Cisco Secure Access

Next Generation Third-Party Landing Zone & Managed Secure Access Solution

February 6th, 2026



Table of Contents

1. Disclaimer

1.1 Disclaimer

Thank you for the opportunity to submit this non-binding (other than pricing for now available products listed in formal quotes), proprietary, and confidential proposal for your consideration.

The objective of this document is to outline the details behind the Secure Access Landing Page and Managed Service solution, highlighting strategic delivery options from **Cisco Systems ("Cisco"), Gruve.ai ("Gruve"), and Presidio, Inc. ("Presidio")**. This document details the various levels of service, technology stacks, and Service Level Agreements (SLAs) designed specifically for **CVS Health Corporation ("the customer" or "customer")**.

The solution described herein provides secure network connectivity to internal applications and systems for CVS partners ("partner" or "partners") through a comprehensive, multi-tenant, and self-service user experience. This proposal includes **flexible implementation paths**—including an accelerated "As-a-Service" model and a bespoke development roadmap—to ensure alignment with CVS Health's operational and strategic requirements.

This document is the base design and strategic roadmap on which this managed service is based. The information contained within can be used for pre-sales, deployment, and operational phases when working with prospects and customers.

The audience that can leverage this document includes:

- Managed Services Product Management Team
- Managed Services Operations Team
- IT Operations and Strategic Procurement Teams
- Security Operations Team

2. Executive Summary

2.1 CVS Health Third-Party Landing Zone & Managed Service

Vision

Cisco, in strategic partnership with **Gruve.ai** (a Cisco Investments portfolio company), proposes a turnkey, automated **Third-Party Landing Zone (TPLZ)** for CVS Health. This solution is designed to transform CVS's current manual, ticket-heavy onboarding process into a high-velocity, secure, and outcome-based "As-a-Service" model. By integrating **Cisco Secure Access (SSE)** with the **SecurityHub365** orchestration portal, CVS will eliminate technical debt, reduce operational overhead, and gain unprecedented visibility into partner connectivity.

The Solution: A Unified Architecture

Our proposal centers on three core pillars:

1) **The Intelligent Frontend (Powered by Gruve.ai/SecurityHub365)**: A multi-tenant, self-service portal that provides CVS and its partners with a "wizard-driven" onboarding experience. This portal replaces the current 15-ticket manual process with automated workflows for IPsec tunnel creation, identity integration, and policy enforcement.
2) **The Secure Backbone (Cisco Secure Access)**: A cloud-native SSE platform that handles session splicing, SSL decryption, and bidirectional NAT. This ensures that third-party traffic is isolated, inspected, and routed without exposing CVS's internal network topology.
3) **24/7 Managed Excellence (Cisco Managed Services)**: Cisco will "quarterback" the entire environment. Our Global SOC provides 24/7 monitoring, incident response, and proactive threat hunting, ensuring that the landing zone is not just a connection point, but a fortified security perimeter.

Key Business Outcomes

- **Operational Velocity**: Reduces partner onboarding time from weeks to hours by automating the "Human-in-the-Loop" approval process via bidirectional **eBonding with CVS ServiceNow**.
- **Cost Transformation**: Shifts the burden from expensive manual labor (10+ teams) to a scalable **Consumption-Based Model**, providing CVS with clear chargeback/showback data for every partner and application.
- **Risk Mitigation**: Implements Zero Trust Network Access (ZTNA) principles, ensuring partners only access authorized applications, with all telemetry ingested into a unified SIEM for real-time detection and response.

3. Strategic Alignment

3.1 Addressing the CVS 3PLZ Core Use Cases

Cisco Secure Access is the secure connectivity engine in the proposed solution. Cisco Secure Access addresses the key CVS 3PLZ use cases with a comprehensive, cloud-delivered Security Service Edge (SSE) solution grounded in zero trust principles. Below is a high-level summary of how it supports each CVS 3PLZ use case:

1) **Secure File Transfer (SFTP, SCP, etc.) to and From Private Resources**
Cisco Secure Access provides secure, granular, application-specific access to private applications and resources through Zero Trust Network Access (ZTNA) and VPN-as-a-Service (VPNaaS). It brokers user access with least privilege principles and contextual device posture checks, ensuring secure tunnels for protocols including those used in file transfers. The solution supports client-based and clientless access, enabling secure file transfers without exposing applications or networks to unauthorized users.

2) **Secure Access to Collaboration Platforms (i.e. Office 365, eShare, Slack, etc.)**
Secure Access includes a full Secure Web Gateway (SWG) proxy and Cloud Access Security Broker (CASB) functionality that provides visibility, control, and protection for SaaS applications including collaboration platforms. It enforces granular policies, blocks risky or unsanctioned cloud apps, and optimizes performance by leveraging direct routing and global peering relationships (e.g., for Microsoft 365). AI-powered threat protection and data loss prevention (DLP) help secure data shared via these platforms.

