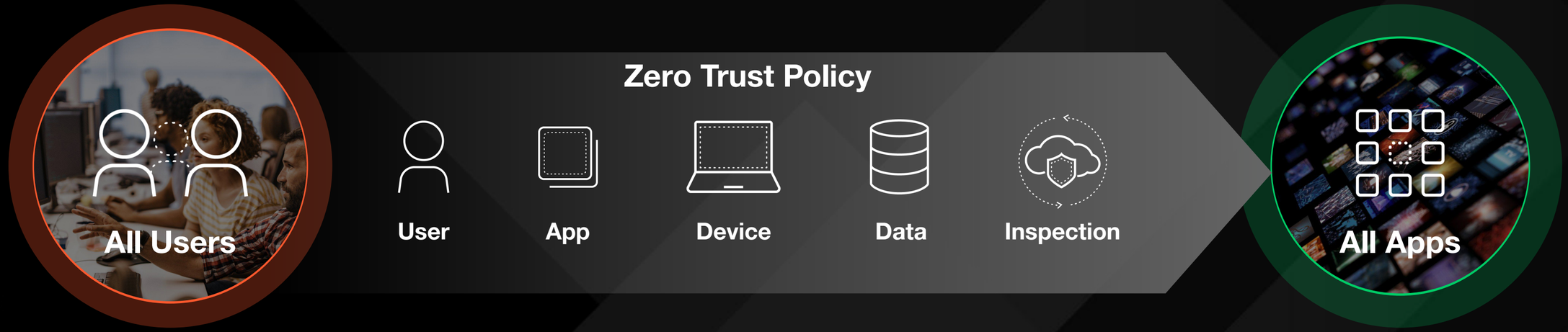
How a platform enables the journey to Zero Trust

paloalto NETWORKS

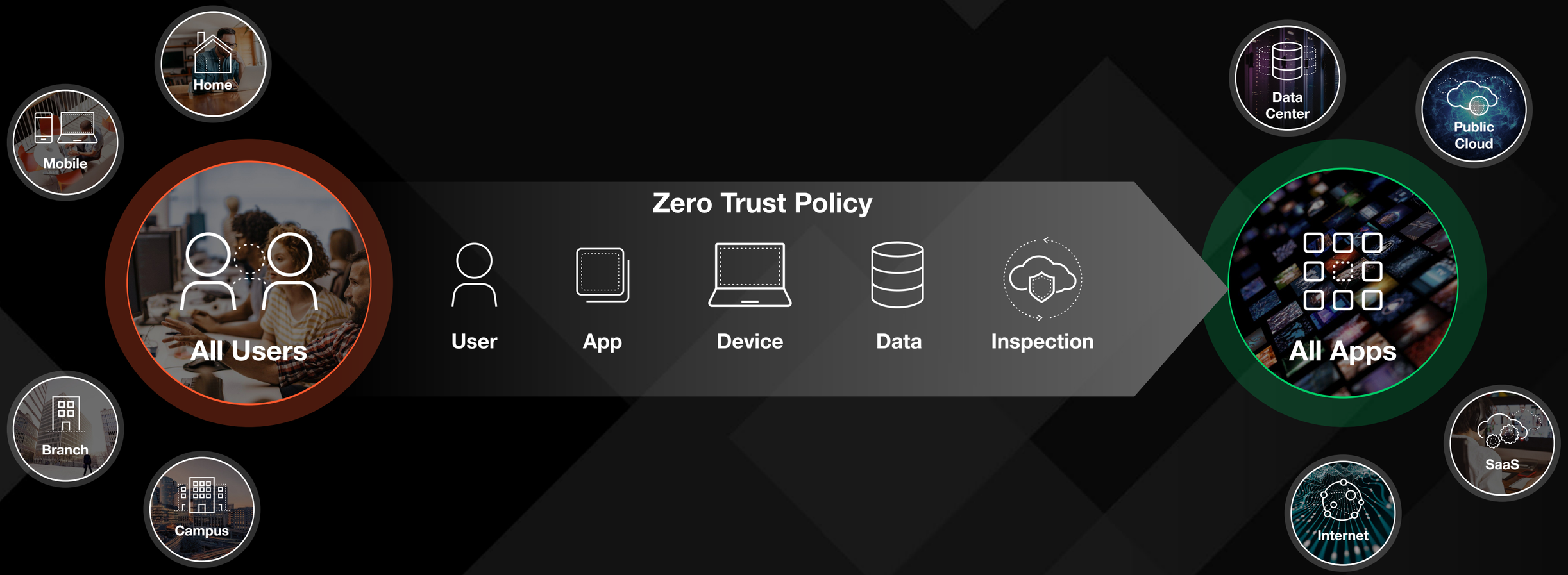
Zero Trust is hard with complex and fragmented network security stacks



Conceptually, Zero Trust is very simple



But the reality is that Zero Trust must apply to the entire enterprise



Palo Alto Networks: A platform approach to Zero Trust

Palo Alto Networks' Approach to Zero Trust

Identify and verify all Users, Devices, and Applications

Enforce least privilege policy

Apply holistic security inspection

Control data access and movement

Optimize user and operational experience

Palo Alto Networks' Approach to Zero Trust

Identify and verify all Users, Devices, and Applications

Enforce least privilege policy

Apply holistic security inspection

Control data access and movement

Optimize user and operational experience

Continuously Optimize with AI and Automation

Palo Alto Networks' approach to Zero Trust under the hood

Identify and verify all Users, Devices, and Applications

Identify **all users**.

Identify **all devices.** Verify **posture compliance**.

Identify **all applications**.

Continuously verify user, device, posture, and application.

Enforce least privilege policy

Contextual policies based on user, device, and apps

Connections allowed based on **business needs.**

Leverage **dynamic access policies** where possible.

Enable Decryption for complete user to application visibility.

Deny all other traffic by default.

Apply holistic security inspection

Prevent as many attacks as possible by **enabling all baseline security features.**

Apply **additional prevention** by use case (IoT, SaaS, RBI, EB, etc…)

Enable Decryption to increase attack prevention capabilities.

Improve **detection analytics** with centralized logging.

Control data access and movement

All data should be **identified, classified, and tagged.**

Use **data context** for access policies.

Optimize user and operational experience

Enhance experience with **user to application** visibility.

Enhance management, threat handling, and operations **with AI**

Use **AI to Predict** user experience issues.

Create consistent policies with **unified management**.

paloalto NETWORKS

Identify and verify user, device, and application – Key elements

All users

- Identify and verify **all users**
- Capture all necessary **user context**
  - Role
  - Location
  - Behavior

All devices

- Identify **all devices**
- Understand all necessary **device context**
  - Category
  - Type
  - Security posture
  - Behavior

All applications

- Fingerprint **all applications** based on network traffic
- Understand all necessary **application context**
- **Classify applications** based on business requirements **into sanctioned, unsanctioned, and tolerated**

Constantly Monitor for Changes

Identify and verify user, device, and application – Implementation

		Capabilities to enable	
	Key elements	**Core**	**Advanced**
All Users	Identify and verify all users	☐ Hardened IdP with MFA (e.g., Okta with hardened config) ☐ Right sized identity provider landscape to ensure user segmentation by classification or compliance rules	☐ Passwordless MFA as per FIDO2 ☐ Privileged account access controls (e.g., JIT) & management ☐ Automated provisioning & deprovisioning (e.g., IGE solution)
	Capture all necessary user context	☐ Each user context includes group, business units, and role ☐ Centralized user information repository within CIE	☐ Each user context includes other attributes such like region, language, etc., for more granular user/group policy decisions
All Devices	Identify and verify all devices	☐ Managed devices hardened with GlobalProtect ☐ Unmanaged devices identified via IdP vendor, internal and SaaS access only allowed using Prisma Access Browser or GlobalProtect. ☐ All IoT devices manually identified based on traffic logs	☐ Managed devices : Enforce GlobalProtect always-on and manage centrally (e.g., Jamf, Intune). ☐ Unmanaged devices: connections enforced via Enterprise Browser and managed via Mobile Device Management ☐ IoT devices fingerprinted with inline IoT Security
	Understand all necessary device context	☐ Host Information Profile (HIP) captured from GlobalProtect ☐ IoT device context such as vendor, model, and version captured	☐ HIP changes automatically change access policy in real time. ☐ XDR on endpoints for capturing expanded context ☐ Adtl. IoT device context such as OS version and CVEs captured
All Apps	Fingerprint all apps based on network traffic	☐ Repository of all identified applications with App-ID/SaaS Inline	
	Understand all necessary business apps	☐ Each application classified based on business use and access needs	☐ Each application classified additionally based on type and sensitivity of data
	Classify necessary apps based on business requirements	☐ Enforce compliance on device by tagging only required apps as sanctioned and partner apps as tolerated ☐ All other identified apps in the environment must be left untagged and therefore unsanctioned	☐ Sanctioned and tolerated business apps reviewed on a regular basis to remove the risky ones from policy

paloalto NETWORKS

Enforce Least Privilege Policy – Key Elements

Define policies based on context

- **All components of context** from users, devices, and applications are **leveraged to compose access policies.**
- Selectively enable **inspection of encrypted traffic** for complete visibility.

Apply policies based on business needs

- Regularly assess **which roles** need access to **which applications and data**. Leverage to create and monitor access policies.
- Leverage **automation** to **make user policies dynamic** based on user and device behavior.

Default-deny for everything else

- All connections are **denied** unless explicitly allowed

Enforce Least Privilege Policy – Implementation

		Capabilities to enable	
	Key Elements	**Core**	**Advanced**
Define policies based on context	All context about users, devices, and applications are leveraged to compose access policies	☐ Create new security policies based on apps observed in the logs while maintaining existing policies in place ☐ Use posture information in security policy ☐ 100% user, device, and app-aware (L7) policies.	☐ Endpoint enforcement to sanctioned app access (BYOD / Managed) ☐ Dynamic Access Policies: leverage automated workflows to change access based on behavior in real time.
	Selectively enable inspection of encrypted traffic for complete visibility	☐ Decryption enabled for unknown websites that are allowed ☐ Decryption enabled for malicious websites that are selectively allowed to certain admin groups such like SOC and IR	☐ Decrypt everything you can.
Define what access is needed based on job function	Establish a process to map roles to sanctioned/tolerated applications and resources. Update regularly	☐ Quarterly access review of policies with business leaders to validate business need vs risk. ☐ Quarterly business leadership meetings for upcoming product launches that will require new app-aware (L7) policies. ☐ Define sanctioned, tolerated, and unsanctioned apps and apply policy appropriately. ☐ Only corporate sanctioned and tolerated apps allowed by policy based on job function.	☐ Monthly access review of policies with business leaders to validate need vs risk. ☐ Corporate procedures to allow security evaluation of any new software or app usage.
	Translate into effective policies	☐ Unused policies that have not been used for over 90 days are retired. ☐ Cloned predefined default security profiles are placed on a security profile group name 'default' for consistency and automatic application to every new policy.	☐ Unused policies that have not been used for over 30 days are retired on a per business unit basis ☐ Cloned predefined strict security profiles are placed on a security profile group name 'default' for consistency ☐ Custom app signatures for private apps
Default-deny for everything else	All connections are natively denied unless explicitly allowed	☐ Existing default-deny policy leveraged ☐ Logging on default-deny policy must be enabled	

paloalto NETWORKS

Apply Holistic Security Inspection – Key elements

Apply core security everywhere

- **Enable Decryption** to increase attack visibility.
- Proactively **block vulnerabilities/exploits** in real-time
- Analyze risky files for **malware**
- Proactively block **malicious websites, phishing attempts** and **fileless attacks**
- Scan DNS traffic and **block DNS-related attacks** in real-time
- **Log everything** centrally.

Layer in additional security features

- Detect **anomalies and prevent threats to and from IoT** devices
- **Manage security posture** and **protect access to SaaS** applications in real-time
- Provide a **secure enterprise browser** for access to all web-applications.
- **Isolate users' web browsing** sessions for risky websites

Collect data for detection analytics

- Use all enforcement points to **collect all relevant data** needed for detection analytics. **Automate responses** where possible.
- **Centralized logging** allows for behavior analysis, enables dynamic policy changes, and event remediation.
- Regularly **update policies for improved detection accuracy** based on threat data.
- **Expose APIs** for real-time response

Apply Holistic Security Inspection – Implementation

		Capabilities to enable	
	Key Elements	**Core**	**Advanced**
Apply core security everywhere	Scan and block in real-time vulnerabilities/exploits	☐ Enable a default Vulnerability Protection and Anti Spyware profiles on all security policies.	☐ Customize the Vulnerability and Anti-Spyware profiles to your specific business needs and exceptions.
	Analyze risky files that could include malware	☐ Enable a default WildFire and File Blocking profiles for known high risk extensions.	☐ Customize the WildFire and File Blocking profile to your specific business needs and exceptions..
	Scan for malicious websites, phishing and other fileless attacks	☐ Enable URL Filtering profile on all outbound security policies.	☐ Customize the URL Filtering profiles to your specific business needs and exceptions..
	Scan DNS traffic and block in real-time DNS-related attack	☐ Enable a default Anti Spyware profile to prevent DNS-related attacks on all security policies	☐ Customize the Anti-Spyware profile to your specific business needs, prioritizing exceptions tuning.
Apply adtl. security per use case	Detect anomalies and prevent threats to and from IoT devices	☐ Create profiles based on device types you observe from the traffic forwarded by your enforcement points to IoT Security.	☐ Enable IoT Security to automatically push/suggest rule changes on your enforcement point to prevent threats.
	Manage security posture and protect access into SaaS apps in real-time	☐ Enable sanctioned apps with security controls, limit tolerated apps data types access, and block unsanctioned.	☐ Strictly control the sanctioned apps configurations to maintain security state and auto-correct config drifts.
	Isolate users' web browsing sessions for risky websites access	☐ Enable Remote Browser Isolation on Prisma Access ☐ Create or update a URL access management profile and attach the default isolation profile to it.	☐ Customize infrastructure settings for RBI global behavior. ☐ Customize an isolation profile to control what want to allow/deny during a RBI session (copy/paste/download).
Collect data for detection analytics	Use all enforcement points to collect all relevant data needed for detection analytics		☐ Enable Enhanced Application Logging on all firewalls. ☐ Add the predefined Log Forwarding profile to Security policy rules in bulk for security services like IoT Security.
	Regularly update policies to improve detection accuracy based on threat data from services		☐ Observe the logs for threats and create exceptions for false positive detected on your legitimate business traffic.
	Expose APIs for real-time response		☐ Specify the lifetime for which your API keys are valid.

paloalto NETWORKS

Control Data Access and Movement – Key elements

Use data context in access policies

- Define **data categories and sensitivity** based on business requirements.
- **Identify** where all sensitive data resides and **classify it by type** (e.g., source code, PII)
- Leverage **data context** to refine access policies

Control and monitor data movement

- **Log data movement** for all allowed connections based on sensitivity or tag
- **Prohibit sensitive data transfer** to undesired devices and/or applications
- Define **response workflows for allowed sensitive data transfers** to desired devices or applications (e.g., require approval, identify malpractice but allow)

Control Data Access and Movement – Implementation

	Key Elements	Capabilities to enable: Core	Capabilities to enable: Advanced
Use data context in access policies	Define data categories and sensitivity based on business requirements	☐ Regular process to manually list of all data used for standard, regulated, and proprietary types	☐ Automatic data categories definition based on identified data in scheduled scans across all data stores ☐ Custom data categories exist for proprietary data
	Identify where all sensitive data resides and classify it by type (e.g., source code, PII)	☐ Inventory of all data types used with their location and access rights/rules via manual processes (e.g., surveys) ☐ Classification of data within crown jewel applications	☐ Applications that perform data classification in within are configured for data visibility (e.g., Salesforce) ☐ Automatic scanning, discovery, classification and dynamic inventory of all data types in a unified view
	Leverage data context (from incl. non crown jewels) to refine exposure policies	☐ Predefined data classifiers within Enterprise DLP leveraged to define data profiles and access policies	☐ Customized data classifiers applied for standard, regulated, and IP data types with specific policies ☐ Over privileged access and overexposed data monitored and removed based on data exposure intelligence
Prevent data movement to undesired locations	Log data movement across all allowed connections based on its sensitivity	☐ Logging enabled for full SOC visibility into all crown jewel apps based on logs	☐ Train users with end-user notification and coaching for DLP policy violations
	Prohibit sensitive data transfer to undesired devices and/or applications	☐ Ingress / Egress policies in Crown Jewels apps to limit data transfer to only specific sanctioned apps ☐ Device control endpoint policy for removable media, printing, network shares ☐ Enforce sensitive data leak policies for corporate outbound email	☐ Visibility and control into sensitive data leak between non-corporate tenants and enterprise entities ☐ Targeted endpoint DLP policy for removable media, printing, network shares
	Define response workflows for allowed sensitive data transfers to desired devices or applications	☐ Single pane of glass to manage data remediation issues based on risk, context, and priority	☐ Automated and scheduled workflows to archive, delete, quarantine, mask, encrypt, and anonymize data ☐ Automated deletion of duplicate, redundant, and unnecessary data based on retention policies

paloalto NETWORKS

Optimize User and Operational Experience – Key elements

Optimize user experience

- End to end **connection monitoring** (user to application)
- Continuous **performance optimization** (e.g., latency)

