Identity Services and Network Cyber Security

Trac-Car Proprietary Ltd
International House,
64 Nile Street
London N1 7SR
United Kingdom

Situation Analysis

“While Software-as-a-Service (SaaS) application usage is proliferating, and workloads are increasingly migrating to IaaS platforms like AWS and Azure, on-premises applications, storage, and private clouds persist. The resulting hybrid IT environment is challenging existing security paradigms, creating complexity, and leaving organisations scrambling to keep up.” Symantec Cloud Threat Security Report 2019

The current SIEM/WAF/Endpoint Prevention and Detection Cyber Security products and offerings are struggling to keep up with threat actors and data breaches – IBM Cost of a Data Breach Report 2020

Trac-Car’s Identity as-a-Service product, Verviam, uses Amazon Web Services to provide a Cyber Security Monitoring Solution that adds a virtual Zero Trust data privacy protection at the OSI Network Layer for digital resource protection. (Most cyber security solutions are applied at the application layer where state sponsored threat actors are finding it easy to exploit vulnerabilities).

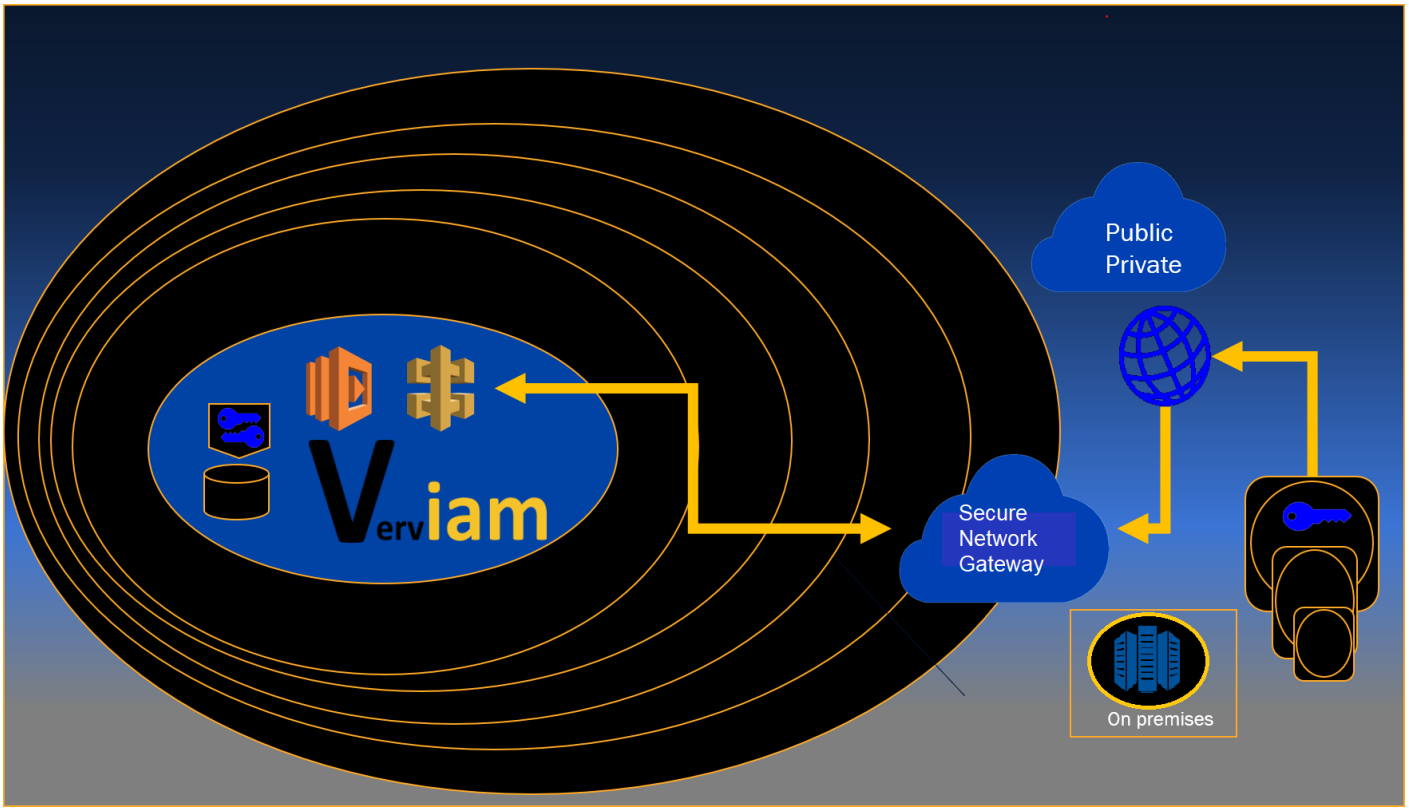

Figure 2: Security Architecture Deployment Overview

This proposal offers identity services, to allow or deny access through to the organisation's network, prior to TCP handshake and TLS certificate termination and the exposure of any application layer functions. The reason for this approach is that it represents an advance in positive threat prevention capability, before exposing an organisation's protected resources.

After authentication, inside a highly secured AWS network perimeter, requests are sent to a secured network gateway able to forward authenticated requests. Authorisation scopes are either configured directly for access to applications, or federated with existing identity management systems permissions.

The secured network gateway, with token based authentication, incurs only milliseconds of latency to existing response times, and takes best advantage of blazing speed, autoscaling and a huge range of inbuilt security measures.

Resources

Overview of the Cyber Security Identity and Network Security Gateway

Overview of the Cyber Security Logging and Monitoring

Presentation to Cloud Security Alliance APAC 2020

Cloud Infrastructure Security Architecture White Paper

Cloud Security Alliance Software Defined Perimeter (SDN) and Zero Trust

Cyber Security Objectives

The major objective is to provide a clear transition from the existing security methods, providing a new capability comprising

1. Network layer allow or deny access control incorporating authentication
2. Federated single sign-on of end users with no exposure of private data or credentials
3. Access monitoring dashboards, alerts and alarms
4. WAF/Endpoint security analytics and dashboards able to integrate existing logging and monitoring