3) **Secure Access to Private Virtual Desktop Infrastructure (VDI)**
Cisco Secure Access supports secure, zero trust access to private applications including VDI environments. It uses ZTNA to provide least privilege, context-aware access with device posture evaluation. Secure Access protects VDI sessions, hiding network details and preventing lateral movement by unauthorized users. VPNaaS also supports secure remote access to private resources like VDI.

4) **Secure Access to Private Web Applications**
Secure Access offers client-based and clientless ZTNA with granular, per-application access policies that secure private web applications. It supports SSL inspection and enforces mutual TLS (mTLS) for strong authentication and encryption. The solution hides private application network details from unauthorized users and prevents lateral attacker movement, ensuring secure, least privilege access.

5) **Secure Access to REST/SOAP APIs**
Cisco Secure Access protects API access by enforcing identity-aware, zero trust policies with strong authentication mechanisms including mTLS. It provides granular control and visibility over API traffic, integrating with identity providers and applying contextual access controls. This ensures secure, authenticated access to REST and SOAP APIs while preventing unauthorized use or data exfiltration.

6) **Automated Partner Onboarding & Legacy Migration** Integrated with the Gruve.ai orchestration portal, Cisco Secure Access addresses the critical need for high-velocity partner onboarding. By automating the creation of IPsec tunnels and providing a "Migration Factory" approach, the solution enables CVS to rapidly transition 360+ legacy tunnels from EoL hardware to a scalable, cloud-delivered architecture. This reduces the manual "Human-in-the-Loop" effort from weeks of coordination to a streamlined, wizard-driven approval process.

In summary, Cisco Secure Access provides a rich foundation to provide CVS business partners with seamless and secure access to any application or resource, regardless of protocol or location. It simplifies IT operations with a single cloud-managed console and unified policies, integrating advanced threat protection and AI-powered security to reduce risk across all CVS 3PLZ use cases.

4. Services Description

4.1 Overview

Cisco (“Cisco”) in partnership with Gruve (“Gruve”) has developed a comprehensive Secure Access Landing Page and Managed Service. This service has been created for CVS Health Corporation (“the customer” or “customer”) to provide network connectivity to specific internal application and systems for their partner (“partner” or “partners”). The Secure Access Landing Page and Managed Service is powered by Cisco’s Secure Access SSE solution, enables an organization’s SSE architecture, allowing them to provide access to specific applications for users and external networks. A multi-tenant, service portal will frontend the service and can be used to onboard users and external networks into the larger SSE network. The service managed by global Cisco partner Gruve, will be delivered by an expert IT Operations Team which provides end-to-end visibility and correlation across an organization’s security infrastructure (as supported by the service) to proactively monitor, visualize, and respond to threats and issues in real-time, helping reduce the security risk for the overall business.

The Secure Access Landing page will act as the center portal for this overall solution, integration with the various products while orchestrating both implementation and operations. Build off the SecurityHub365 platform, Gruve’s multi-tenant solution for delivering managed security services, this platform will enable onboarding, management, orchestration, and communication for this Secure Access Managed Service.

As a multi-tenant solution there will be three standard levels of access into this portal. Organization level admin access, partner level admin access, and user access. Organization level admin access enables users from the Gruve IT operations team and the customer to have a full read/write access over all users and partners onboarded into the solution. Partner level admin access can be provided to the IT teams of partners selected by the customer to be onboarded to this service. This is a self-service portal which allows the partner to manage which of their network services will be visible in the customer network and which of their users will be onboards to the service. Finally, user level access will allow for self-service of individual users from onboarded partners into the services. Users and Partners both will have the ability to open tickets a make service requests which can get routed to the Gruve Managed Service team for response.

The Secure Access Landing page will integrate directly into several systems. First it will integrate with Secure Access via the API. After collecting relevant configuration data from the customer and customers partners, the Secure Access Landing page will initiate the orchestration of the required configuration changes in Secure Access. Whether it’s the creation of a new partner, the addition of a user, or the updating of a network resource definition, the change will be orchestrated through the Secure Access Landing page. The Landing Page will also be directly integrated, bidirectionally, with the customers Information Technology Service Management System (“ITSM”). This will enable the customer open tickets in their system while having them visible via Landing Page. All new ticket requests and ticket responses made from the Landing Page will also be visible in the customers ITSM platform ensuring consistent, up-to-date, communication throughout the lifetime of the service.

The final component of this offering is the Managed Service components. Gruve in partnership with Cisco will provide a 24/7 managed service as part of this overall offering. This service will cover two main areas, management, operations, and development of the Landing Page and 24/7 monitoring and incident response services for the Secure Access environment.