Optimize Operational Experience

- **Predict or detect in real time** any operational disruptions before the business is impacted
- **Automate remediation** for rapid resolution

Unify Management

- **Centralized management** across all enforcement points
  - Hardware
  - Virtual Firewalls
  - Cloud-Native Firewalls
  - SASE

Optimize User and Operational Experience – Implementation

	Essential controls	Capabilities to enable: Core	Capabilities to enable: Advanced
Optimize user experience	End to end connection monitoring (user to app)	☐ Health and performance for all users, branch sites, applications, and IT infrastructure monitored via ADEM	☐ Proactive notifications to users for self-serve via ADEM
	Continuous performance optimization (e.g., latency)		☐ App Acceleration enabled ☐ Metric collection enabled to verify app performance when using App Acceleration
Optimize Operational Experience	Predict or detect in real time any operational disruptions before the business is impacted	☐ Unified pane of glass for all incidents and alerts across network via AIOps ☐ Alerts correlated into single incidents and enriched with impact, cause, and resolution recommendations via AIOps	☐ Future capacity requirements forecasted to significantly reduce downtime via AIOps
	Automate remediation for rapid resolution		☐ Automated remediations based on AIOps insights across all form factors used to reduce MTTR and downtime
Unify Management	Centralize management in a single pane of glass across every enforcement point	☐ Strata Cloud Manager (SCM) or Panorama established as the unified pane of glass across all form factors	

Reduce Complexity with a Unified Zero Trust Platform

SUB-CATEGORY	ONE PLATFORM
Firewall	Strata Network Security Platform
Intrusion Prevention	
URL Filtering	
Sandbox	
DNS Security	
IoT / OT Security	
Data Loss Prevention (DLP)	
Cloud Access Security Broker	
ZTNA / Remote Access	
SD-WAN	
Remote Browser Isolation	
Enterprise Browser	
Secure Web Gateway (SWG)	
User Experience Management	

#platformization

paloalto NETWORKS

Focus People Effort on Right Side of Cyber Attack Lifecycle

Automated Detection and Prevention

Focus on this side

Strata™

SaaS Security

Prisma™ Access

Prisma™ Cloud

Cortex™ XDR

Reconnaissance

Weaponization and Delivery

Exploitation

Installation

Command and Control

Lateral Movement

Actions on the Objective

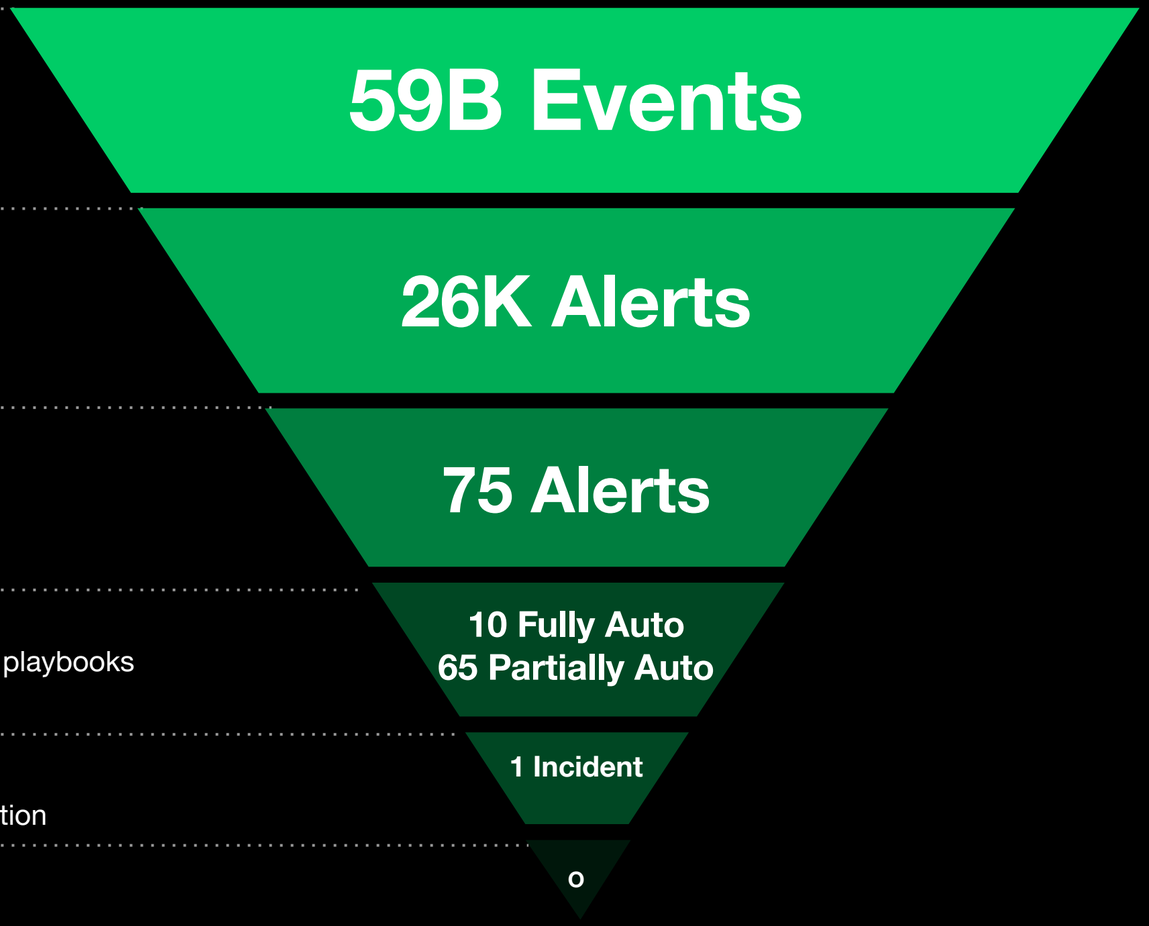
Cortex™ XSIAM

Focus on this side

Threat Alerting and Hunting

Daily Log & Alert Volume

DAY IN THE LIFE OF THE PALO ALTO NETWORKS SOC



Log Events
Includes all log events ingested to XSIAM

Raw Alerts
After AI-driven data analysis by XSIAM

Alerts
After grouping, exclusions, deduping by XSIAM

Analysis
Automated fully or partially by playbooks

Incidents
Any alert that requires SOC action

Major Incidents

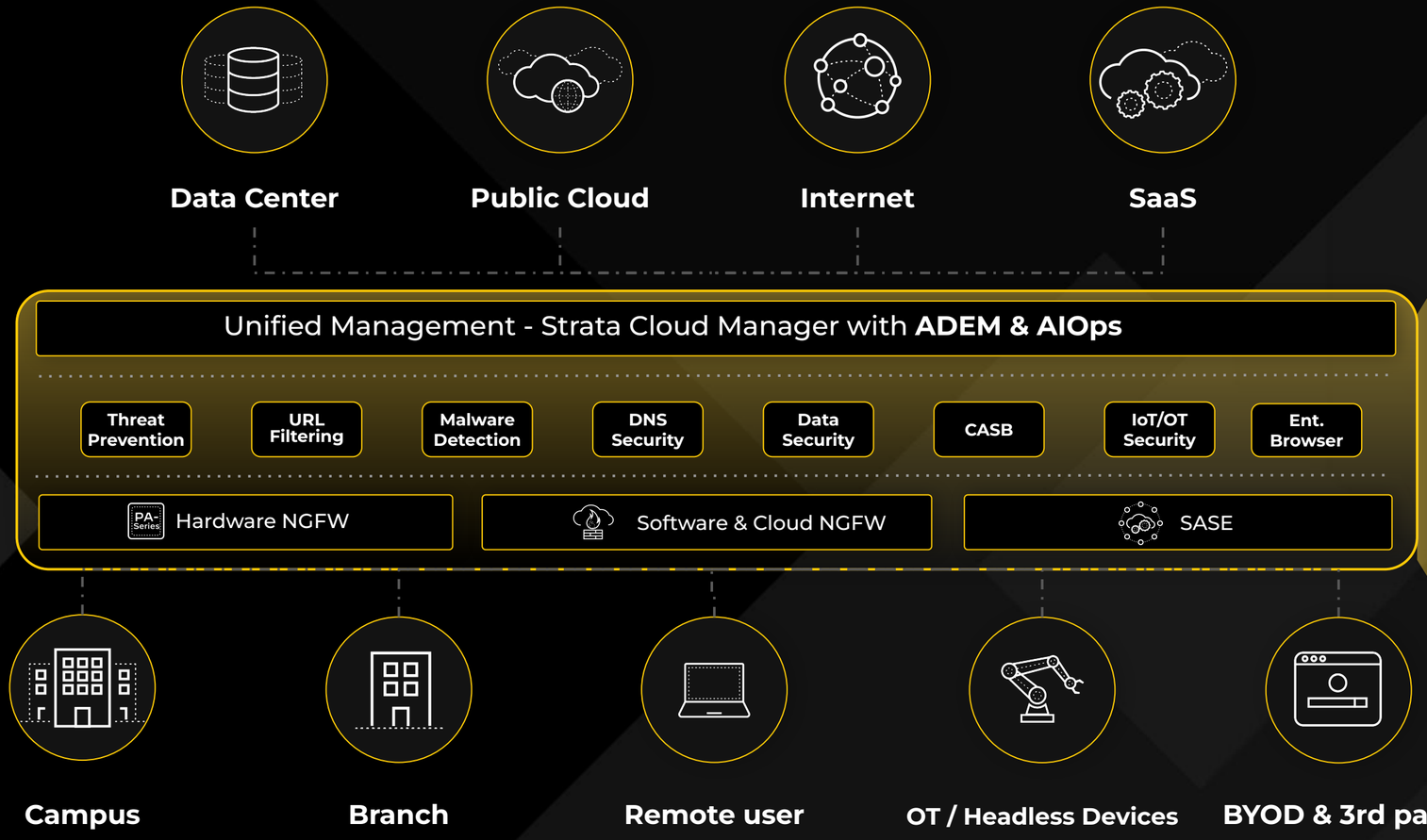
7
MINUTES
Mean Time to Detect

1
MINUTE
Mean Time to Respond
(High priority)

65
FTE
Staff automation efficiency savings
(per annum)

How the Strata Platform maps to the 5-pillars

Strata Network Security Platform is modular so you can choose your path to Zero Trust



AI-Powered Unified Management

Predict disruptions, enable security best practices, and deploy unified policies.

Cloud Delivery Security Services

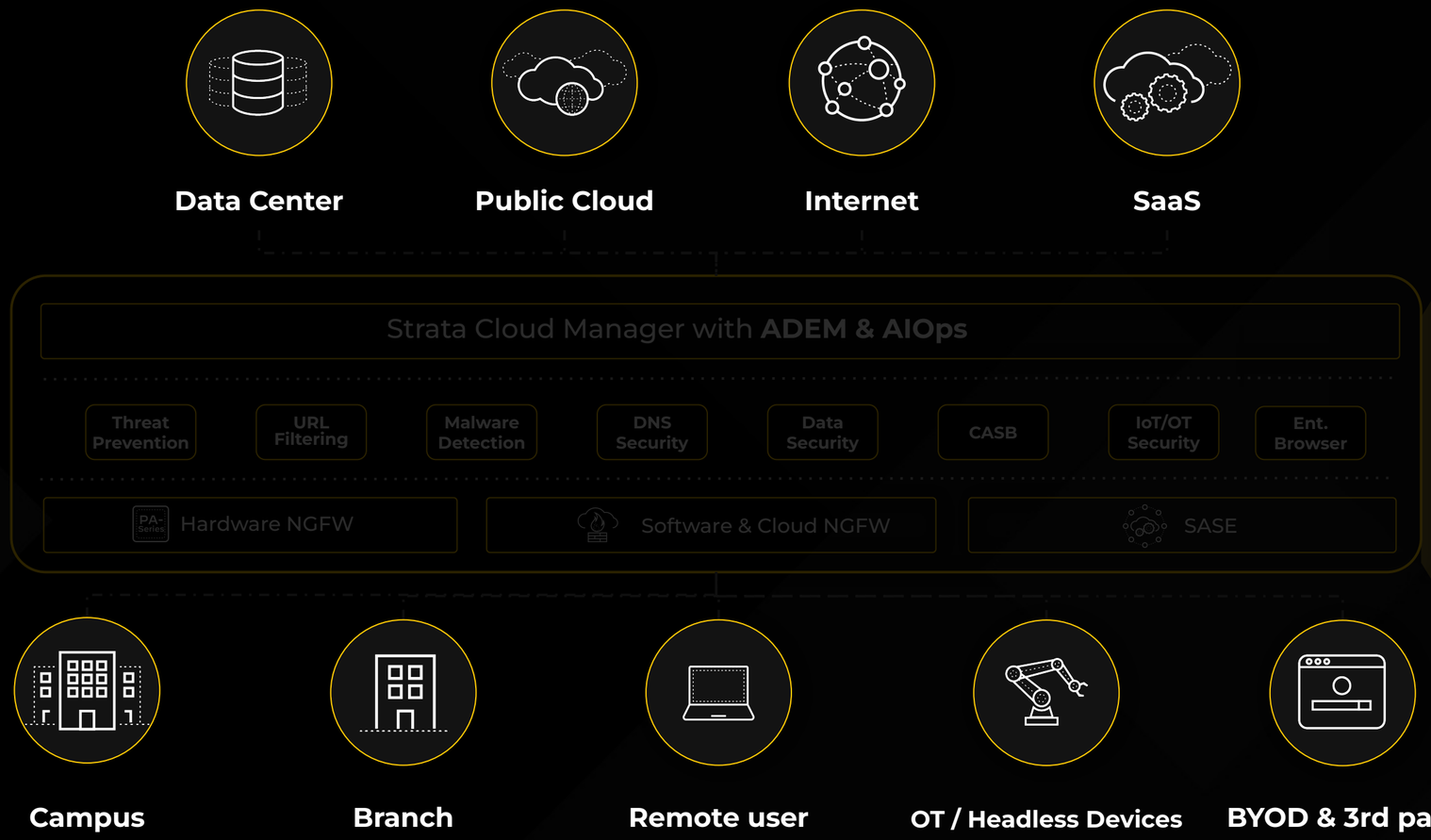
Advanced security inspection techniques prevent threats in real time using AI & Automation

Best-in-class enforcement points

Industry's only recognized leader in Network, Virtual & Cloud Firewalls, SASE, and SD-WAN.

paloalto NETWORKS

Strata Network Security Platform is modular so you can choose your path to Zero Trust

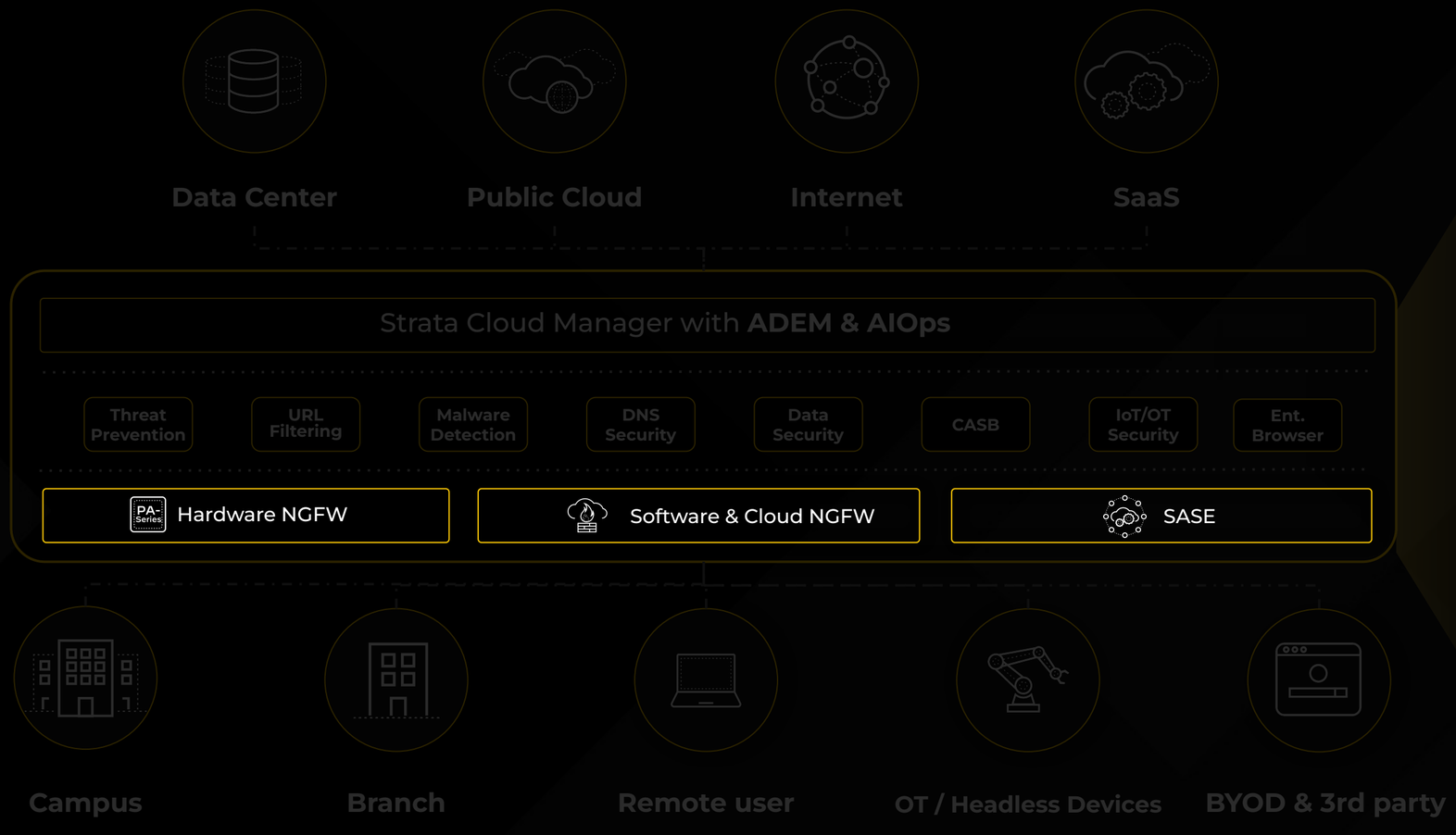


Zero Trust Principles

1. Identify and Verify all Users, Devices, and Applications

- ❑ Identify all users.
- ❑ Identify all devices. Verify posture compliance.
- ❑ Identify all applications.
- ❑ Continuously verify user, device, posture, and application.

