Zero Trust and Identity as a Service (IDaaS)

Nya Alison Murray
CEO Trac-Car

Foreword

"Identity-related attacks are a critical threat vector in cloud, making proper identity and access management the fundamental backbone of security across domains in a highly virtualized technology stack." Cloud Security Threat Report 2019 – Symantec

"Customers' personally identifiable information (PII) was the most frequently compromised type of record, and the costliest, in the data breaches studied. " Cost of a Data Breach Report 2020 – IBM Security

According to Forrester, there are three main concepts of Zero Trust:

1. Ensure that all resources are securely accessed no matter who creates the traffic or from where it originates
2. A least privilege strategy that enforces access control to eliminate temptation to access restricted resources.
3. Continuously logging and monitoring user traffic for signs of suspicious activity.

Security Landscape

Security Landscape 2020

Over 500 organizations with a data breach - average cost $3.86M USD

Main causes

1. Compromised credentials
2. Platform vulnerabilities

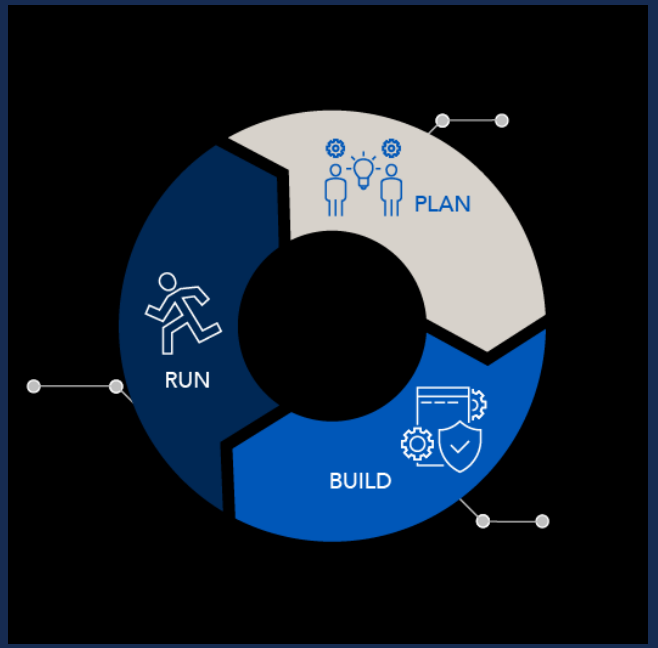
80% involve customers' Personally Identifiable Information (PII)

Complex Security Environment - cloud migration, increasing use of DevOps and infrastructure build automation, increase in remote working.

Increasing security incident responses reduces the costs of data breaches

Focus has to be on protecting the identity credentials and implementation of best practice network, platform and application security

Reference Architecture



Reference Architecture

Technical Foundation for Defence-in-Depth

- Application Security Management
- Security Logging and Monitoring
- Deployment Management
- Service Operations Monitoring
- Application Platform Technical Security Architecture

Security Principles

- Network Segmentation
- Anti-DDoS
- API Authentication and Authorization
- Encryption and Secure Key Management
- Software Defined Perimeter

Identity Management

Identity Management - Policy

Policy based access to resources combined with Identity Management/Role Based Access Control is common for all cloud services across all Cloud Service Providers (CSPs).

Users added into groups with permission sets

Resource privileges the role, user, group, application or service scope of the access policy.

Multi Factor Authentication - this ensures that there is an additional level of security mechanism for user validation as well as the default authentication method.

Privileged Identity Management - can be configured to control and monitor privileged users e.g. administrators and developers with resource fine-grained access control to view, modify, copy etc.

Monitoring – CSP logging and monitoring can be configured to view and report on access to protected resources

Identity Management - New Best Practice

Historically, UserID and Password have been replaced by tokens and MFA at the application layer, and VPNs and TLS (HTTPS) for network connections.

Basic vulnerabilities in every connection protocol TCP/IP, TLS, SSL and IPSec VPNs.

Basic flaws in every authentication mechanism - including SAML, OAuth 2, JWT, biometrics even if supported by multi-factor authentication.

Encryption is important, PKI certificates (min 2048 bit private key), symmetric ephemeral keys (AES min blocksize 256) HMAC hash algorithms (min SHA2 (SHA256))

Emerging pattern is that any complex handshake at connection can be exploited by expert hacker organisations.