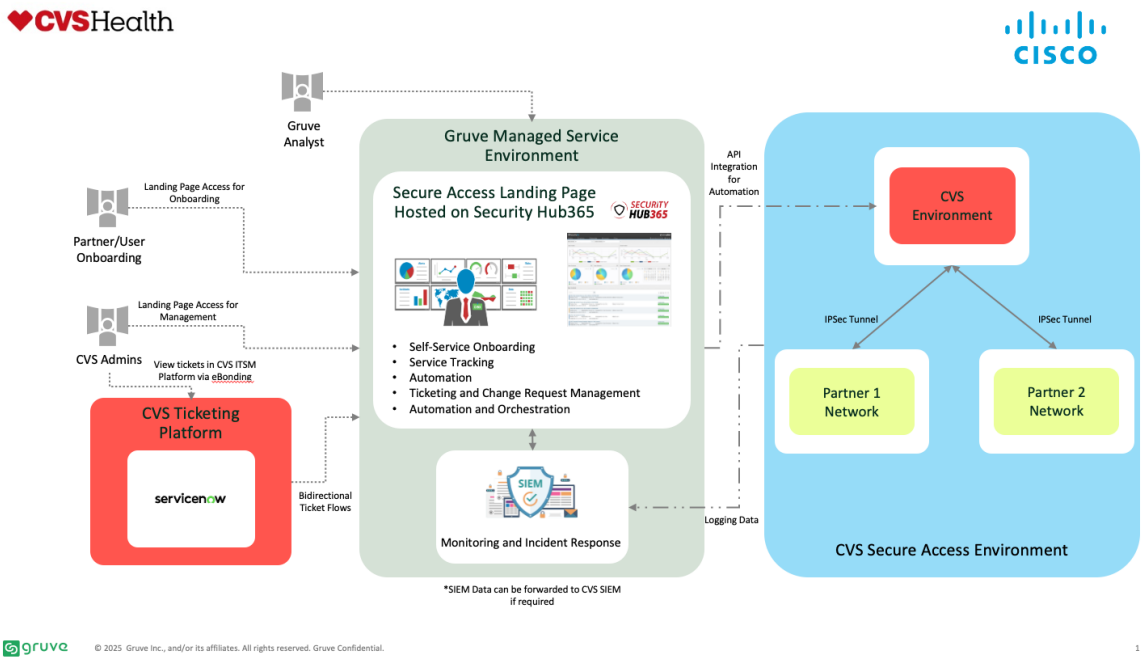
The Gruve IT operations team will monitor the availability of the portal and ensure it is running smoothly. The Gruve Platform Engineering team will work with the customer to customize the

portal to meet their requirements. This portal and all its components will be monitored, managed, and developed by the Gruve team with input from the customer.

24/7 monitoring and incident response of Secure Access will consist of ingesting data from Secure Access and other available customer security tools into a unified SOC platform, applying machine learning and analytics to quickly arrive at correlated detections. The service can take remediation actions to mitigate threats for endpoints and networks equally. This extensible solution can bring together third-party telemetry sources with underlying threat intelligence from Cisco Talos to enrich incidents with added context and asset insights.

This service, delivered by an expert IT Operations Team, reduces false positives and enhances threat detection and response through clear prioritization of alerts, providing the shortest path from detection to response. The combined approach of the Secure Access Landing Page and Managed Service powered by Cisco and delivered by Gruve's expert IT Operations Team presents a new approach that surpasses the traditional approach by shifting the focus on achieving and addressing outcomes that will help reduce the security risk for the overall business.

The technology behind this offering is provided by Cisco's Secure Access solution and the SecurityHub365 platform, which will be the foundation of the Secure Access Landing Page. This is combined with 24x7x365 monitoring and management provided by Gruve's expert IT Operations Team operating from a Security Operations Centre ("SOC").



High-Level System Architecture

4.2 Services and Packaging

The Cisco/Gruve Secure Access Landing Page and Managed Service offering is described in this document. This service includes, Cisco's SSE platform Secure Access, a landing page to manage onboarding built off SecurityHub365, and 24/7 monitoring and incident response in the customer's Secure Access network.

Cisco's Secure Access solution will be utilized by the customer to provide access to/from their network for their partners. This zero-trust solution will be the technology utilized by this service to provide the desired network access to the relevant partners. By onboarding to this solution partners will have relevant access to authorized customer applications while being able to expose, in a controlled fashion, application from their own internal network to the customer.

The Landing Page will be built using the SecurityHub365 platform as a foundation. This multi-tenant tool will enable the onboarding of partners into this service. It will allow the IT operations team and the customer to manage these partners, while enabling the partners themselves to manage their own users in a self-service fashion. SecurityHub365 at its foundation is a ticketing system, so all onboarding, management, and change requests will be tracked as tickets in the system. The Landing Page will also be integrated with the customers ITSM platform allowing them full visibility to all the tickets created and updated for this service. The customer will even be able to update tickets directly from their own internal ITSM platform.