Strata Network Security Platform is modular so you can choose your path to Zero Trust



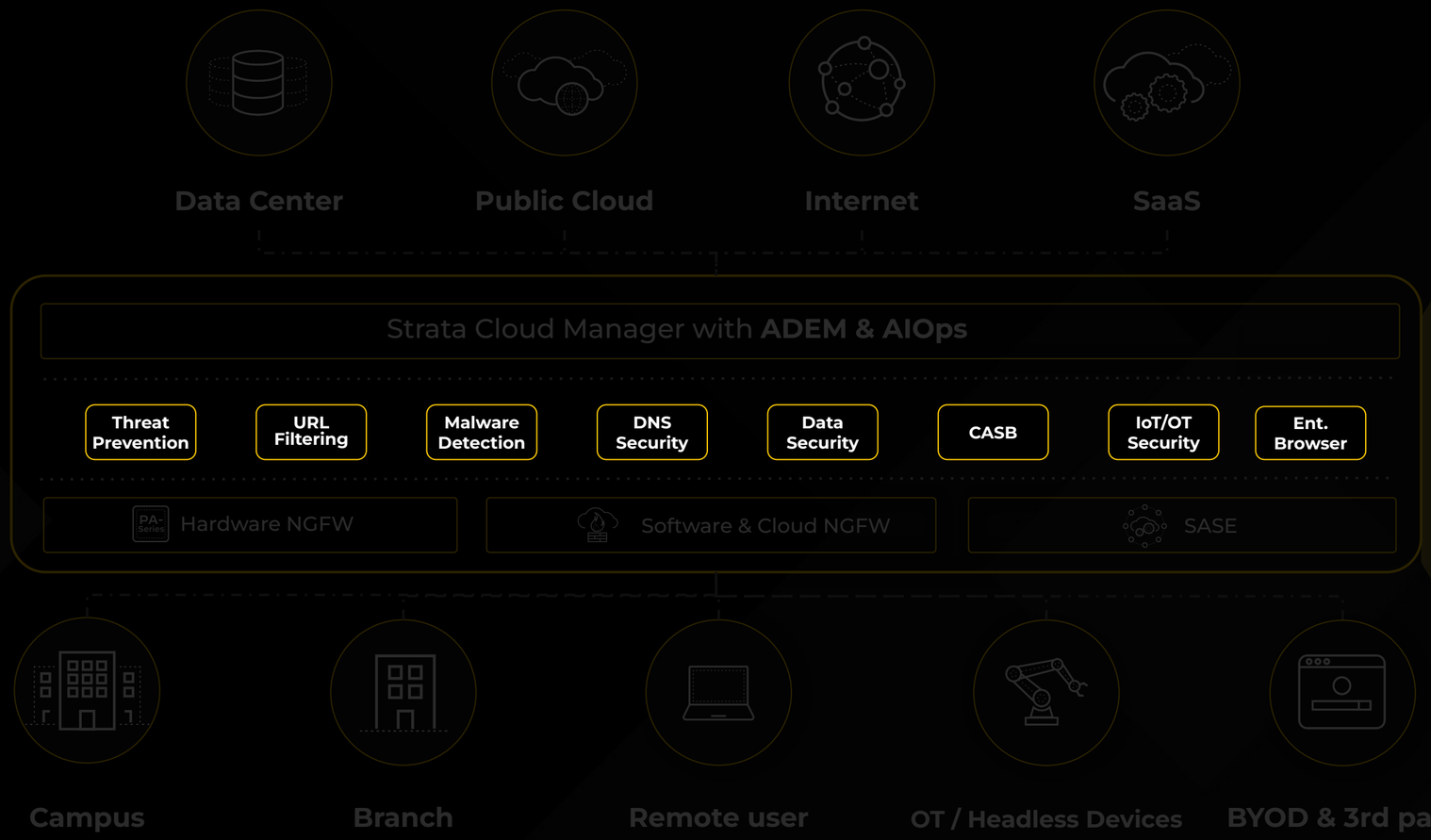
Zero Trust Principles

1. Identify all Users, Devices, Applications, Data
2. Enforce least privilege policy
3. Apply inside security inspection
4. Control data access & movement
5. Enhance User and Operator Experience
6. Automate Security Actions with AI and Automation

- ❑ Contextual policies based on user, device, and apps
- ❑ Connections allowed based on business needs.
- ❑ Leverage dynamic access policies where possible.
- ❑ Enable Decryption for complete user to application visibility.
- ❑ Deny all other traffic by default.

paloalto NETWORKS

Strata Network Security Platform is modular so you can choose your path to Zero Trust



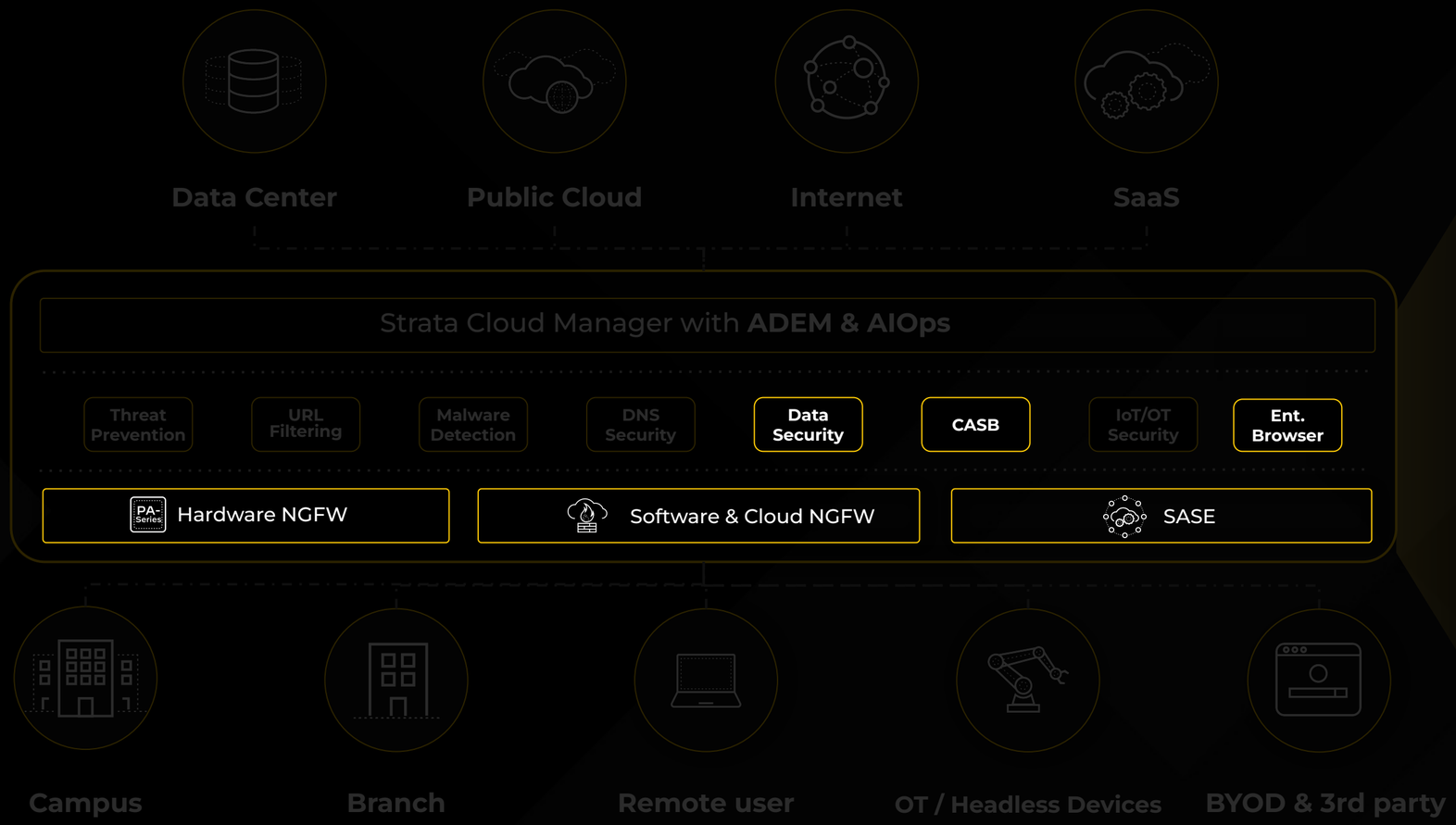
Zero Trust Principles

1. Identify all Users, Devices, Applications, Data
2. Enforce least privilege policy
3. Apply holistic security inspection
4. Control data access & movement
5. Enhance User and Operator Experience

- ❑ **Prevent as many attacks as possible by enabling all baseline security features.**
- ❑ **Apply additional prevention by use case (IoT, SaaS, RBI, EB, etc…)**
- ❑ **Enable Decryption to increase attack prevention capabilities.**
- ❑ **Improve detection analytics with centralized logging.**

paloalto NETWORKS

Strata Network Security Platform is modular so you can choose your path to Zero Trust



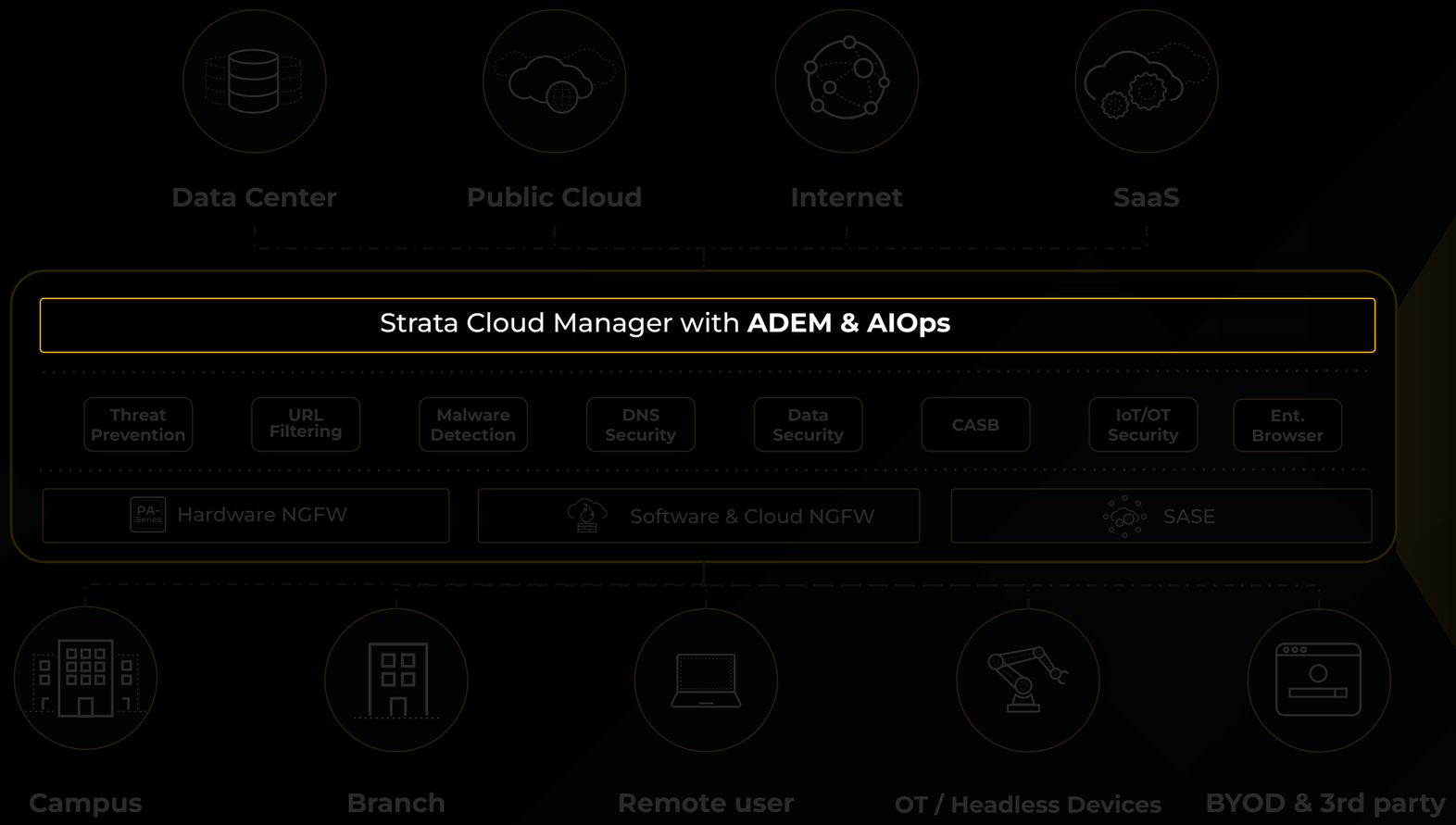
Zero Trust principles

- ❑ All data should be **identified, classified, and tagged.**
- ❑ Use **data context** for access policies.