The solution adds an SDN IDaaS (Identity as a Service with Software Defined Networking Access Control) as a gateway to existing systems by providing a network layer allow/deny security posture, with real-time access logs, centralised threat intelligence and full log WAF security analytics dashboards.

This approach requires a phased, prioritised rollout, adding protection to existing systems. Organisation specific AI (Artificial Intelligence) machine learning models can be developed, based on aggregated organisation data sources to enhance attack prevention, in collaboration with internal and external stakeholders.

To address the requirements of current escalating threats, it is advisable

1. to add SDN Gateways to high priority systems first
2. to heighten monitoring such as additional anti-DDoS protection
3. to add additional thresholds on existing alerts and alarms, and defining new alerts and alarms for early detection of possible threats.

Technology Approach

The technology approach to existing organisation identity and network security is as follows:

1. Addition of a software defined Network Security Gateway in front of all end user access, providing allow/deny authentication prior to allowing access to protected resources on premises or in the cloud.
2. Identity federation, with authentication and field level encryption, perimeter protected encrypted tokens with no exposed protected or private data.
3. Real-time access monitoring dashboards, building custom AI models to analyse and report on logs, integrated with internal security logs to identify security anomalies, vulnerabilities and potential threats.

The technology works because

1. All access is protected by identity authentication, and network access control prior to allowing access to protected resources in an organisation's DMZs.
2. The Network Security Gateway remains shut until positive identification via token authentication of the end user and the authorisation scope of the user's destination URI.

3. An encrypted identifier with signed JWT(JSON Web Token) is exchanged for the actual organisation identity credential (e.g. AD group, userID/Password, access token) behind a highly secure, highly protected infrastructure perimeter.

4. After a request is authenticated, the Software Defined Network Security Gateway allows or denies, end user access to permitted systems, monitored and managed by existing networking.

5. All end user requests for access are first examined at the network layer outside of the organisation DMZ. Network access and authentication requests, both successful and unsuccessful, are logged and monitored.

6. Both real time and aggregated logs can be accessed and viewed for potential incident response on a monitoring dashboard.

7. Logs are stored for integration with existing logging and monitoring capabilities.

8. The access monitoring dashboards can be viewed in parallel with existing security monitoring capabilities to provide a more comprehensive picture of access to protected resources.