Finally, the Gruve IT Operations team will be monitoring the Secure Access environment for the customer on a 24/7 basis. The team will monitor for incidents, create tickets when incidents are found, and perform the relevant remediation action when able. The team will also provide incident response recommendations for the customer to implement if the IT operation team does not have access to the relevant system.

4.2.1 Service Offering Overview

The table below describes Secure Access Landing Page and Managed Service Offering.

Managed Security Service Offering Overview

	Managed Security Services
High Level Description	Provide an SSE solution (Cisco Secure Access) which can be used by a customer to onboard partner users and networks into the customer environment to provide access to a specific set of authorized applications. This solution will be managed via the Secure Access Landing Page which is build off the SecurityHub365 platform. This landing page will provide onboarding and management services for both the customer and the partner. The customer will be able to use this portal to manage the onboarded partners, and partner will be able to use this page as a self-service portal which allows them to onboard users and network into the service. This entire environment will be monitored on a 24/7 basis by the Gruve IT Operations team. This team will provide incident response services for the Secure Access environment as well as monitor the landing page. The Gruve Platform Engineering team will work will the customer to customize the landing page and optimize the user experience for both the customer and their partners.

High Level Landing Page Overview	• Multi-Tenant portal built off the SecurityHub365 platform. • Ticketing platform used to track all implementation activities, incidents, and change requests. • Bidirectional integration (“eBonding”) with the customers ticketing platform to ensure complete visibility for all new tickets and ticket updates. Enables customer to update and open tickets directly from their existing ITSM system. • Role based access control to provide the relevant access to the customer, partners, and users. • Orchestration engine used to deploy and update Secure Access configuration. • Provide partners with relevant site-to-site VPN configuration templates which can be utilized to integrate their environment into the Secure Access architecture. • Provide partner with relevant identity store integration process. • Secure document store which can be utilized to share relevant documentation with both the customer and partner. • Parter and user onboarding wizard to enable self-service onboarding and user management. • Partner and user change requests can be made directly through this portal, with the customer having complete visibility via eBonding. • Create dashboards for data visualization. • Generate and pull reports. • SAML integration.
Landing Page Managed Service Delivery Overview	• 24/7 Monitoring and Management of the Secure Access Landing page for availability and access. • Access to the Gruve team for troubleshooting issues with the landing page. • Utilization of the Gruve Platform engineering team to customize the onboarding wizards, the dashboards, and overall user experience. • Security patching. • Optimize eBonding configuration. • Service requests for the portal can be raised by the customer directly in their existing ITSM platform. These requests will get shared with the Gruve IT operations team via the eBonding configuration allowing the team to service the request. • VAPT of portal and its components.
Secure Access Managed Service Delivery Overview	• Onboarding of the Secure Access platform into the SIEM platform. • 24/7 Monitoring, Detection, and Response via The SIEM platform. • Security monitoring of the customer’s Secure Access environment and onboarded endpoints via The SIEM platform. • Incident identification and response recommendations. • SIEM platform Security configuration. • Alert/Alarm notification configuration. • Implementation of automation workflows from the automation service catalogue where applicable, with input from customer prior to rollout. • Creation, testing, validation, and rollout of up to three (3) customer requested incident response automation workflows per year. • Automation monitoring, troubleshooting, and optimization. • Quarterly Threat Hunting by the IT Operations Team. • Access to SecurityHub365 platform for onboarding, ticket management, and reporting.
Customer Profile	Large Enterprise
Pricing Model	See **Billing and Payment** section.

Optional Add-Ons	Complete 24/7 monitoring and incident response of the entire customer network. Digital Forensics and Incident Response. Custom Parser Development for SIEM platform. Additional Threat Hunting EDR/EPP AND/OR FW solution management.

4.2.2 Technology Stack

The following sections outlines the technology stack which will be utilized for this Managed Security Service:

	Secure Access Landing Page and Managed Service Offering
SSE Platform	Cisco Secure Access
	License Ownership: Customer OR Gruve Pricing: User Protection Suite or Secure Access License (Private Access). Priced per User.
Landing Page / Managed Service ITSM Platform	SecurityHub365
	License Ownership: Gruve Pricing: Bundled into overall pricing.
SIEM Platform	Internal Gruve Hosted SIEM Platform
	License Ownership: Gruve
Customer ITSM Platform	Service Now
	License Ownership: Customer

NOTE: The SIEM solution utilized for this service will be owned by Gruve. The customer will have option to request the utilization of their own internal SIEM platform for this service or request the SIEM logs collected by the Gruve team are forwarded to the customer's internal SIEM tooling.