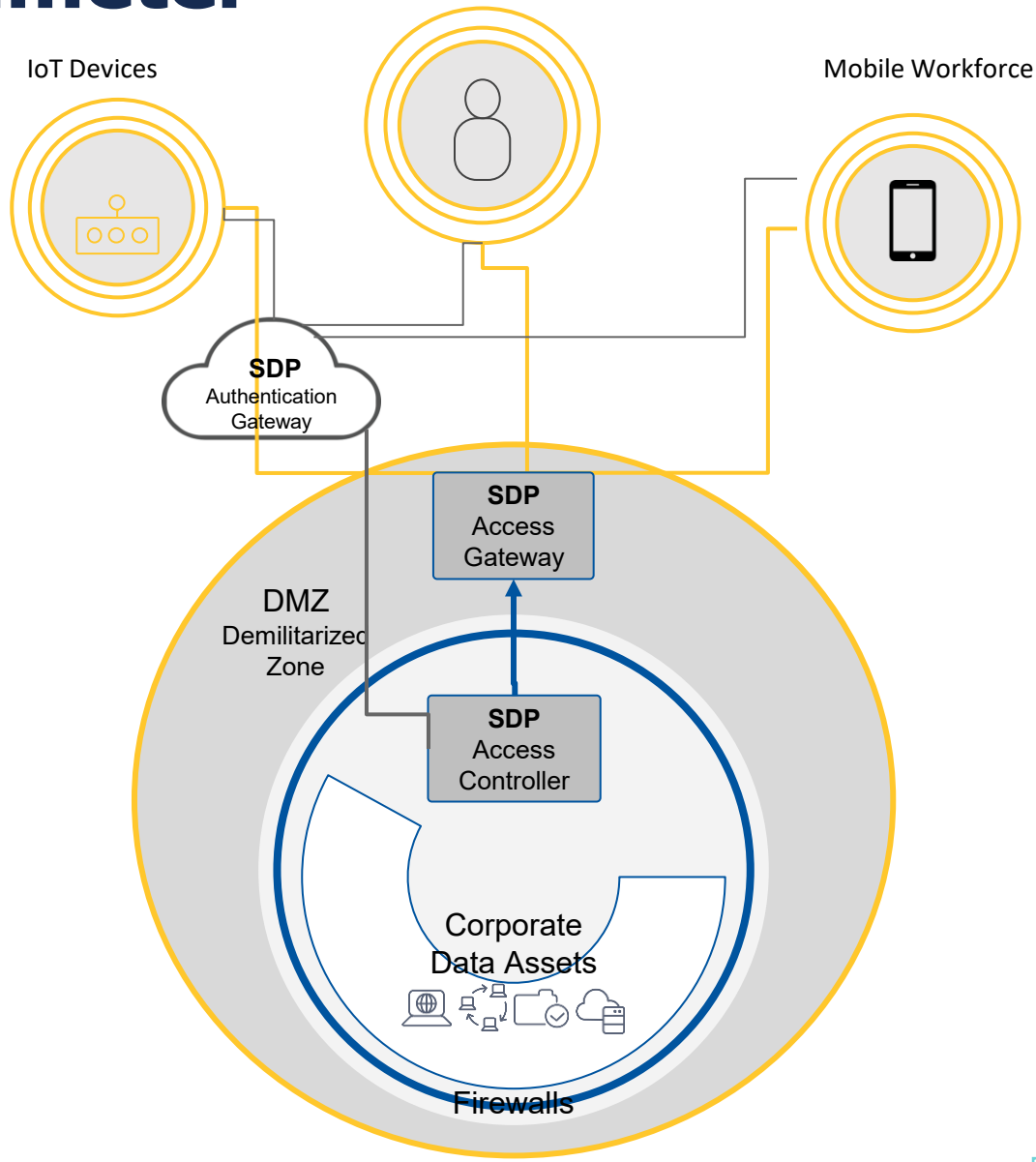
Conclusion: Identity Management and Zero Trust network connectivity security automation are both critical factors to ensure overcome inherent defence weaknesses in identity management and application, platform and infrastructure deployments.

Software Defined Perimeter

What is Software Defined Perimeter

Software Defined Perimeter is a specification produced by the SDP Working Group under the auspices of the Cloud Security Alliance. The major objective is authentication at the network layer, prior to any access.