There are a number of advantages to this approach.

The technology can be rolled out incrementally, utilising existing security endpoint detection and prevention measures during phased transition. Some of the critical elements on offer that adds value to existing cyber security measures are

1. Allow or deny access prior to any protected resources being exposed.

2. Security compliance with industry standards e.g. ISO 270001, PCI-DSS, GDPR, benchmarks etc

3. Well documented user guidance

4. Strong transition strategy based on stakeholder engagement to develop a Transition Plan

Logging and Monitoring

Log data can be integrated with existing log data collections. The monitoring capability can be allied with internal security monitoring systems.

Over time, trained event models can be identified and applied with machine learning technology to provide analysis of end user access by people, network connections, applications and devices.

Anomaly detection can be augmented from databases containing vulnerability alerts and threat signatures to anticipate and prevent existing attacks. Anomalous behaviour response can be designed to counter Zero Day threats.

Solution Overview

The Identity-as-a-Service with Software Defined Network Security Gateway solution works with end users routed through consolidated secure internet gateways, or directly to internal network security firewalls and gateways. The allow or deny posture prior to exposure of protected resources, including sensitive, classified, private data and credentials, means that end user communication can be safely routed over the public internet. For example, remote workers, contractors, suppliers and trusted third parties can use public internet access to organisation functionality.

Verviam IDaaS allows for definition of end users as people, devices, applications, services or network connections. The primary access for all end users is a JWT token credential that contains an encrypted identifier (no private identity or endpoint data) to the target system. The encrypted identifier can be federated with existing identity systems, or newly configured as a complete identity management system, as required by the organisation use case.

Where existing access is via federation with an Identity Management System, such as Active Directory with privileges mapped to a User Group, the end user/endpoint token can be validated and exchanged for the User Group and forwarded by the Network Security Gateway to the AD endpoint.

Security Features

The following features are important advances over existing cyber security measures:

1. The JWT token can be exchanged for configured credentials that are recognized by the organisation's existing systems. This configuration can either be via a console or via a scripted automated integration.
2. Authentication has inbuilt protection against token replay. Tokens can be invalidated by rotating the RSA 2048 public/private keypair either on demand or to a schedule, e.g. daily or even hourly if required.
3. All end user access is logged and monitored for network access as well as authentication.
4. A dedicated logging and monitoring capability provides dashboard reports over time, with source and destination, and access success or failure. Events can be aggregated and monitored for anomalies with AI routines.
5. Logs can be aggregated and analysed with data sources from existing monitoring solutions.

6. No private data or credentials are ever exposed over the internet. Only the person entering private data sees clear text. The identity token has an encrypted identifier, and the validation is based on decryption and expiry.

7. Access to organisation resources can be routed through the Network Security Gateway. This can be delivered incrementally based on priorities, in line with industry best practice (around 80% of incursions occur at the network layer).

8. Cyber security monitoring is based on an AWS monitoring capability, providing dashboards, and reporting on alerts and alarms from advanced features such as CloudWatch, WAF, GuardDuty. Audit capability is available with CloudTrail.

The basic capability requires configuration only, and is provided out of the box. Configuration requires collaboration amongst organisation business and technical stakeholders to determine risk threshold metrics.

As an added capability, access to reports, alerts and alarms are available from dashboards in real-time. More advanced analytics can be configured by adding a full logging analytics capability. Reports can be shared, and power users can provide self-service. The technology forwards standard Verviam logging, plus any other existing organisation log sources, integrated and aggregated to AWS Athena/QuickSight operational intelligence tools that not only provide analytics, but also machine learning algorithms.

AI/ML models can be developed in collaboration with personnel, based on their subject matter expertise on types of known risk exposure and the tolerated risk profile for any given situation.

Solution Architecture artefacts can be produced during the initial configuration phase, and provided to business and technical stakeholders.

Business Benefits

The proposal offers a simplified approach to protecting and defending organisation information technology systems and resources, and most importantly to provide protection for information and data, in transit, in process and in storage.

This is achieved by allowing/denying access at the network layer prior to any exposure of resources.