4.2.3 Service Architecture

The architecture for the Secure Access Landing Page and Managed Service is centred around Cisco Secure Access and the Landing Page built off SecurityHub365. The Landing Page is the frontend of the service enabling self-service onboarding and partner/user management. Secure Access is the technological foundation of the service, enabling the communication between the customer and their partners.

After collecting the onboarding information from a user or a partner via a pre-configured onboarding wizard, the orchestration of the deployment can begin. This includes two main components, using automation to configure the service side elements, include DNS, IP ranges, users, network objects, etc…, and providing configuration templates to the partner to complete the partner integration into the service.

All endpoint and network device telemetry information relevant to the Secure Access architecture can be sent to the managed service SIEM platform. This will be utilized to monitor the environment for incidents and respond where necessary. The Gruve IT operations team will be monitoring the Secure Access environment on a 24/7 basis enabling the quick identification and resolution of incidents.

4.2.4 Service Delivery Inclusions

The Secure Access Landing Page and Managed Service offering will include the following:

	Managed Security Services

Landing Page Development	• Collect detailed customer requirements related to access control, onboarding flow, and process.
	• Exchange (Responsible, Accountable, Consulted, Informed ("RACI") matrix and identify a special point of contact.
	• Review existing ITSM process to determine best integration flow for eBonding configuration.
	• Design and architect the onboarding wizards based on the information collected from during the requirement gathering process.
	  ○ Partner Onboarding Wizard – Customer Side
	  ○ Partner Onboarding Wizard – Partner Side
	  ○ User Onboarding Wizard – Partner Side
	• Design and architect the automation flows based on the customer requirements and information collected from the onboarding wizards.
	  ○ New partner creation
	  ○ User onboarding
	  ○ Network Object Creation
	  ○ Certificate management
	  ○ DNS management
	  ○ NAT management
	  ○ Routing management
	  ○ Access Policy creation
	• Connectivity Validation: Design and architect automated workflows to validate connectivity to the partner environment immediately following onboarding. This ensures endpoint availability and link stability before the service is officially activated or presented for final approval
	• Design and architect the partner configuration template creation process.
	  ○ Identity Source Onboarding
	  ○ Site-to-Site VPN
	  ○ Certificate management
	  ○ Logging management
	• Review Landing Page support structure and feature request flow.
	• Plan out Landing Page development and roll out schedule. Features can be added on a rolling basis to reduce time to service activation.
	• Test and validate all onboarding wizards, automation workflows, and template generation processes.
	• Document portal design and architecture.
	• Document service delivery flows.

Managed Service Onboarding	• Provide customer team with necessary access into SecurityHub365. • ITSM platform and incident response / request ticket workflow review. • The SIEM solution configuration and integration with relevant products. Customer will be responsible for sharing the required access information to integrate with the relevant products. • Ingest overview and integration configuration review. Customer will be asked to share a list of alarms, notifications, and previous incidents triggered in their SIEM platform. This information will be used to design the overall integration and workflow for the SIEM ingest components. • Review automation service catalogue and identify automation workflows to implement for the customer for incident response. • Support the deployment of the SIEM Collectors as needed. • Review customer requirements for custom automation workflows and begin the design process.

Service Activation	• Secure Access Landing Page is live available for the customer and partner while being monitored 24/7 for availability. • Official start of 24/7 monitoring and incident response Managed Security Service for Cisco Secure Access as per SLA. • Discuss automation implementation workflow and customer requirements for incident response automation production rollout. • Begin to implement automations for incident response. • Baselining of SIEM incidents ingested into the SIEM platform.
Ongoing Landing Page Support	• 24/7 Availability Monitoring. • Troubleshooting support. • Security Patching. • Customization and optimization support. • Feature additions. • Regular security assessments. • Regular reporting. • Overall status review provided during Quarterly Business Reviews.
Business as Usual Activities – Cisco Secure Access	• 24/7 Monitoring and Incident response. • Respond to alarms/notifications and create required ticket. • Management of the SIEM Platform. • Perform incident investigation and ticket enrichment. • Provide incident response recommendations. • Continuous design, implementation, and optimization of automation workflows. • Track remediation efforts, whether implemented by the customer or by automation. • Integration health monitoring. • Quarterly Threat Hunting. • Monthly reporting with Quarterly Business Reviews.

4.2.5 Data sovereignty

As part of successful delivery of the services offering, Cisco will be required to collect and store telemetry data from the Customer environment that will be used by the SIEM platform and the Gruve IT Operations Team to deliver the managed service. The Secure Access SaaS service will also generate and store this data.

Cisco will provide details on the available locations for data storage, by default United States based instances of Secure Access will be selected. For Cisco Secure Access, currently data processing does occur 100% within the United States.