Separate authentication flow from access flow
Allow only application level access
Remove users from the network
Reduce malware propagation
Support any user type (managed and unmanaged)



Secure Network

Secure Networking

Document the design for secure networking in advance. Cloud Application Platform network segmentation facilitates private IP address space for deployed Virtual Machines and other Cloud Application Platform services that support private IP addresses in the Cloud Application Platform

Secure Design Principles

Secure network segment – depending on virtual network and subnet function. Consider isolation of subnets for data privacy

Judicious use of network security groups – design for convenience as well as security, or people will break the rules to deploy an application under time pressure

Analyse the security impliciations and design site-to-site network connectivity requirements to make appropriate choices with security front and center

Test extensively for inbound/outbound flows for applications, platform services, databases, data stores , network connections including network level authentication

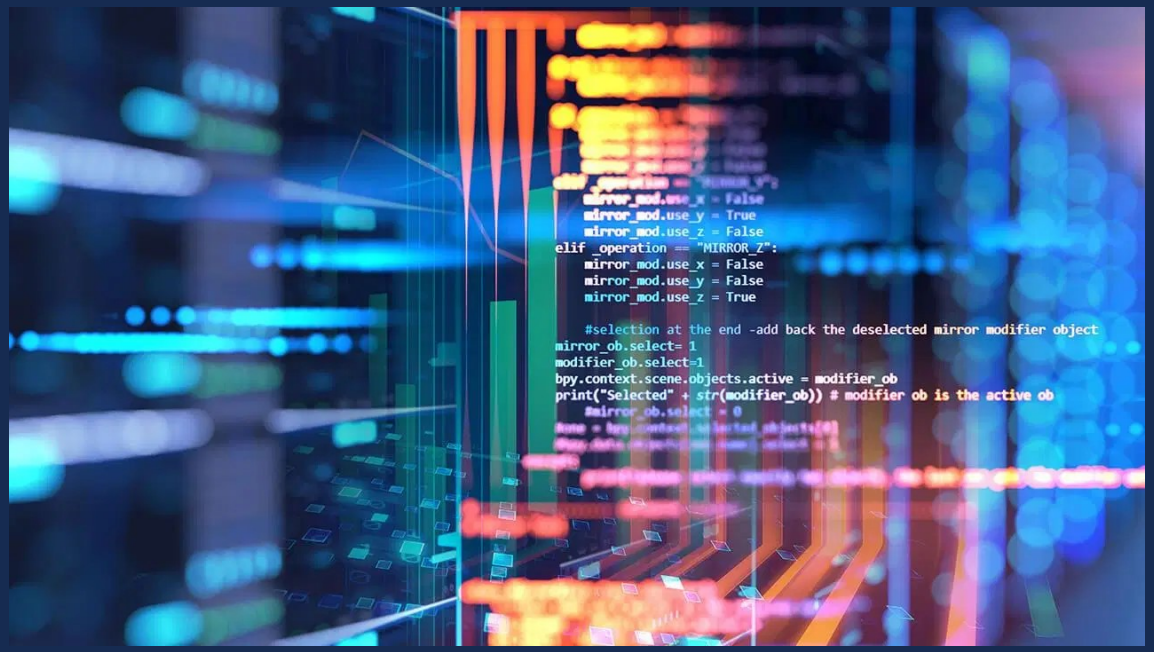
High Availability

High Availability is Security

Part of the security of the Cloud Application Platform is high availability. A highly available application absorbs fluctuations in availability, load, and temporary failures in the dependent services and hardware.

1. VMs - ensure capacity and high availability even in case of partial VM outage occurring due to maintenance tasks.
2. PaaS services - ensure high availability of all the PaaS services, e.g. a primary and a replica, automatic failover
3. Database – design to connect to secondary instance in case of failure in primary instance
4. Environments - Provide a detailed sizing document for IaaS and Paas components in production environment. Ensure DR and Test are adequate
5. Storage – encryption and redundancy. Backup data across regions for business continuity for virtual machine disks, blob/bucket storage, storage for logs and storage for backup data.