Benefits include:

1. The solution adds a complete layer of security on existing ICT functional capability without modification, designed to augment existing security practices, endpoint protection and detection, logging and monitoring services and data.

2. No exposure of PII (Personally Identifiable Information) or private data during authentication, either internal personnel or public data. Authentication can encompass identity federation.

3. Single Sign-On (SSO) can be configured from a workspace dashboard, or integrated with existing CRM, CMS, portal or Identity Federation system.

4. Authentication, secure networking, and identity federation can be added in front of ALL applications/services/systems, incrementally over time in view of business priority.

5. Organisation networks are closed by default. No open networks or internal applications are exposed to remote employees, customers, business partners, third party vendors, mobile devices, and connected devices without authentication prior to network access.

6. Currently SIEM/WAF/Endpoint Protection and Detection systems are proliferating, with limited correlation and analysis of the findings from aggregated log monitoring. With the network layer SDN IDaaS monitoring solution, the logs and analytics can be consolidated and centralised.

7. Accessible logging dashboards, integrating relevant data sets, are configurable. This capability is the basis for developing specific data analysis and AI models to determine potential vulnerabilities, and to detect anomalies

8. Security SMEs can collaborate on standard monitoring dashboards and can easily configure new dashboards for deeper analysis.

Product Information

Trac-Car is a Security Architecture Consultancy with an international presence (Australia, UK, Switzerland and Norway) providing

1. Security Architecture, Design, Development and Deployment Consultancy for Software Defined Perimeter and Identity Management as a Service (IDaaS) applications.
2. Network, Identity Management and Federation, Authentication and Authorization security for cloud and on premises applications.
3. Cloud threat and vulnerability cyber intelligence and zero trust perimeter security reporting. Enterprise cloud technology migration roadmaps, development, deployment and operations monitoring.

Verviam IDaaS

Verviam Identity as a Service is cloud native identity management for internet users, devices and applications, able to federate and integrate with enterprise Identity Management and Federation Systems, integrating with Network Security. Authentication and authorisation services provide data privacy and protection for access to systems over the public internet with encrypted credentials.

Organisations can choose access requests forwarded as a signed JWT token, secret credentials, or a direct connection string, either encrypted or unencrypted in accord with security requirements. Decryption algorithms are available for use prior to presentation at organisation request endpoints.

Secure Networking

Verviam can integrate with any secure network gateway, either by routing configuration, or by the development of routing adaptors to existing organisation network gateways. Verviam uses AWS secure network gateways to forward requests to organisation network gateways using the HTTPS protocol over TCP/IP in standard REST (representational state transfer) format.

Monitoring Dashboards and Analytics

AWS CloudWatch is a monitoring and observability service, providing data and actionable insights to monitor access to applications. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing dashboard displays, and alerts/alarms notifications.

WAF web application firewalls monitor web exposed APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF provides security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic from known bad sources and sites.

To develop AI models and apply machine learning, logs can be forwarded to AWS Athena/QuickSight technology where they can be analysed with internal data sources, e.g. integrated with SIEM data from existing security log technology. QuickSight is a cloud-scale business intelligence (BI) service with easy-to-use interface combining data from many different sources. QuickSight can include AWS log data, third-party log data, big data, spreadsheet data, SaaS data, B2B data, and other sources into dashboards containing different data series and graphs.

Pricing

Human Resources

Trac-Car works collaboratively with internal and external business and technology stakeholders, e.g. architects, security SMEs, and developer/ operations team members, as well as business owners and program management.

Responsibilities for consultancy services include the following specific configuration, based on the priorities for system rollout

1. Configure technology to customise Trac-Car's developed solutions with organisation applications.
2. Configure and/or automate provisioning of AWS cloud-based infrastructure and application deployment/configuration to organisation control standards.
3. Collaborate with internal and external stakeholders on IAM federation strategy.
4. Identify, develop, implement and improve monitoring dashboards and configure logging ETL, analytic and AI log integration dashboards
5. Troubleshoot and resolve issues in all environments through proven detail-oriented analysis in root cause scenarios and technical deep dives
6. Contribute to team efforts to maintain processes and tools for infrastructure, monitoring and operations with clear documentation

Available resources include:

Cloud Security Architect/Engineer resources, available on and off site as required.