4 Control data access & movement

5 Optimize user and operational experience

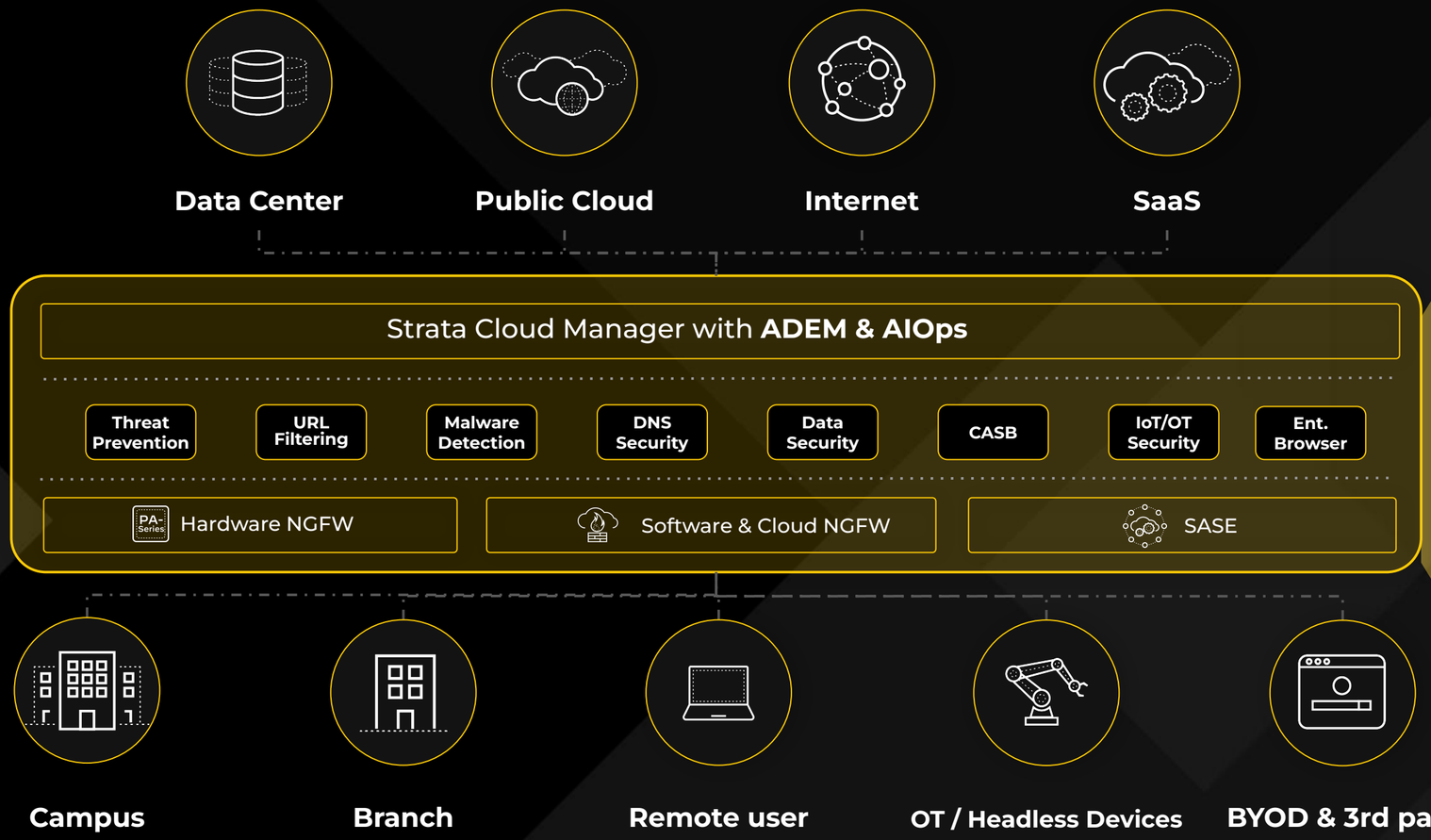
Strata Network Security Platform is modular so you can choose your path to Zero Trust



- ❑ Enhance experience with **user to application** visibility.
- ❑ **Enhance** management, threat handling, and operations **with AI**
- ❑ Use **AI to Predict** user experience issues.
- ❑ Create consistent policies with **unified management**.

5 Optimize user and operational experience

Strata Network Security Platform is modular so you can choose your path to Zero Trust



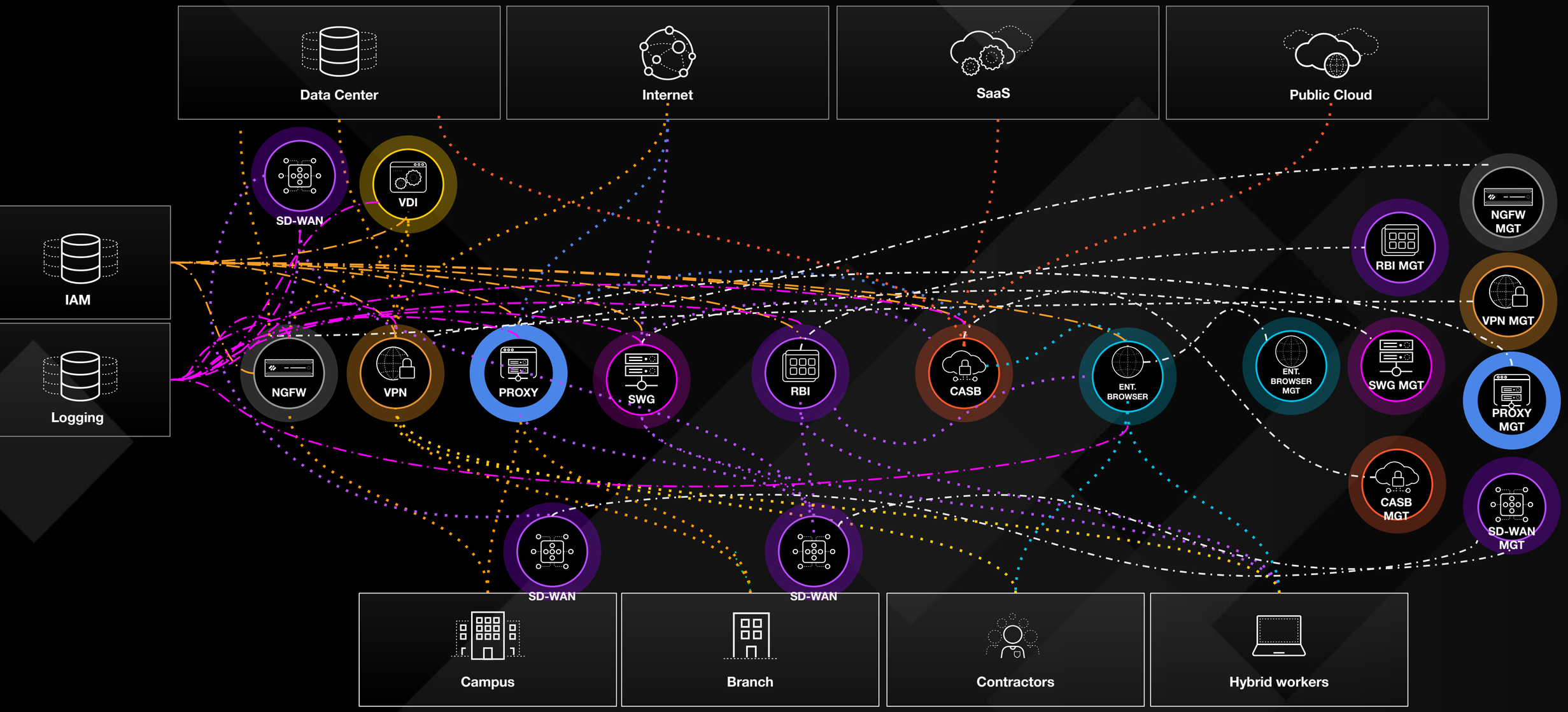
Zero Trust Principles

1. Identify and verify all Users, Devices, and Applications
2. Enforce least privilege policy
3. Apply holistic security inspection
4. Control data access & movement
5. Optimize user and operational experience

paloalto NETWORKS

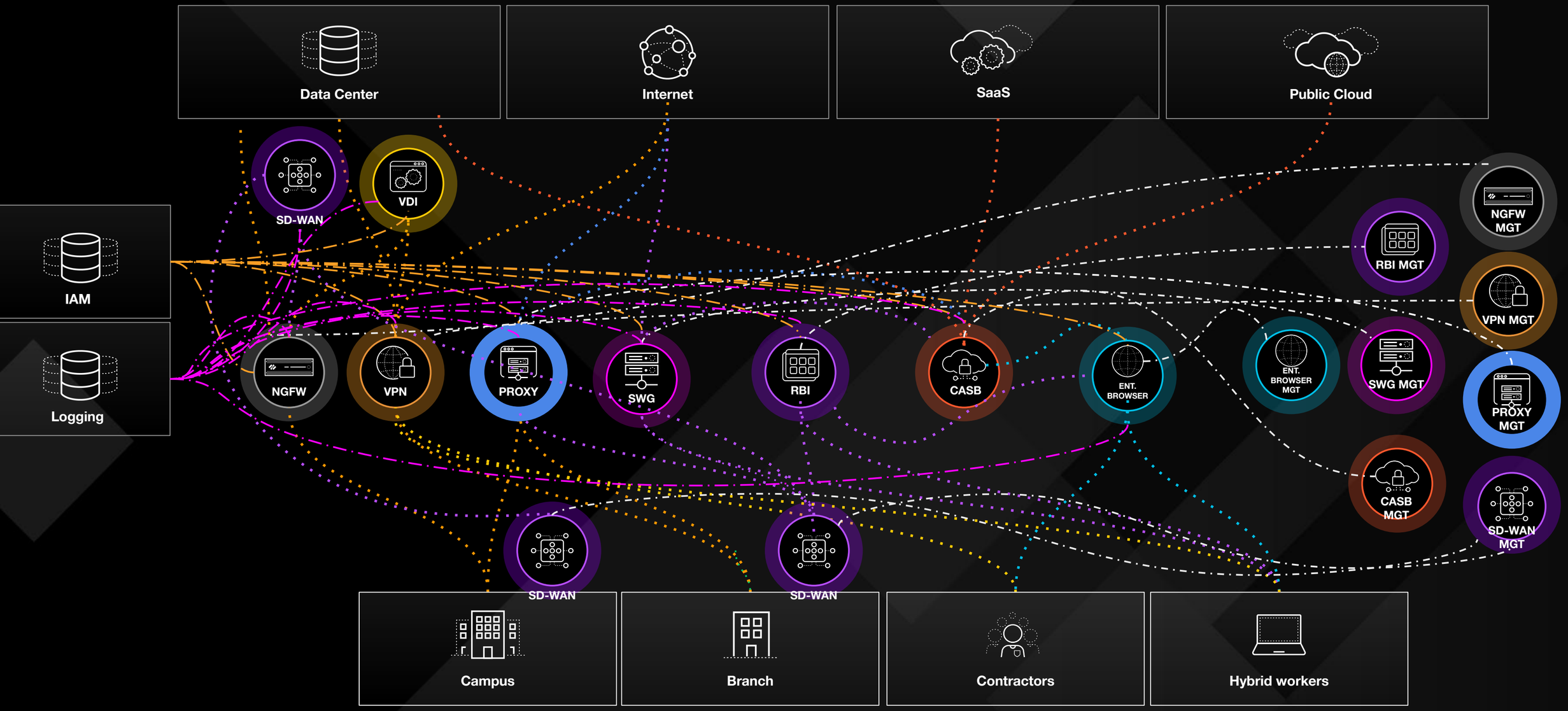
A Sequence to introduce why PANW started this ZT Journey

Why did Palo Alto Networks Begin this Journey to Zero Trust?