Logging and Monitoring



Logging and Monitoring

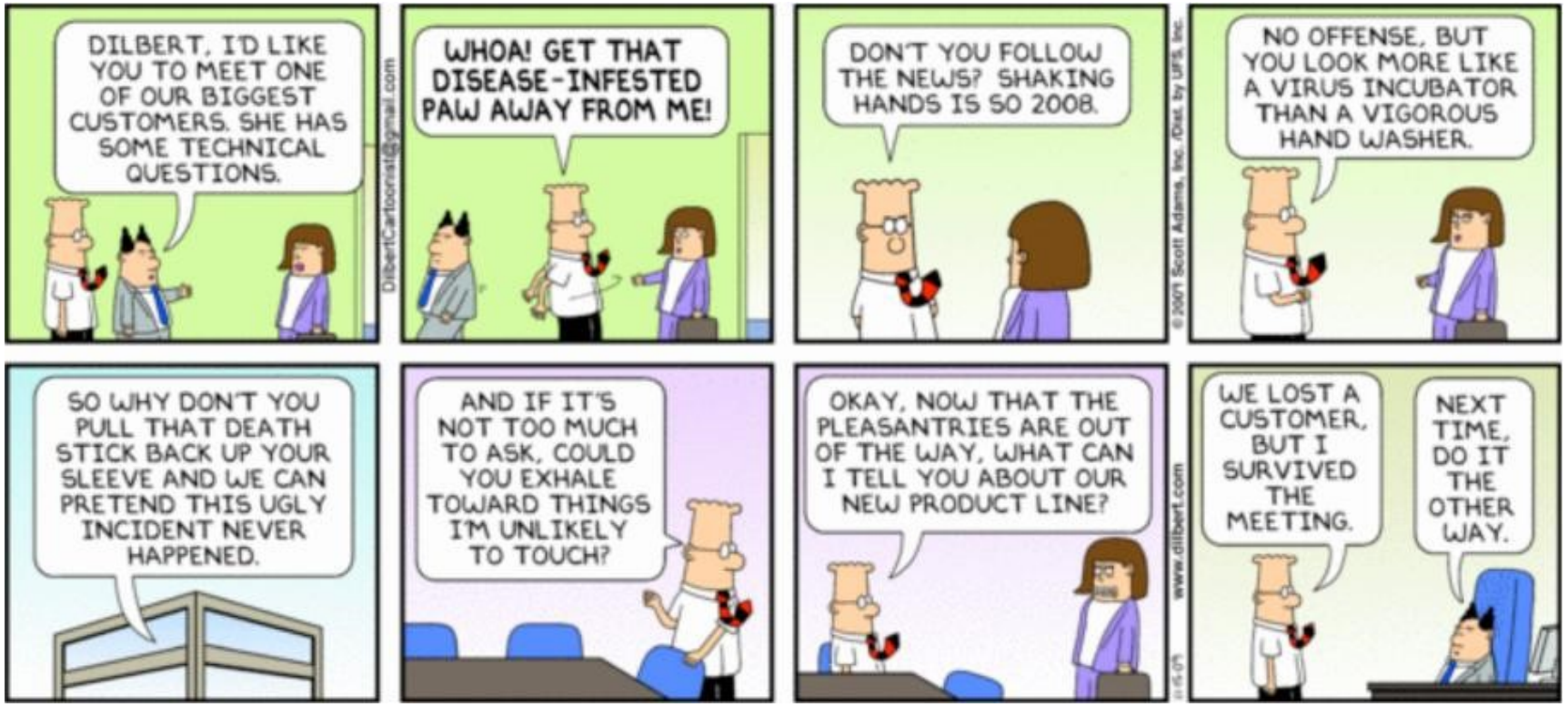
Watch everything, trust nothing. Monitoring solutions for both infrastructure and application security & performance monitoring requirements. Document which monitoring tools will be used for a specific monitoring requirement.

1. Compliance - ISO 27001, PCI-DSS, GDPR, Minimum Control Standards
2. Data Retention - xGB depending on the deployment size for x years
3. Encryption – Provide metrics for data in transit, in process and at rest – e.g. TLS 1.3 encryption for data in transit and strong symmetric/asymmetric encryption for transaction data
4. Infrastructure metrics - Host metrics (host details, RAM/CPU usage, hard disk IO usage, network activity, and database transactions) and various application runtime metrics
5. Endpoint access monitoring – cloud account and event history, and analytics of end user access - machine learning and security analytics.
6. Take advantage of CSP logs which are often best practice – IAM/RBAC, WAF, certificate, key vault logging, gateway, application and database access logs.

Disaster Recovery

Disaster Recovery Takes Planning

Business Continuity depends on Disaster Recovery! Region selection is based on business user location, the disaster region is chosen as the nearest. Provide a rationale for choosing Active or Passive DR configuration e.g. is primarily due to increased complexity or latency of stateful services.
With COVID19 remote working from home is the new reality.



Zero Trust and Identity as a Service (IDaaS)

Nya Alison Murray
CEO Trac-Car
nya.murray@trac-car.com