Senior Cloud Cyber Security Solution Architecture resources available as required, for example to troubleshoot difficulties, on an ad hoc basis, on and off site as required.

In the event of a data breach, support to Incident Response personnel is available pro rata per normal business hours and additional hours. 24 hour incident support available on site as required.

Prices available on application.

Network, Hosting, Platform, Software Infrastructure

Pricing is based on a combination of infrastructure configuration and metering of authentication requests, depending on the customisation required.

A typical configuration comprises reporting and dashboard customisation for integration and customisation of logging and monitoring with existing endpoint detection and prevention systems, customisation with existing identity management systems, and integration with end user deployments.

The base price, with no customisation, and configuration performed by organisation personnel, is 0.01 USD per login, once the technology is deployed.

A 60 day trial for one end user endpoint is available from Verviam.

Transition Plan

Transformation and Transition: By determining maturity—in terms of vision, steering, culture, people, processes, and technology—organisations can establish an architecture baseline and create a roadmap for improving the security of service cost effectiveness and lifecycle.

The approach involves strategic planning at the enterprise level, while maintaining the flexibility to address immediate tactical requirements.

This activity establishes expectations in terms of organisation stakeholder engagement to develop a program framework. The objective is to move incrementally from current technology to target technology. Identification of technology adaptation required to meet compliance and governance requirements, for example for audit trails and accountability, is part of the transition planning outcomes:

Architecture and Design

The basis for any integration existing developments is an architecture process leading to a transition plan. Any customisation for integration implementation and deployment is based on a solution architecture, developed in collaboration with organisation personnel, agreed and provided as part of stakeholder engagement. The methodology includes the following artefacts to be shared with business and technology stakeholders.

1. Business Architecture Context (BAC) – Provides an overview of the business context and requirements. It also includes a high-level service design.
2. Architecture and Design Assessment (ADA) – Provides an analysis of the technology context and proposed technology solution, including timeframes and recommendations.
3. Infrastructure Architecture Definition (IAD) – Defines the overall technical infrastructure, implementation to guide and inform delivery, and support ongoing maintenance.

Goals and Objectives

It is critical to schedule workshops for stakeholders to agree and formalise the following goals and objectives:

1. Define business and technology goals and objectives for incremental technology changes and improvements
2. Define automated security monitoring in view of current tools and technologies and target technology requirements
3. Stakeholder engagement with business and technology SMEs, determine delivery expectations, and clarify roles and responsibilities
4. Develop review mechanism including continuous feedback
5. Determine value proposition in terms of additional/retained/upgraded/replacement tools and technologies, team culture and working practices
6. Document transition approach, guidelines and references

People and Processes

Stakeholder engagement workshops for technology and business personnel is required to

1. Determine system access monitoring priorities and evaluation KPIs
2. Determine acceptance criteria and provide information about delivery release practices and protocols.
3. Determine value propositions for integration with existing retained/upgraded tools and technologies, reviewing current working practices.
4. Document scope and assign delivery activities to internal and external stakeholders
5. Establish stakeholders and SMEs participation

6. Develop a program framework to move incrementally from current technology stack to target technology

7. Document technology adaptation required to comply with governance requirements for audit trails and accountability

Delivery Governance

Prior to program commencement, it is essential to determine the success metrics for configuration and deployment of SDN/IDaaS capability, and the deployment priority of existing systems.

Determination and specification of security testing and quality control measures is also essential, including identity management audit and access controls. A prerequisite for delivery planning is to close the loop between ICT operations and business stakeholders to ensure a collaborative review and endorsement of priorities and schedule for the addition of IDaaS and SDN gateways.

Activities include the following:

1. Determine a safe, incremental pathway towards continuous delivery

2. Provide templates for feedback and review by business and technology stakeholders for improvements in security monitoring

3. Determine additional activities for integration of security monitoring.

4. Determine compliance measures for legislative regulations and internal security governance requirements

An initial pilot is the recommended pathway to adopting this comprehensive cyber security defence technology. A six week engagement can produce a roadmap to scope the delivery, the timeframe and resourcing, and inform and enable a clear path to technology knowledge transfer to internal teams.