The data ingested into the SIEM platform will be hosted in the United States.

It is the Customer's responsibility to ensure any sovereignty requirements or regulations they need to meet are supported to an appropriate level within the delivered service. If sovereignty requirements are not met, Customer must notify Cisco/Gruve to discuss corrective action.

4.2.6 Stored data lifespan

It is the Customer's responsibility to ensure data is being managed in accordance with Customer sovereignty requirements.

There are the components to consider for data retention:

1. SIEM Platform
2. SecurityHub365 (Landing Page)

For the SIEM platform the data retention location will be the United States. The default data retention period will be for twelve (12) months with ninety (90) days of hot storage.

SecurityHub365 is currently hosted in locations in India and the United States. The customer has the option to utilize the region which meets their data retention requirements. The customer also has the option to select a specific Azure cloud region for the deployment of the SecurityHub365 platform. Ticket data will be stored for one (1) year by default.

It is Cisco/Gruve's responsibility to ensure the stored data lifespan allows the IT Operations team to meet its agreed upon service obligations and service level agreements as defined within this service description. Cisco/Gruve reserves the right to evaluate ongoing storage and retention requirements with the Customer and make recommendations to the Customer regarding stored data lifespan.

4.2.7 Service Reporting

The IT Operations Team provides service reporting to Customer on a quarterly and/or monthly basis depending on the level of service selected and as part of periodic business reviews with Customer. Standard reports are made available on a regular basis via the SecurityHub365 customer portal.

- Alert and Incident Volume Report.
- Most active partners.
- Remediation Report.
- Recommendation Report.
- Partner and User Count Reports.
- Secure Access Utilization Reports.
- License utilization reports.

The IT Operations Team provides a near real-time, service portal called SecurityHub365 to allow Customers to observe service activity on a self-serve, as-needed basis. This portal can also be utilized to pull reports and make service requests.

4.2.8 Service Exclusions

Cisco/Gruve services do not include:

- Setting up connectivity between Customer locations and the unified SOC platform.
- Any additional products or licensing for Customer elements required for the service.
- Configuration of end products to facilitate integration with the SIEM platform.
- L1 Helpdesk support for general employees. The IT Operations Team will NOT communicate directly with Customer employees who are not on the Customers IT Operations or Security team. Responding to employee help desk calls will be the responsibility of the Customer.

4.2.9 Customer Responsibility

- Partner tracking and initial onboarding authorizations.
- Monitoring of the network environment exclusive of the Secure Access architecture components.
- All Telemetry Sources for data ingestion into the SIEM platform, as identified by the Customer and the IT Operations Team:
    - Security software or equipment such as security devices (virtual/physical firewalls, etc.).

- Endpoint security tools.
- IAM tools

- Support connectivity necessary for connecting to the SIEM platform from the Customer environment (Internet Connectivity).

4.2.10 Standard Packaged Service Feature Definitions

Service Feature	Definition
Secure Access Landing Page	Onboarding portal used by the customer, partner, users, and the IT operations team to manage and operate this service. This landing page will be built off the SecurityHub365 ITSM platform. It will be used to collect all the relevant onboarding configuration, orchestrate the configuration of Secure Access and the relevant components, and track all incidents and change requests via tickets.
Security Incident Management	Pre-built processes, analysis, and analytic tools, combined with security analyst expertise and automation. The IT Operations Team then will identify, triage, contain, and develop response and remediation plans based on the incident risk and Customer business exposure.
Threat hunting	Based on Cisco/Gruve and industry knowledge of threat actors Tactics, Techniques and Procedures (TTPs), developing a hypothesis and a set of fact-finding tests to determine if there is evidence that a threat has been seen in the Customer environment. If evidence is found, develop a remediation plan and eradication recommendations.
eBonding	Integration of the customer ticketing platform to SecurityHub365 for by directional ticket updates through SecurityHub365.

4.2.11 Add-On Services

These add-on services can be purchased to bolster this overall Managed Security Service offering.

Service Feature	Definition
Complete 24/7 Monitoring and Incident Response Services	The current service definition covered 24/7 incident response for the Secure Access environment. This addon would extend those incident response services to the entire customer environment. The customer has the option to include additional components of their network environment to be included in the 24/7 monitoring and incident response services being provided for Secure Access.
Customer Parser Development	Support the development of customer parsers utilized to ingest data into the SIEM platform. These parsers may be required if the customer would like to ingest data from customer applications into the SIEM platform.
Additional Threat Hunting	Perform additional threat hunts in additional to the quarterly threat hunts included in the managed security services.
Digital Forensics and Incident Response	Utilization of Cisco Talos, the dedicated Digital Forensics and Incident Response team to do deeper analysis of an incident. This includes deep forensics of impacted devices, deeper root cause analysis, and recommendation on future mitigation.