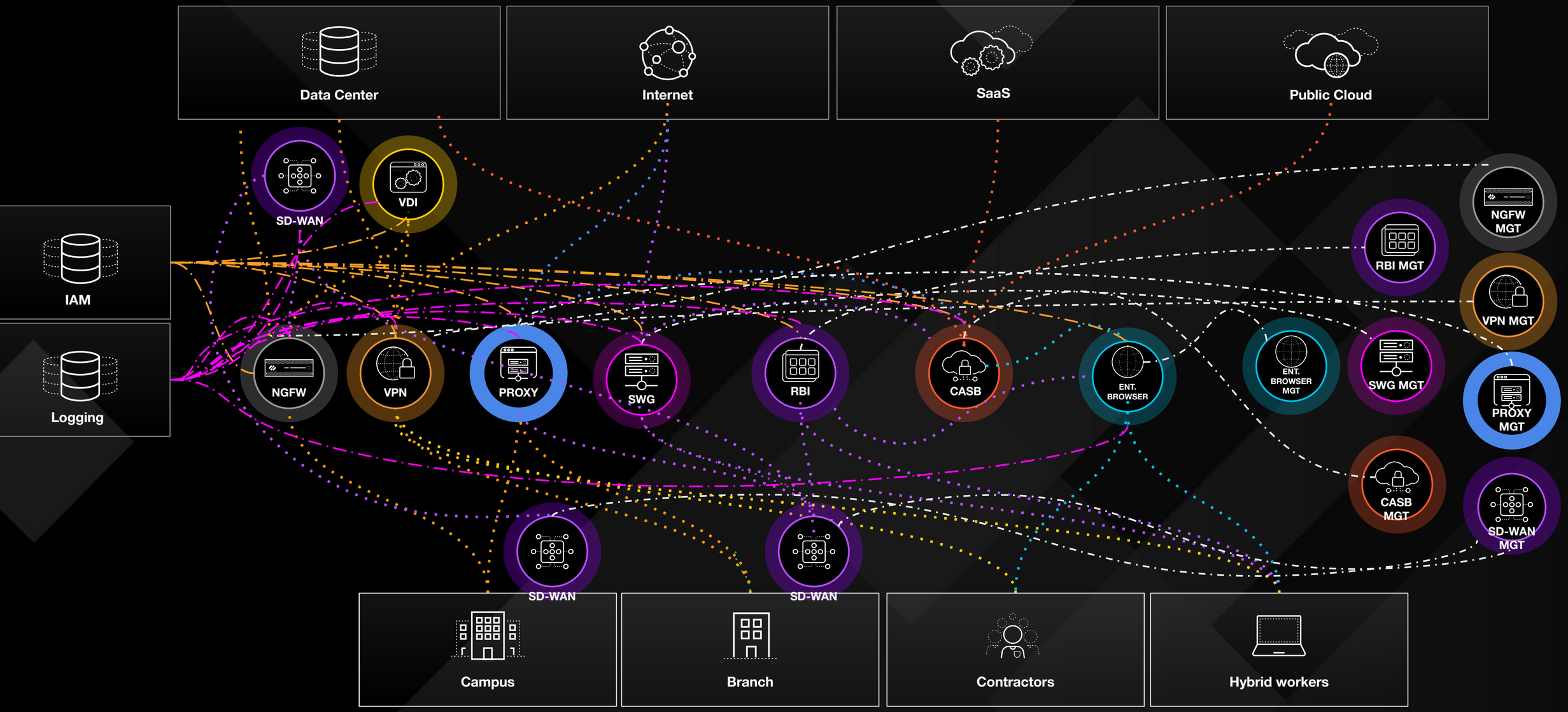
paloalto NETWORKS | STRATA

Without A Platform Approach, Network Security was a Mess

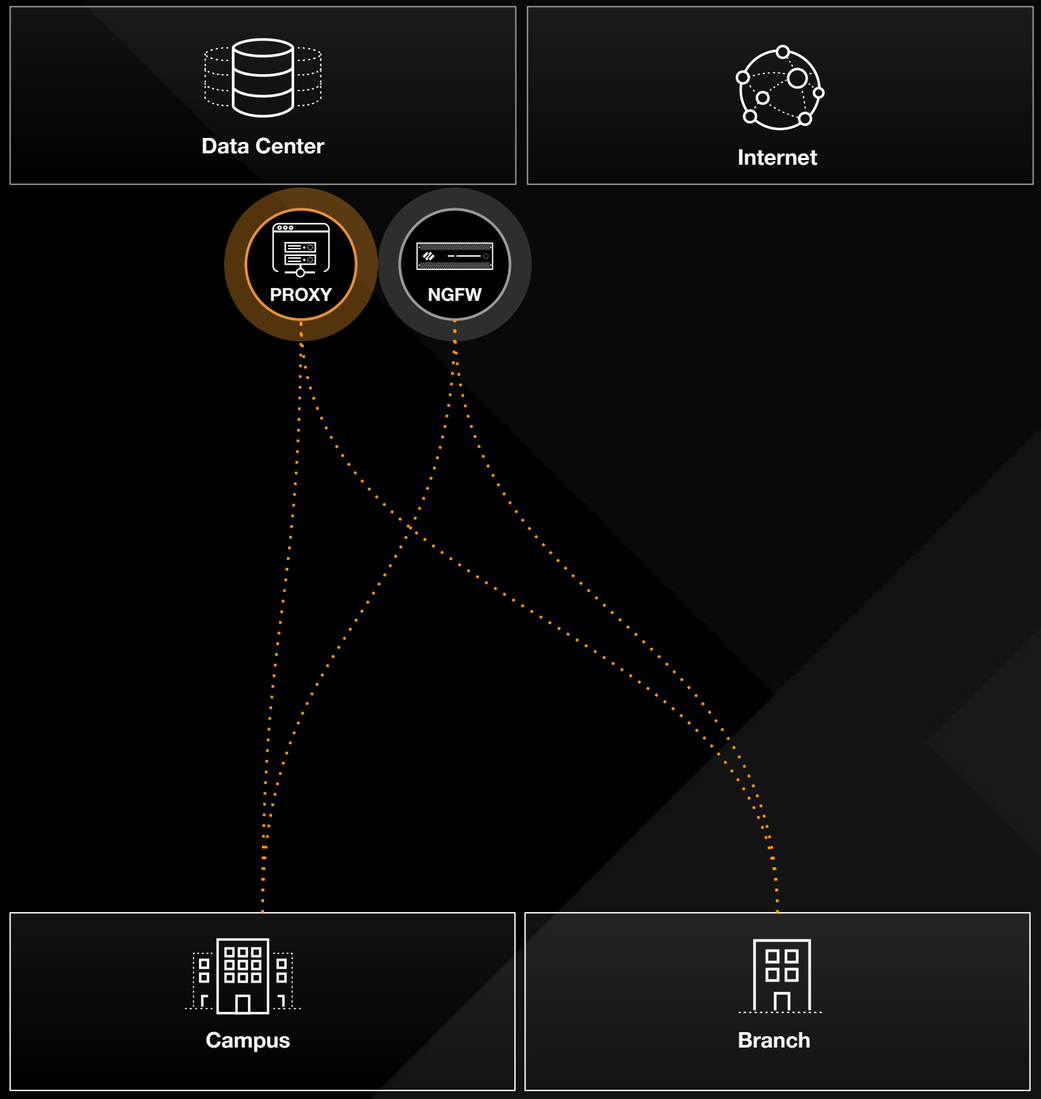


paloalto NETWORKS | STRATA

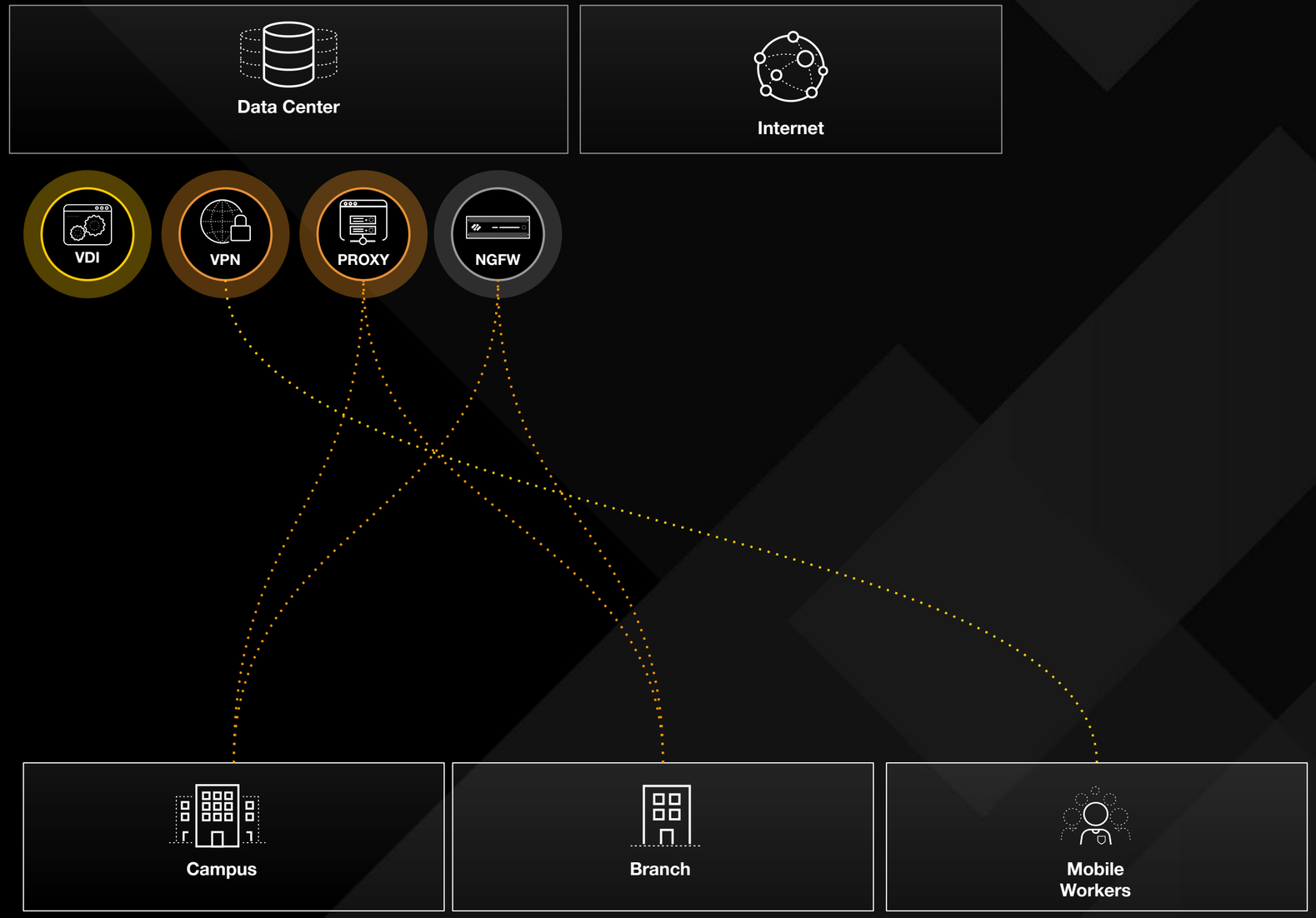
How did we get here?



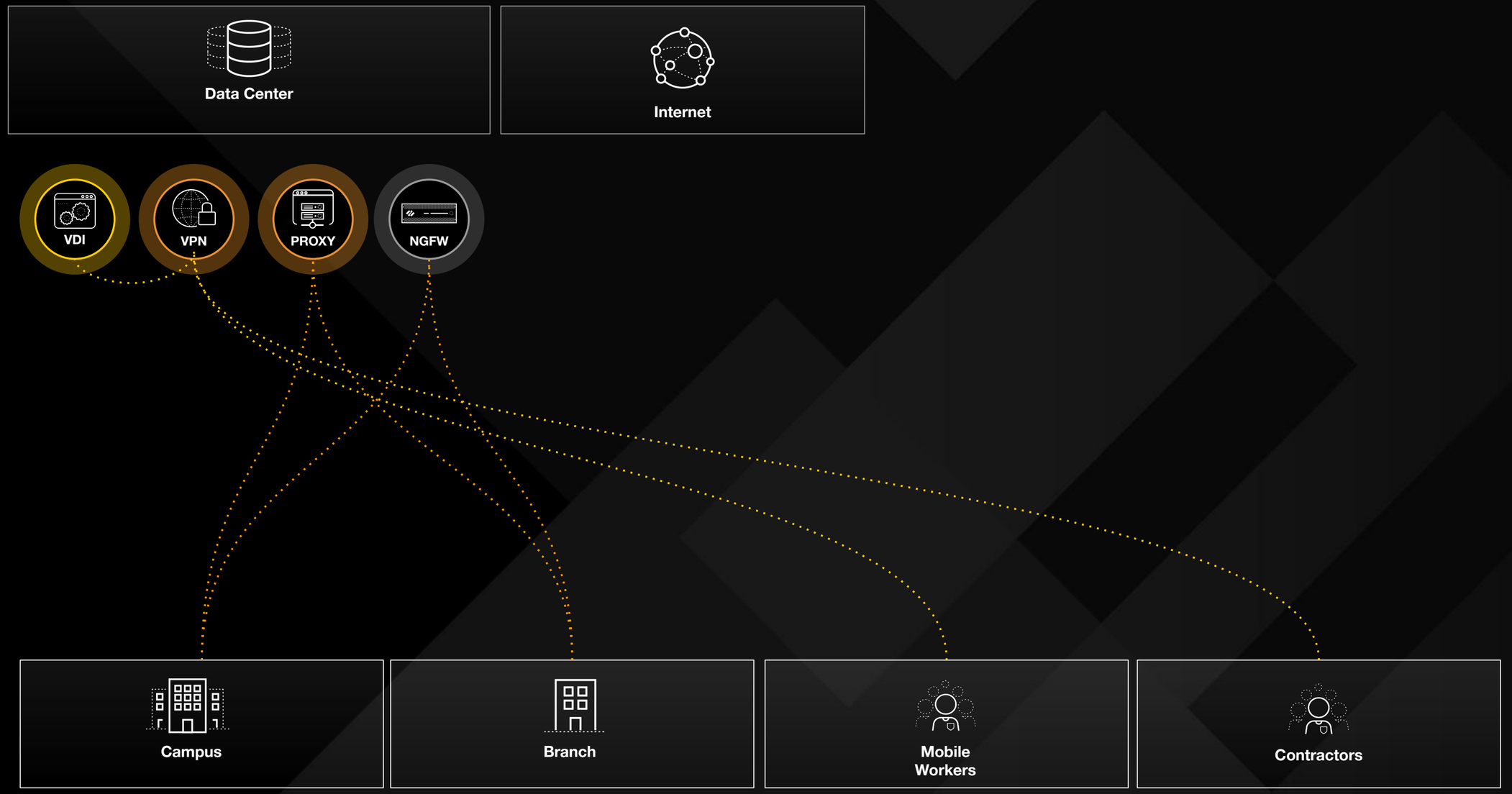
In the past, employees worked from a central location…



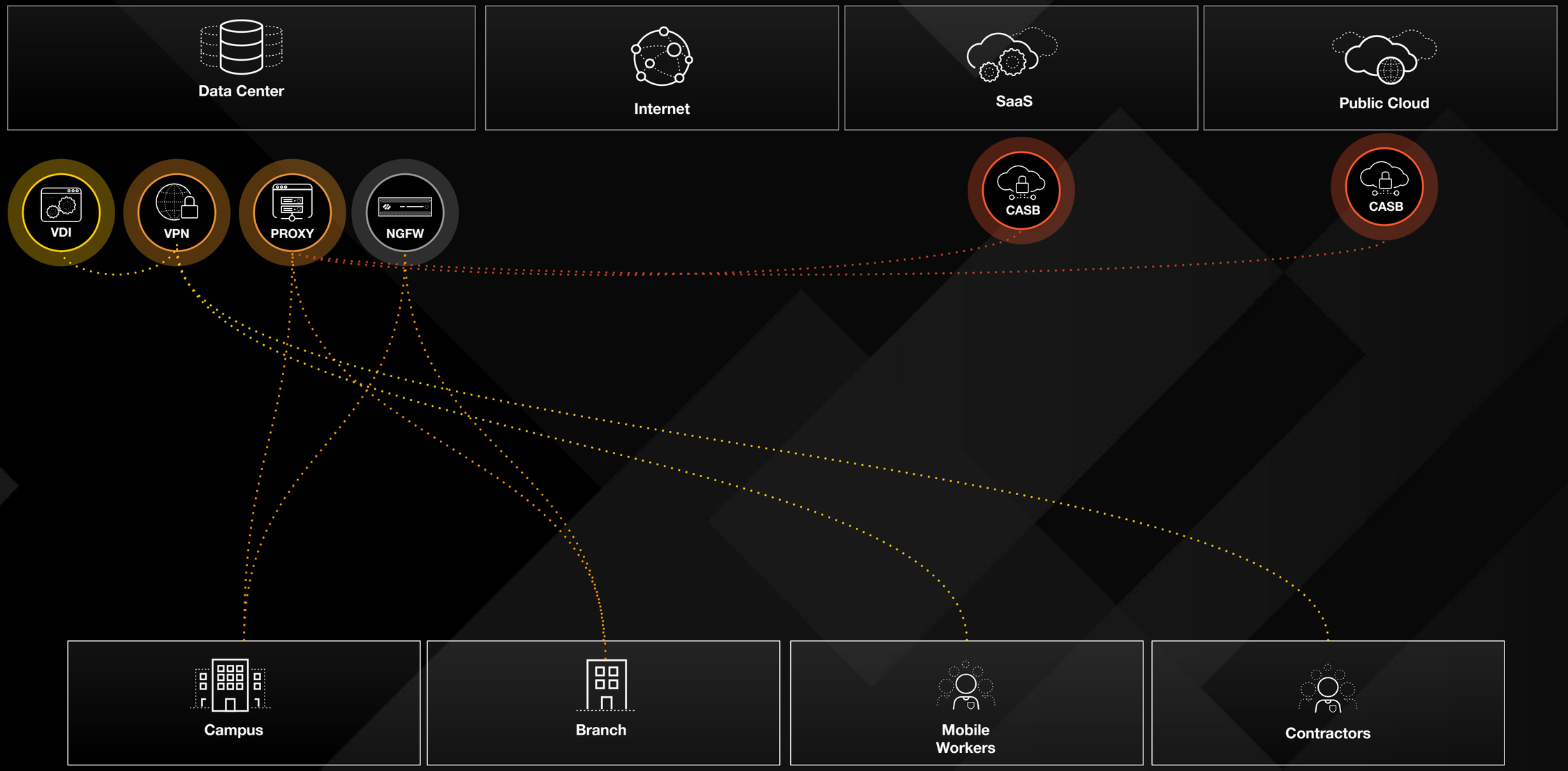
…then occasionally from a remote location



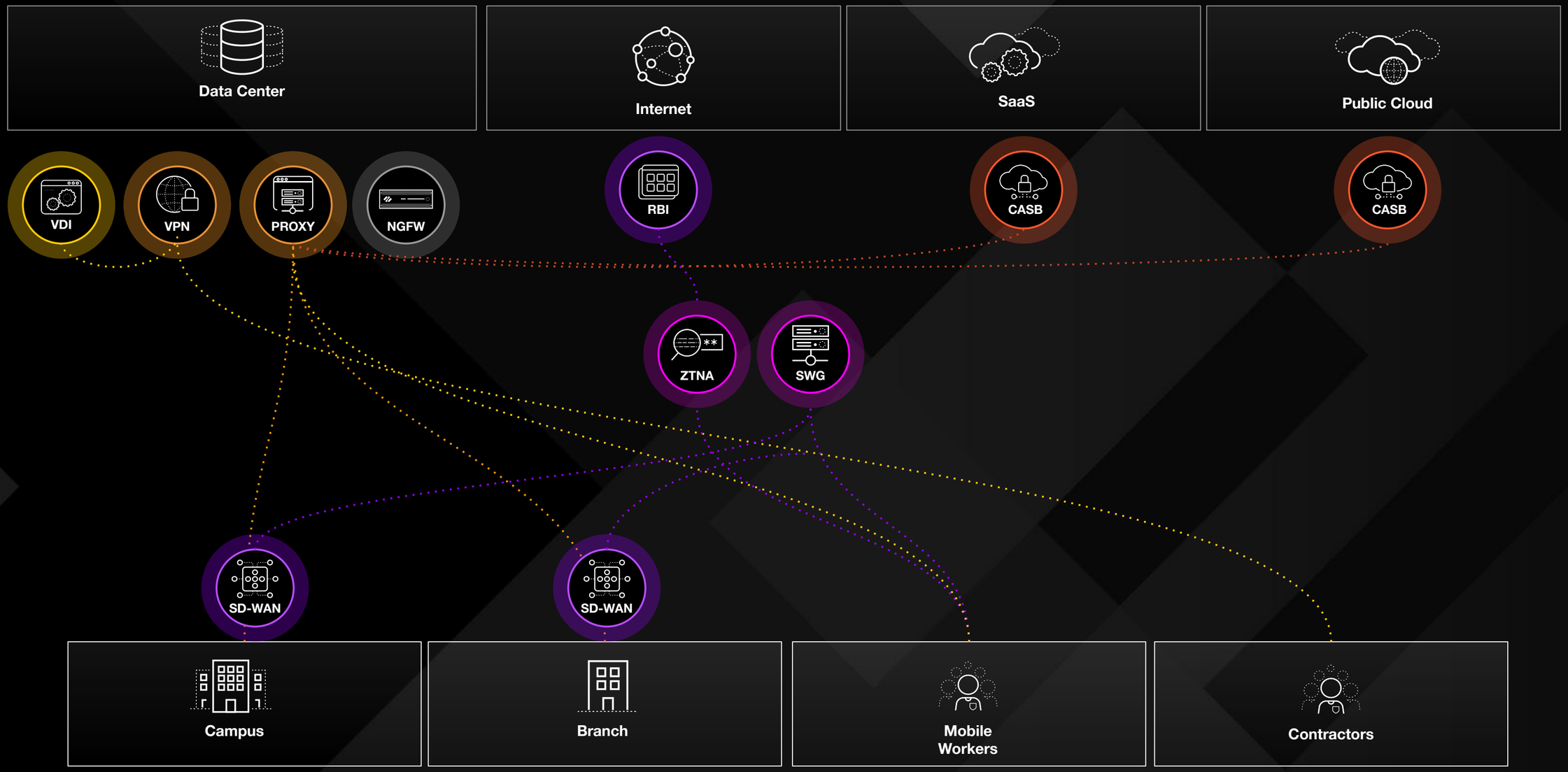
…and contractors needed access to corporate info via managed devices



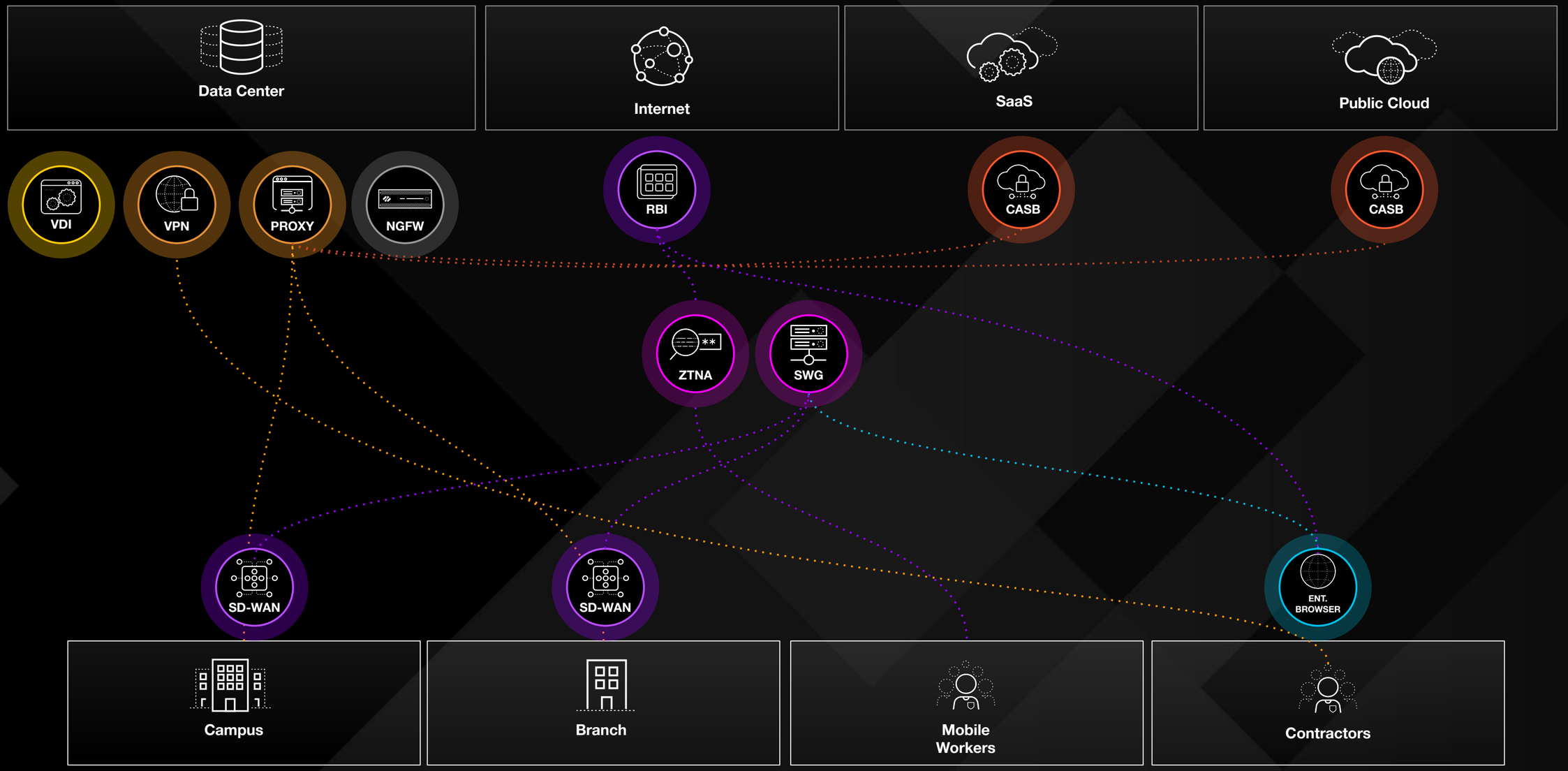
SaaS apps and public cloud access secured through CASB



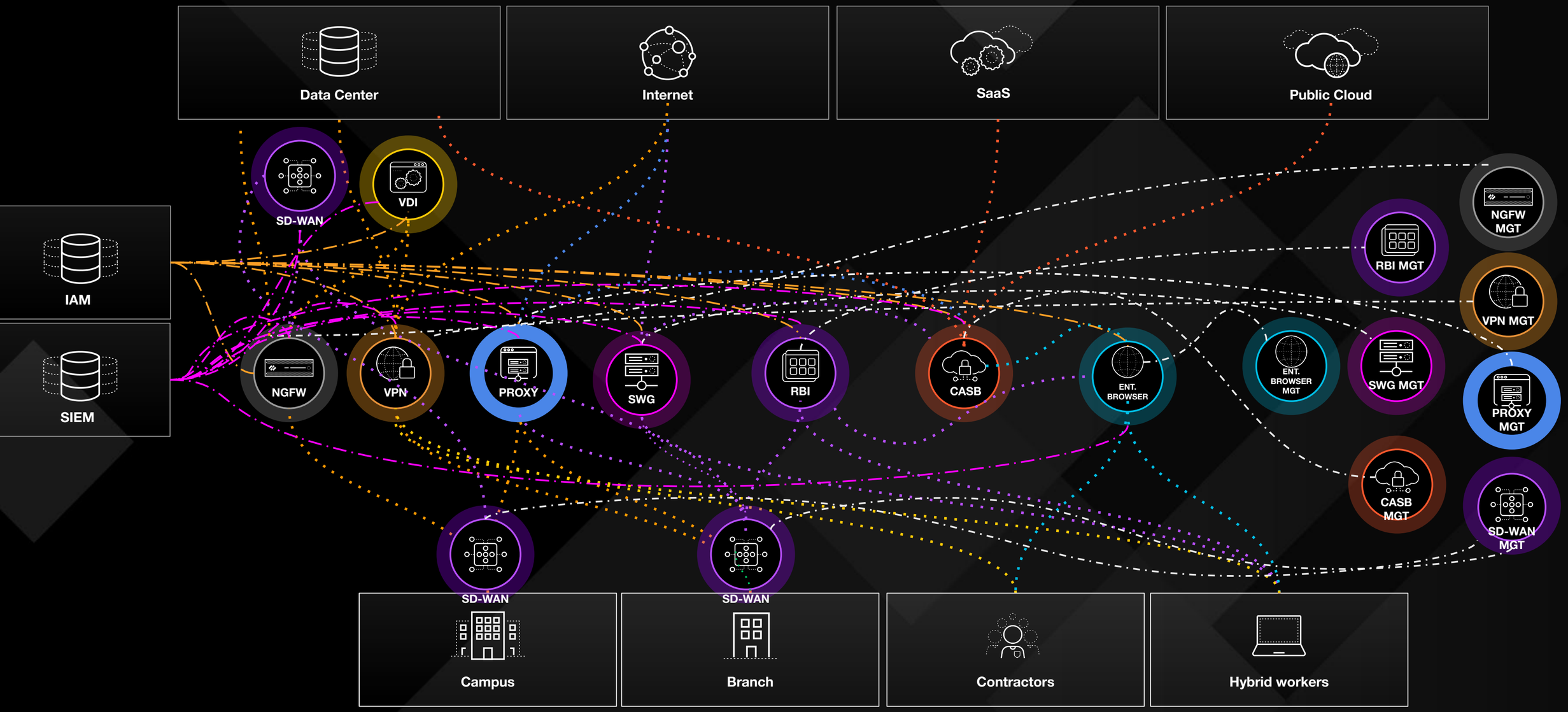
Increasing hybrid work necessitated SASE



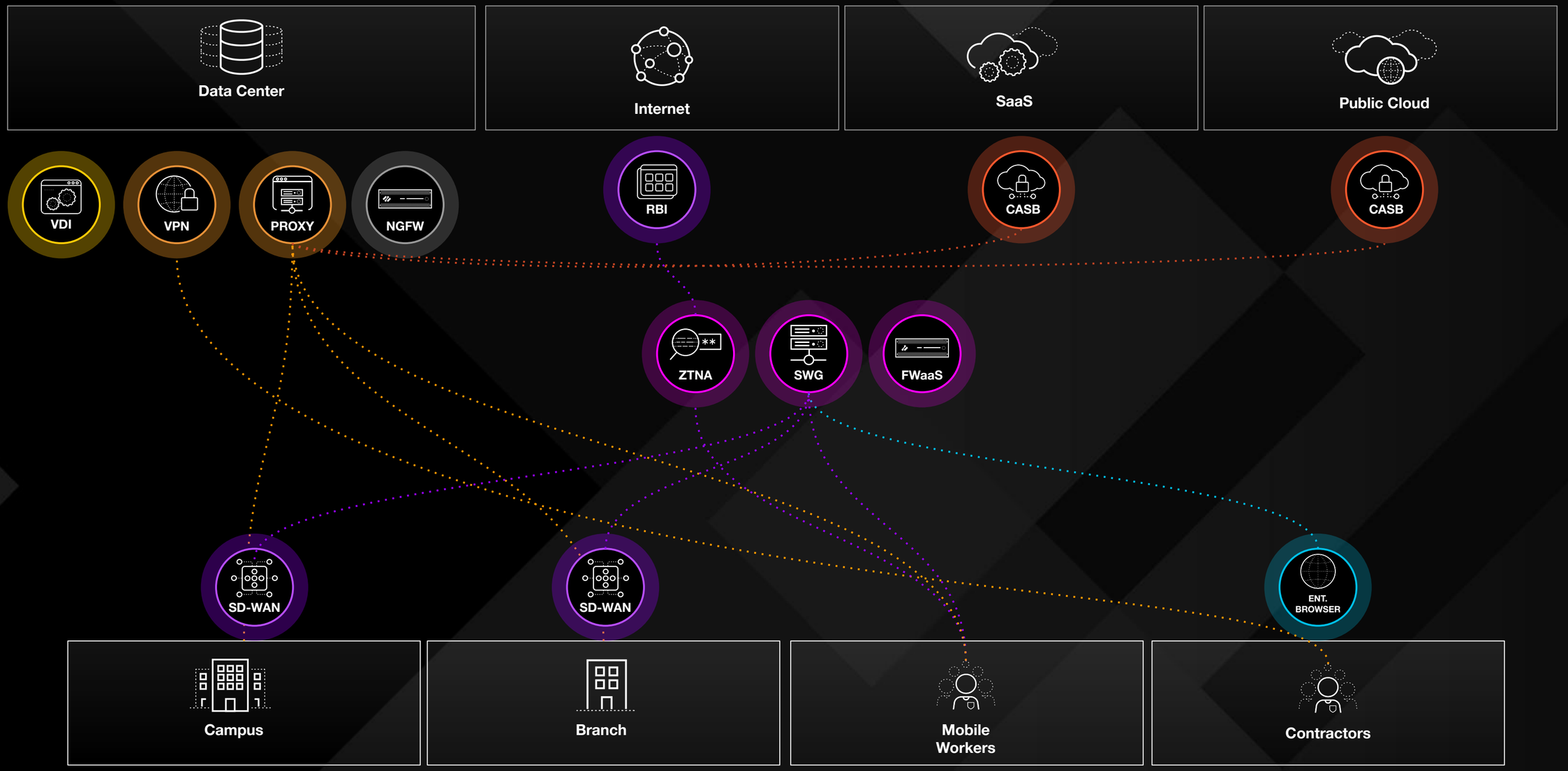
Contractors and Unmanaged Devices secured through Enterprise Browser