EDR Migration	Professional services migration from the existing EDR platform in the customer environment to a supported EDR platform. This includes the design, testing, migration support, and validation.
FW Management	24/7 Management and configuration support for the firewalls in the environment. This includes configuration changes, policy updates, troubleshooting and upgrade support.

5. Service Enablement

5.1 Provisioning Planning and Management

The Managed Security Service consists of two primary phases:

1. Development and Onboarding
2. Continuing Services (Managed Services)

When the customer purchases the service there will be a scheduled kick off scheduled at least four (4) weeks from engagement closure. This kick off will be utilized to introduce the services team with the customer and plan the development and onboarding schedule.

Service Onboarding will begin with a series of emails sent directly to the customer which will include a variety of information on the onboarding process. This includes the schedule of the onboarding process, a list of information to be collected from the Customer, and instructions on how to access the SecurityHub365 Portal.

Cisco/Gruve supports and delivers high-touch onboarding capabilities as part of the service. High-touch onboarding is designed to accelerate turn-up of the service will facilitating and documenting Customer success requirements over the lifecycle of the service.

Service development and onboarding will be handled in two streams. One stream will work with the customer team to collect the requirements, develop/test, and eventually deploy the Secure Access landing page. The second stream will work on onboarding all the components of the 24/7 Secure Access Managed Service.

Continuing services, which includes the delivery of all the components of the managed service outlined in this document and SLA tracking. Continuing services also includes the management and support of the Landing Page created to manage partners and users. Continuing services will begin once the onboarding process has been completed. The official start of continuing services will be determined during the onboarding process.

5.2 Service Development and Onboarding

Gruve provides service development program to facilitate a seamless development of the Secure Access Landing Page. The following will be provided:

- Dedicated project manager.
- Landing page design and architecture.
- A platform engineering team which will be utilized to develop and customize the landing page.
- Periodic progress reviews as agreed upon with Customer at the beginning of the onboarding engagement.
- Documentation detailing the requirements and deliverables of Secure Access Landing Page development process.
- Access to the SecurityHub365 portal which will be utilized to track the development process and allow the customer to raise service and feature requests.

The expected duration for service development must be agreed upon at purchase of this service and is expected to be between six (4) to twelve (12) weeks.

Gruve provides an onboarding and activation program to facilitate a seamless enablement of the Managed Security Service. The following will be provided:

- Dedicated project manager.
- Project plan development and project management.

- A dedicated specialist technical a resource.
- Periodic progress reviews as agreed upon with Customer at the beginning of the onboarding engagement.
- Documentation detailing the requirements and deliverables of Managed Security Service including Customer success metrics and Customer reporting.
- Access to the SecurityHub365 portal which will be utilized to track the onboarding process and allow the customer to raise service requests.

The expected duration for service onboarding must be agreed upon at purchase of this service and is expected to be between four (4) to six (6) weeks.

Customer must provide:

- A dedicated point of contact to manage enablement through the duration of the onboarding cycle. Information on Personal Time Off ("PTO") and work schedule should also be supplied for scheduling purposes.
- Technical or specialist cyber security resources as necessary.
- Technical or specialist ITSM resources as necessary.
- Access to any required systems or tools to evaluate necessary technical integration needs.
- Access to the ITSM platform for eBonding configuration.
- API keys and credentials for required telemetry source integrations with SecurityHub365 and Secure Access.
- Network device access credentials to allow the Gruve IT operations team to apply any automated remediation workflows as agreed upon by Customer and the IT Operations Team.
- Access credentials to IaaS or SaaS cloud services to be integrated with this service as agreed upon by Customer and the IT Operations Team.
- Planned maintenance to required tools, networks, cloud services or infrastructure.

Development and Onboarding can happen in parallel. The duration will be contingent on customer availability. Leveraging the Gruve team's extensive experience with large-scale firewall and connectivity migrations, our team is prepared to design the required workflows needed to migrate CVS's legacy tunnels with maximum efficiency. This 'Migration Factory' approach ensures that existing third-party connections are transitioned to the new Secure Access architecture with minimal manual intervention and optimized downtime.