Add in SIEM, Identity, Management… Don’t forget overlapping functionality

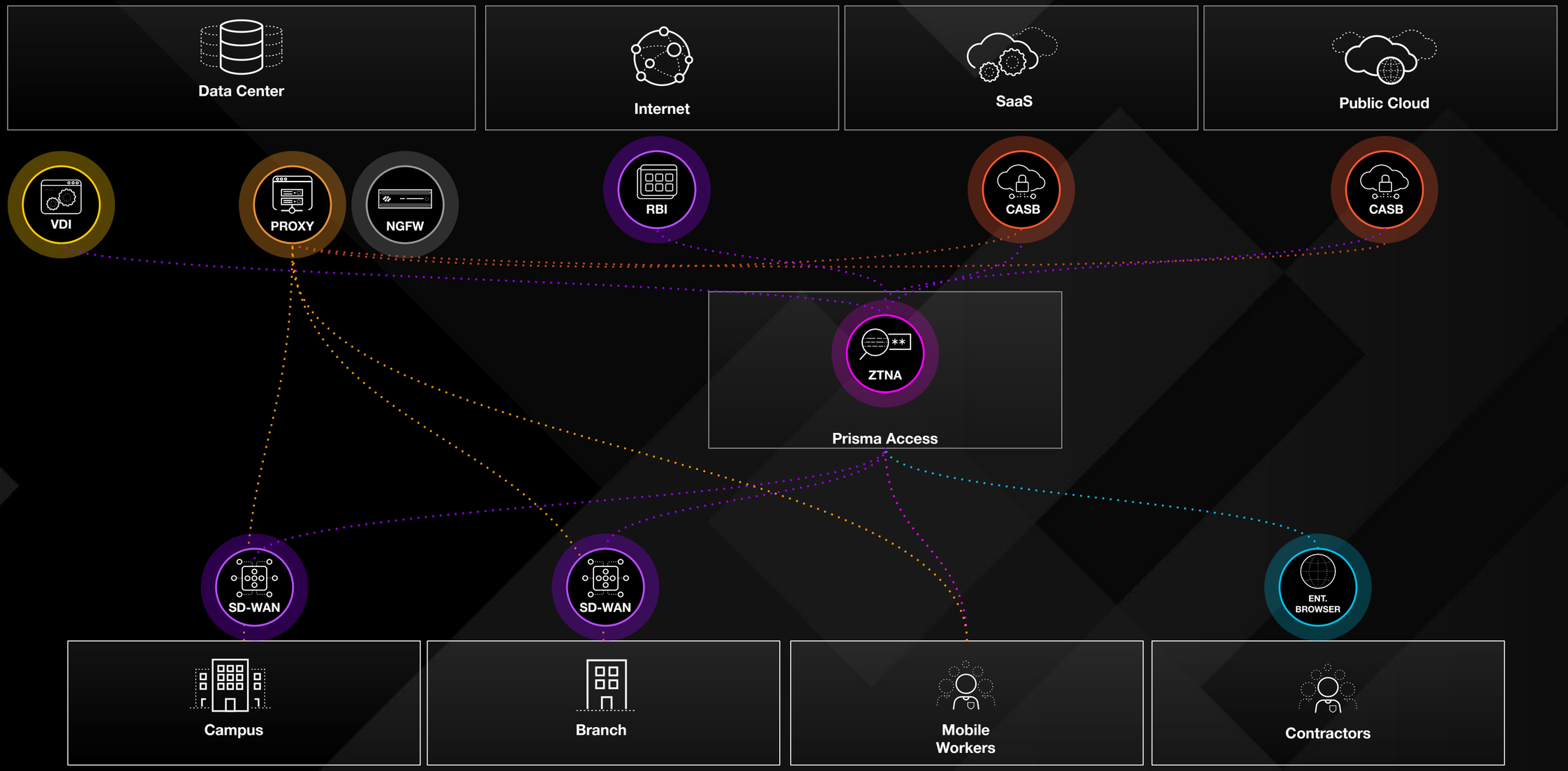


A platform approach doesn’t mean migrate everything at once

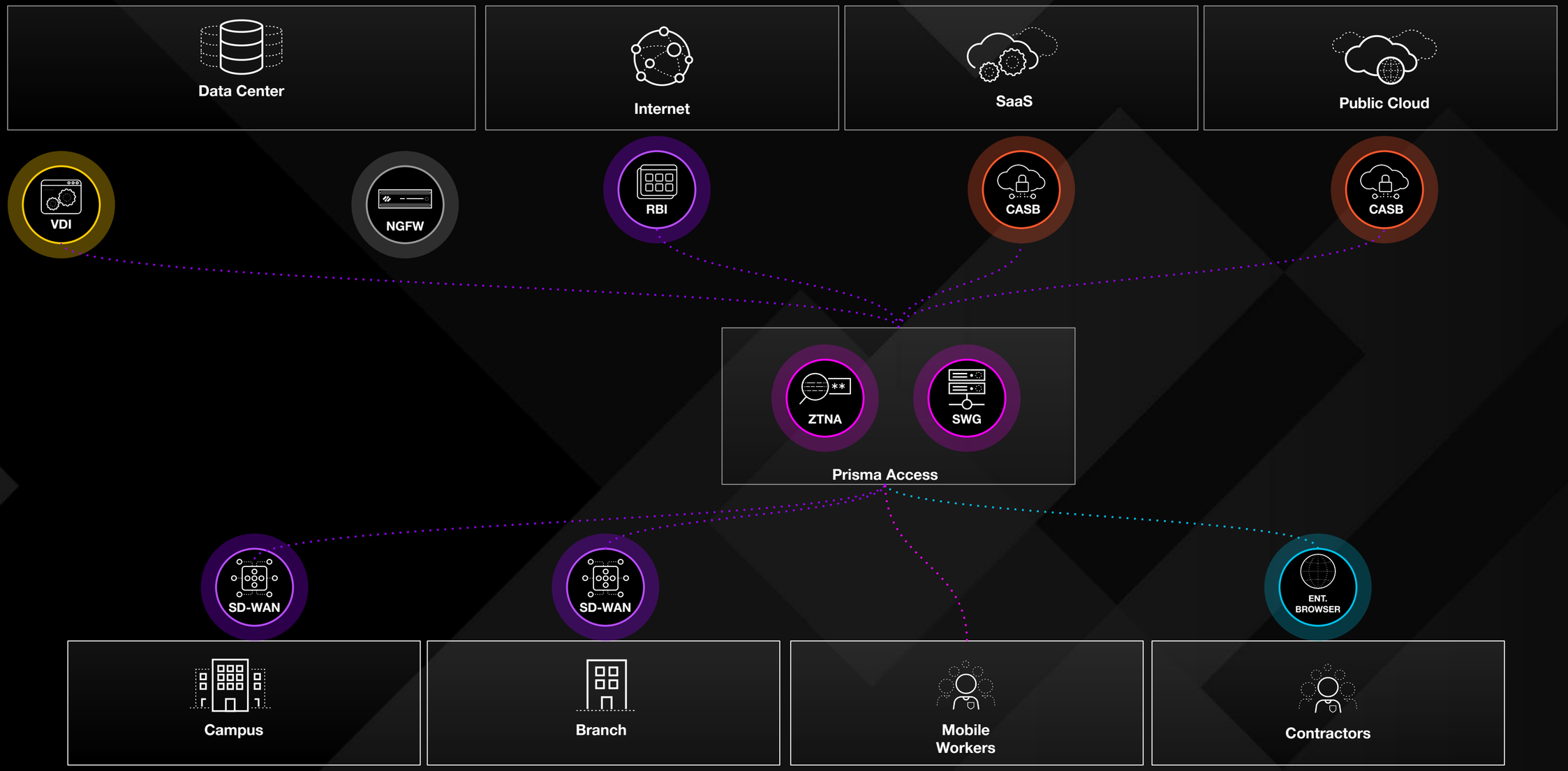


paloalto NETWORKS | STRATA

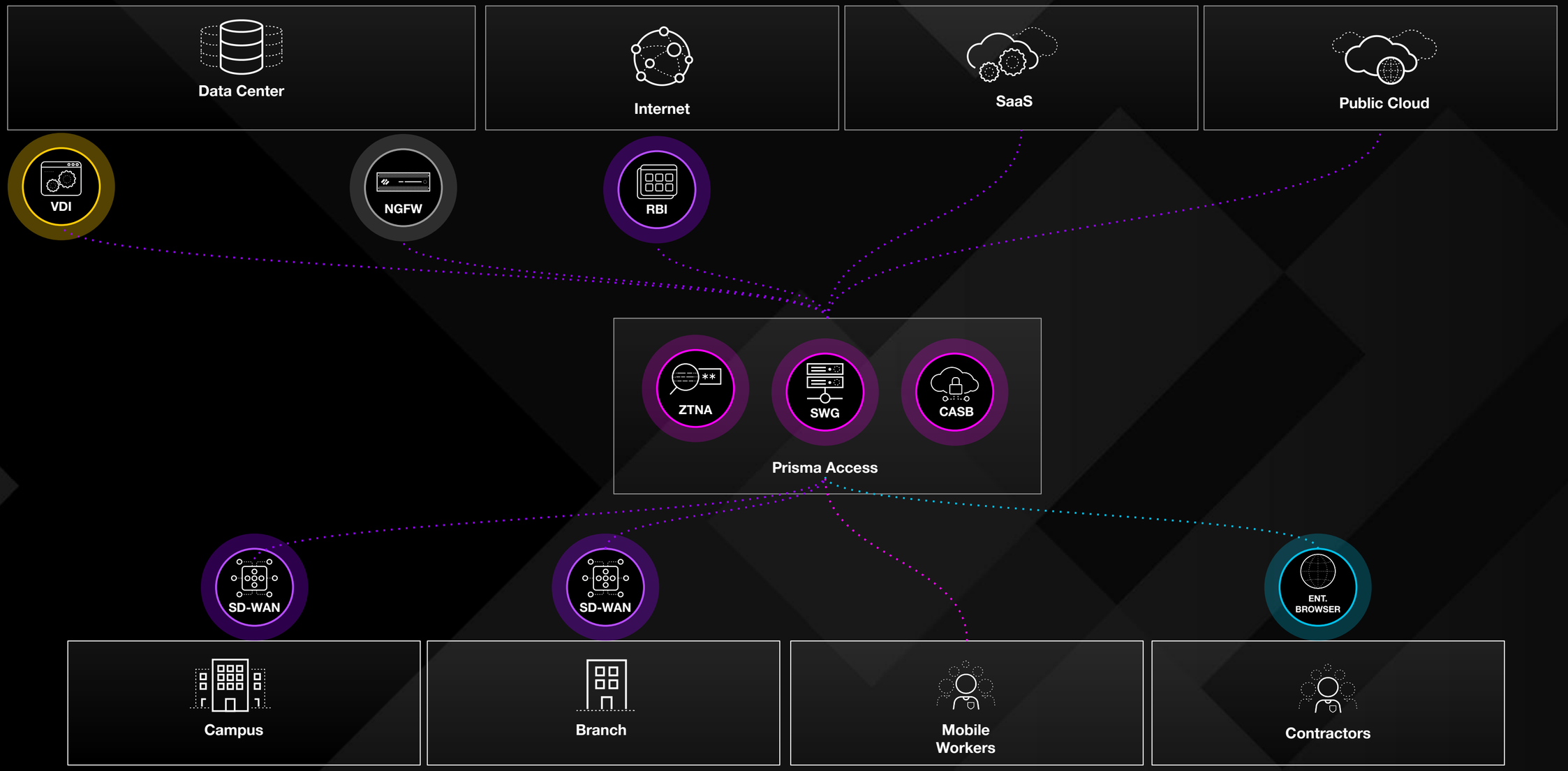
Migrate User Traffic - VPN to ZTNA



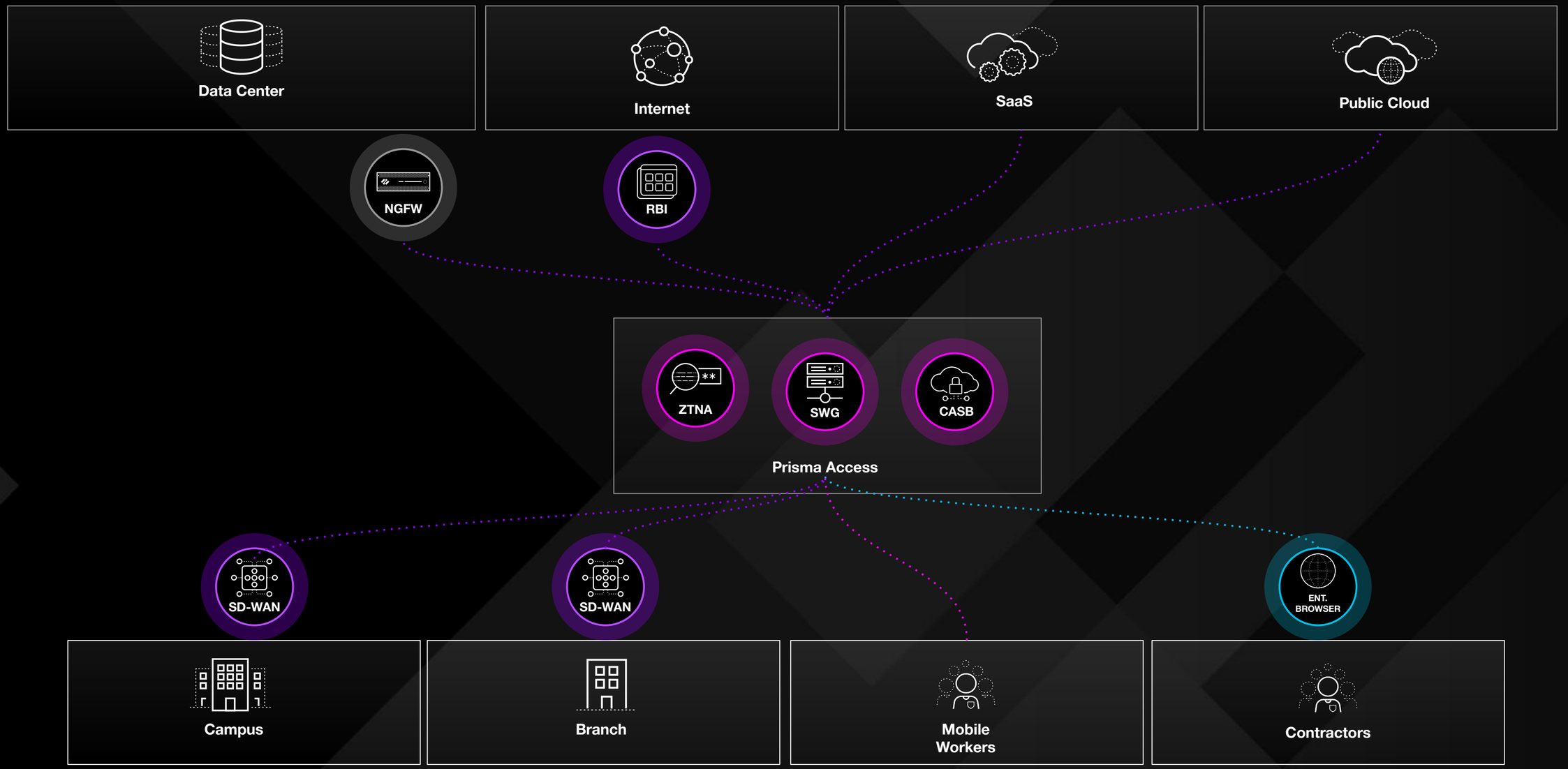
Continue to Migrate User Traffic - Proxy to Cloud SWG/Proxy



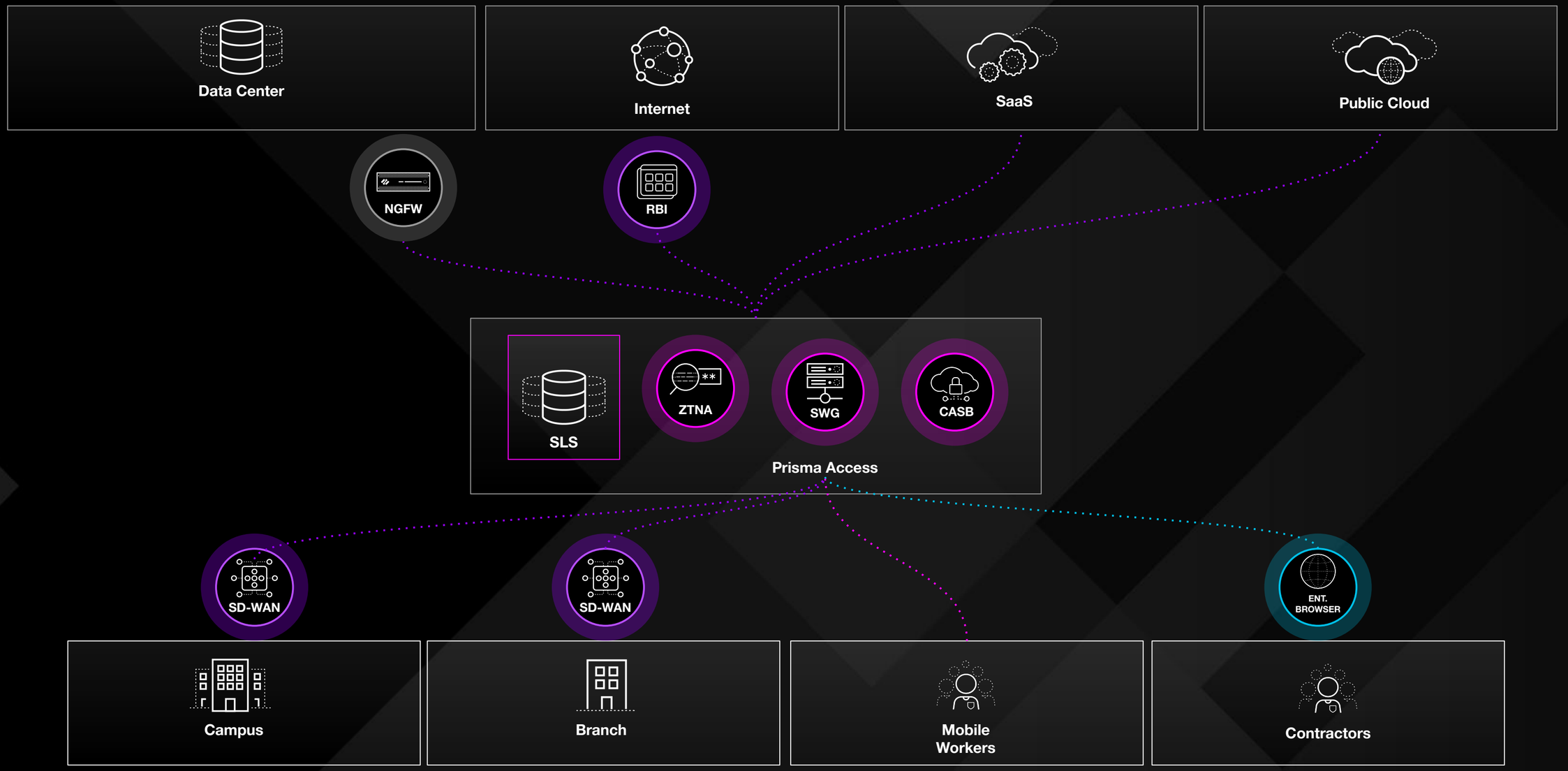
Leverage the Platform for CASB/DLP



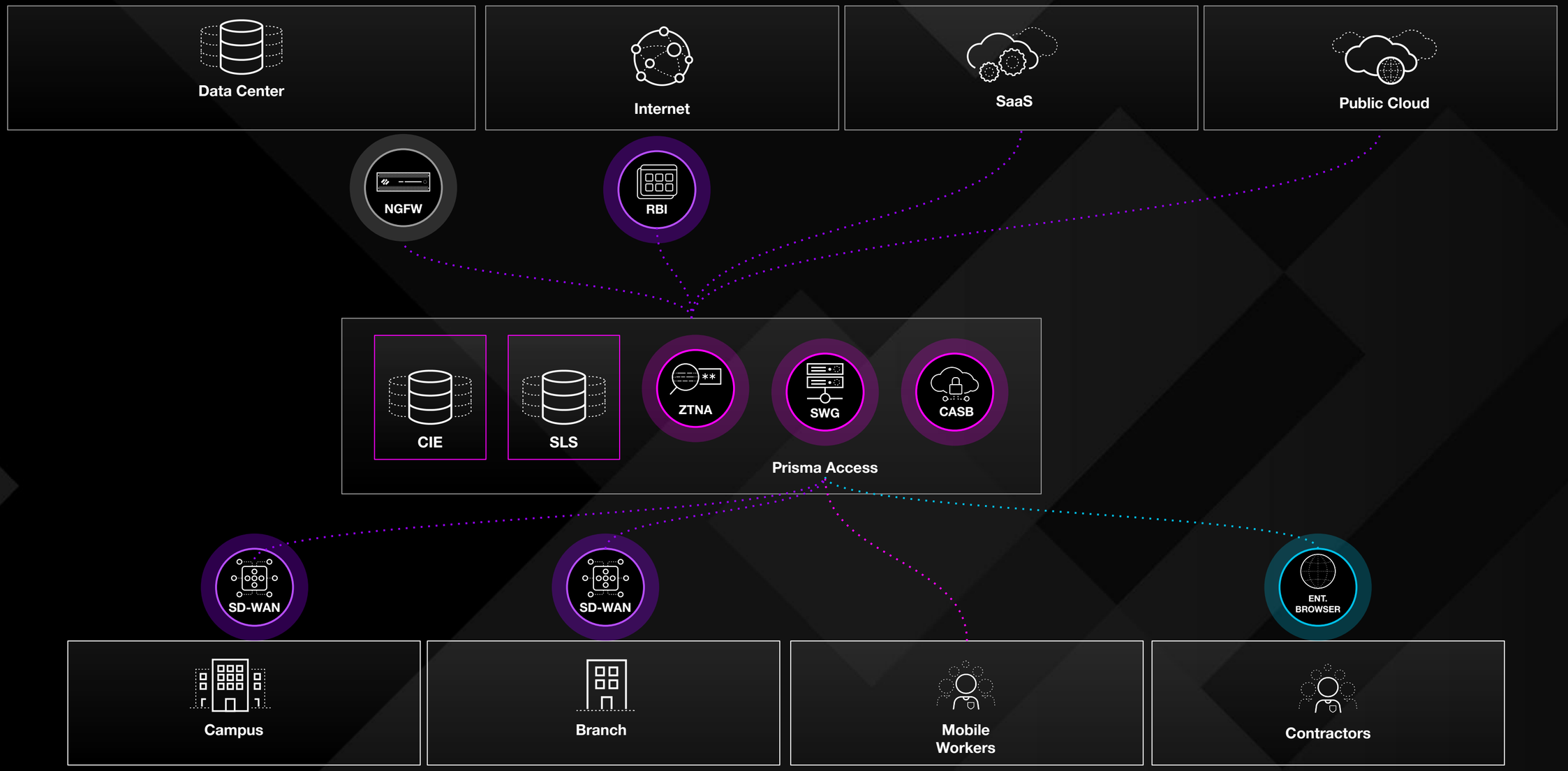
Enterprise Browser can reduce or replace VDI



The Platform includes centralized logging - Strata Logging Service

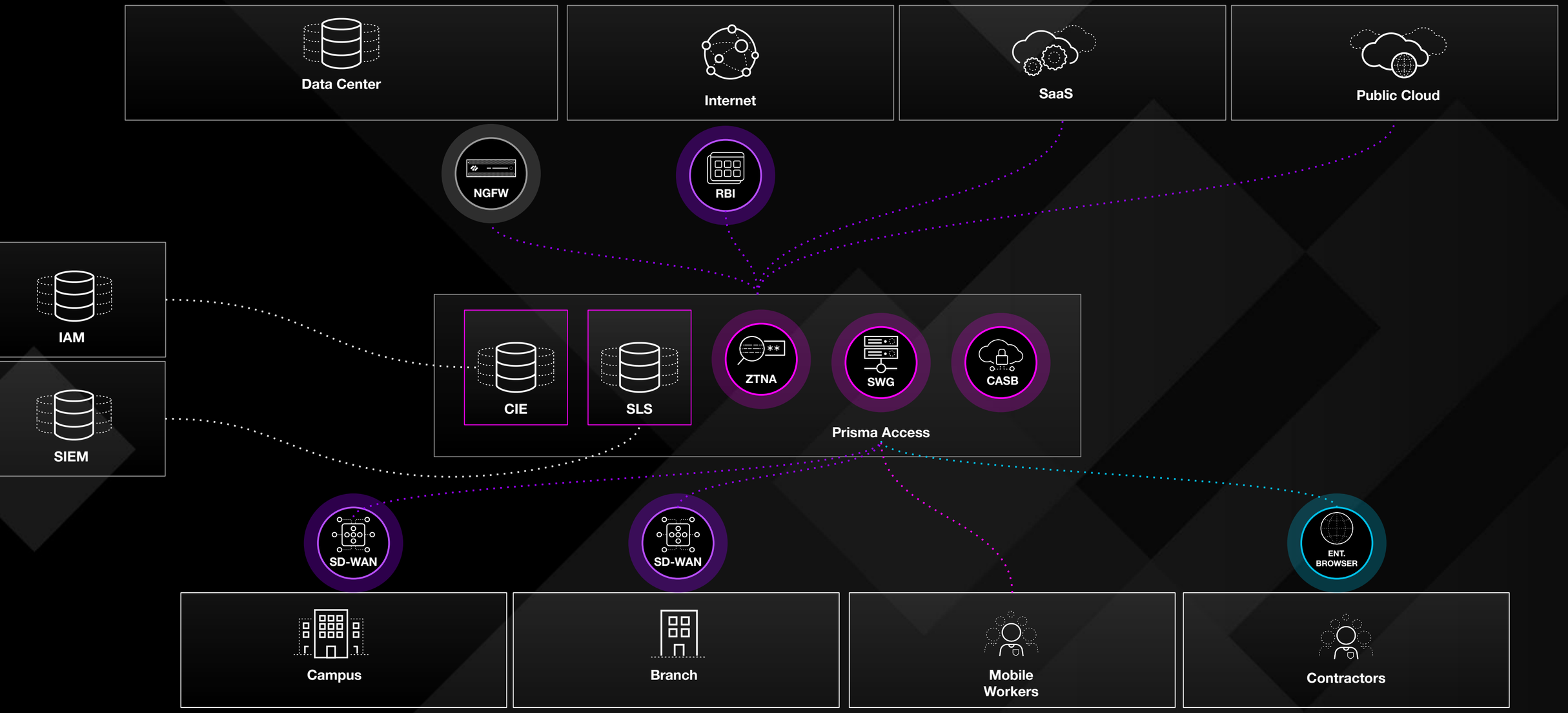


…and a Centralized Identity Engine

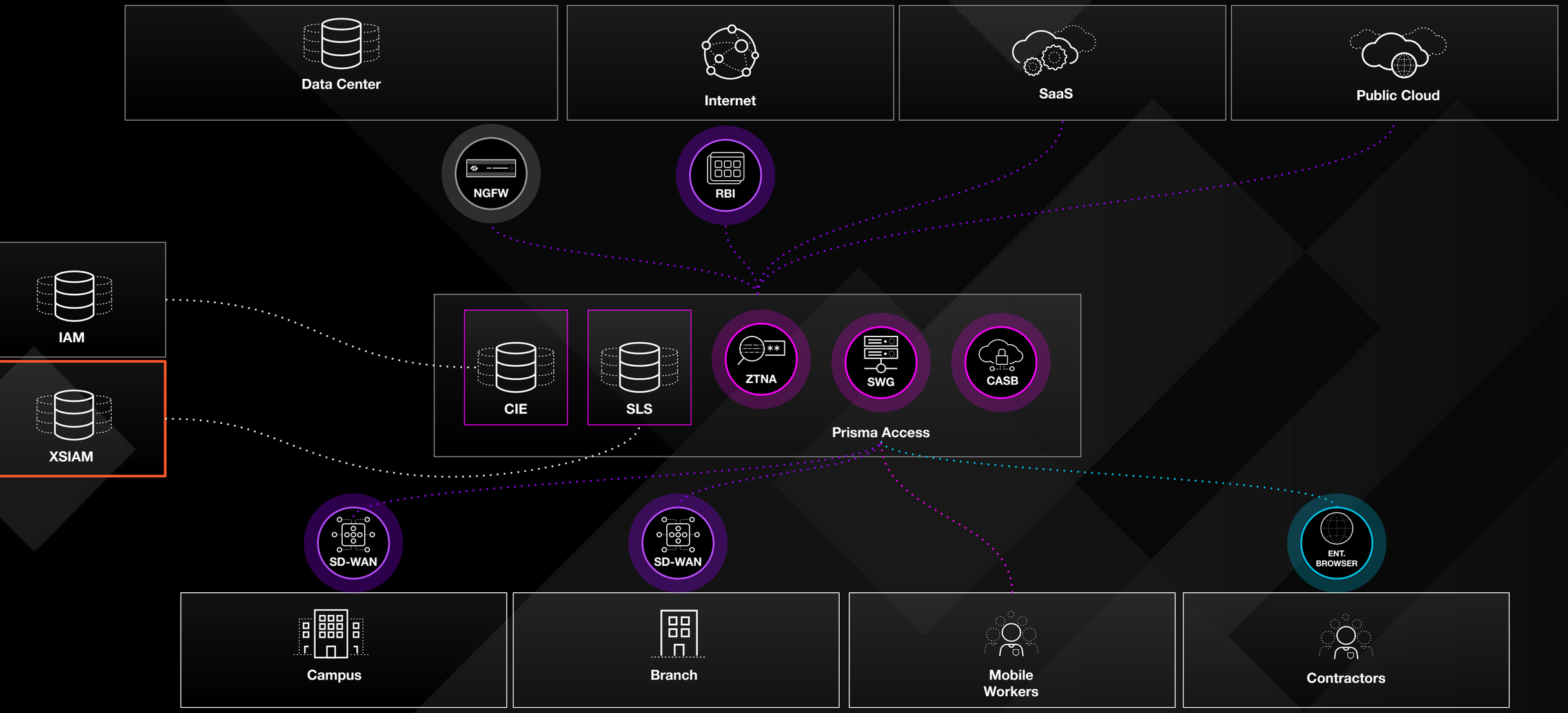


paloalto NETWORKS | STRATA

Simplifying Identity and logging consumption

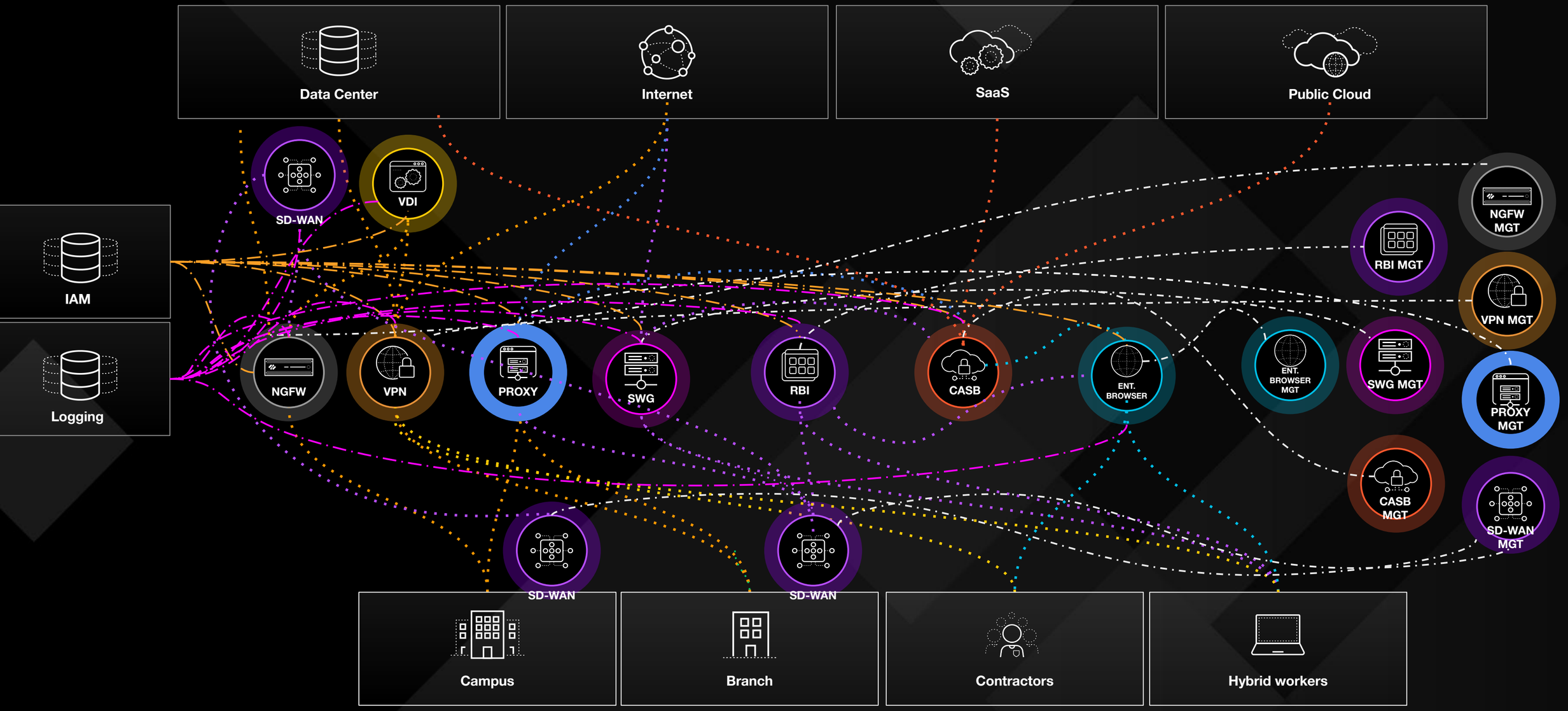


Improve the SIEM and extend the Strata Platform with XSIAM



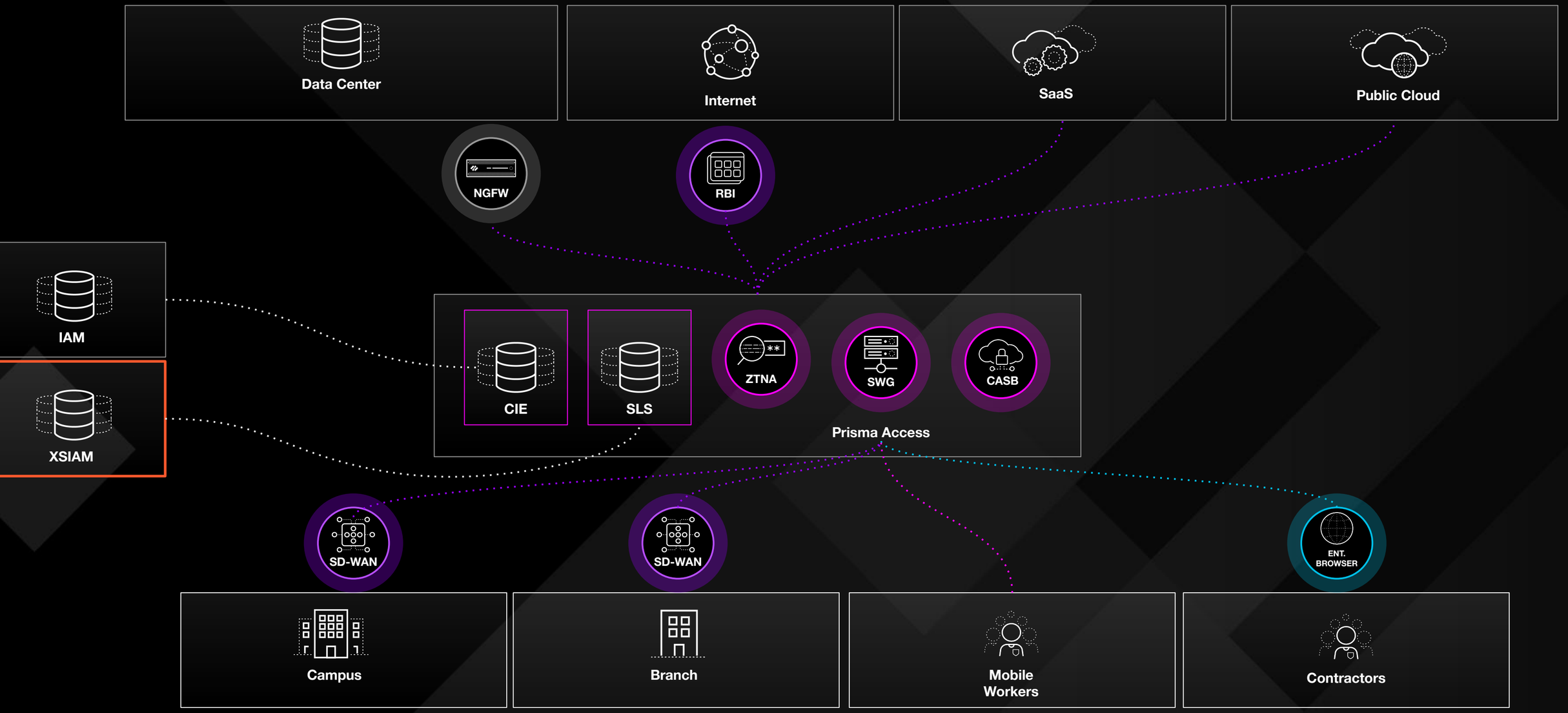
paloalto NETWORKS | STRATA

Strata can Transform the Netsec Architecture from messy



paloalto NETWORKS | STRATA

…to Simple while improving Security Posture as part of a Zero Trust Journey



Enable the path to Zero Trust with Automation and AI

paloalto NETWORKS

Understanding and Securing AI Usage

Secure AI usage requires specific visibility and controls (should be iterative to reduce risk)

Establish visibility into AI activity
Leverage endpoint data with Prisma SASE, network data with NGFW and cloud data with Prisma Cloud

Refine Infosec policy
Establish appropriate usage of sanctioned tools/vendors

Reduce the exposure
Select a subset of 3rd party LLM SaaS/PaaS providers and bind them with commercial agreements to ensure your data/IP isn't stored or utilized

Establish controls
Limit and monitor usage to sanctioned tools/vendors with NGFW, Prisma SASE and Prisma Cloud

Implement SOC monitoring
Establish playbooks to automate incident remediation with Cortex XSOAR and XSIAM

Thank You

APPENDIX

SIMPLIFY SECURITY WITH BEST OF BREED PLATFORMS

SUB-CATEGORY	NETWORK SECURITY PLATFORM
Firewall	Network Security Platform
Intrusion Detection	
URL Filtering	
Sandbox Detection	
DNS Security	
IoT Security	
Data Loss Prevention	
Cloud Access Security Broker	
Posture and Health Management	
Remote Access for Users	
SWG	
SD-WAN	

SUB-CATEGORY	CLOUD SECURITY PLATFORM
Cloud Security Posture Management	Prisma Cloud
Cloud Workload Protection	
Identity & Access Management	
Code Security	
Web Application / API Security	

SUB-CATEGORY	MODERN SOC PLATFORM
Security Information & Event Management	Cortex XSIAM
Endpoint + EDR	
NTA / UEBA	
SOAR	
Attack Surface Management	