5.3 Continuing Services (Managed Security Service Delivery)

A core component of the Continuing Services Gruve provides is a Landing Page Support Service to manage and operate the Secure Access Landing Page. The following will be provided:

- 24/7 Monitoring for availability
- Security Monitoring
- Troubleshooting support
- Feature Development
- Security Patching

An additional component of the Continuing Services Gruve provides is a Managed Security Service to monitor the Secure Access environment. The following will be provided:

- 24/7 Monitoring

- 24/7 Incident Response
- Incident Management
- Incident Response Recommendations
- Notifications and alerts via the SecurityHub365 platform
- Incident Response Automation Development
- Product lifecycle support
- Configuration support
- Policy updates
- Troubleshooting support
- Alert configuration
- Regular Reporting
- Quarterly Business Reviews
- Quarterly Threat Hunting
- Service Level Agreement (SLA) Management
- Escalation Management

Gruve will provide these additional services for the relevant products when the EDR/EPP AND/OR Firewall management add-on option is selected:

- Product lifecycle support
- Configuration support
- Policy updates
- Troubleshooting support
- Alert configuration

Customer must provide:

- A dedicated point of contact to manage enablement through the duration of the service delivery. The IT Operations Team needs to be notified if this point-of-contact changes during the duration of the service. Information on Personal Time Off (“PTO”) and work schedule should also be supplied for scheduling purposes.
- Provide access to Cisco Secure Access (only required if the customer chooses to own the license).
- Support the required configuration needed to integrate the relevant tools, applications, and devices into the SIEM platform.
- Provide list of users which will require access to the Landing Page (SecurityHub365, the ITSM platform utilized to deliver these services).
- Customer to provide authenticated and authorized access including email address to the IT Operations Team.
- Escalation matrix.
- Customer to provide the asset/application list and network diagrams.
- Participate in regularly scheduled project review meetings or conference calls.
- Provide internal resources to support the service initiation.
- Direct employee helpdesk support.

5.3.1 Service Start Date

Service will start on the activation date selected by the customer when purchasing these services. SLA tracking will begin once all Onboarding activities have been completed, and the service will continue to the agreed upon duration of the contract.

5.3.2 Continuing Services Description

The following section provides additional details on the continuing services included in the Managed Security Service offering:

Service Component	Key Activities
Managed Secure Access	• 24/7 Monitoring • 24x7 Incident Response. • 24x7 Security monitoring security breaches, abnormal activities, etc. detected by the SIEM platform. • 24/7 SIEM management. • Design, Implementation, and Monitoring of up to three (3) customer requested custom incident response automation workflows for Cisco Secure Access. • Communication handled via the SecurityHub365 portal. • Automation monitoring, modifications, and updates. • Monitoring of the SIEM Integrations. • Deployment and monitoring of any required SIEM collector virtual appliances. • Secure Access configuration support • Secure Access troubleshooting support. • Secure Access client management support. • Monitor partner and user onboarding activities. • Provide partner and user onboarding support when needed. • Secure Access automation development, monitoring, and troubleshooting. • Quarterly Threat Hunting.
Incident Response Management	• Analyse different Security Indicators of Compromise (IoCs) and identify the IoCs that are important for the Customer's network. • Identify, triage, and escalate any malicious events occurring on the Customer's network. • Incident detection and response update via ticketing platform. Create, update, and evaluate tickets generated for security incidents on the network. • The IT Operations Team will be working closely with the Customer's security operations team to recommend and support any changes required as part of an incident response plan/procedure. • If/When a security incident is identified and mitigation plan identified, an engineer will recommend the required changes to the Customer team. The Customer's device management team will then implement these recommendations. • Implementation of relevant incident response automations from the automation service catalogue to improve the overall efficiency of the incident response process. • As per the Managed Security Service description, custom incident response automation workflows can be requested by the Customer team and created to automate the incident response process for specific use cases.
On-Going Landing Page Support	• 24/7 Availability monitoring. • 24/7 Troubleshooting support. • Feature development and deployment. • Security assessments and reviews. • Security patching.
Reports	The following reports on incidents and service delivery operations will be provided: • Weekly Reports • Monthly Reports • SLA Reports • Alert and Incident Volume Report.

	• Most active partners. • Remediation Report. • Recommendation Report. • Partner and User Count Reports. • Secure Access Utilization Reports. • License Utilization Reports **All service reports will be published as agreed to or defined during the onboarding process.**
Quarterly Business Reviews	**The IT Operations Team will conduct service review meetings once every quarter to discuss the following:** • Review of Secure Access utilization and user counts • Review partner onboarding status • Analyse partner usage statistics. • Review incidents and escalated events with Customer. • Review of most critical events (as needed). • Review any edge cases, defined as any incidents that required response outside of the normal Customer escalation process. • Discussion around event handling & communication improvements. • Service status and compliance with SLAs. • Personnel changes. • Customer's plans for the managed solution and relevant IT infrastructure. • Customer's feedback on quality of service. • Any other matters that are agreed upon between Customer and Cisco/Gruve. • Review of quarterly Threat Hunting reports.

5.3.3 Services Personnel

The following personnel will be delivering the offerings described in this document.

	Personnel
Managed Secure Access	• Shared PM to Manage Onboarding • Transitioned to Shared CSM for service delivery • Shared Ops Manager, SOC Manager, and Solutions Architect • Shared L1, L2, and L3 engineers from the 24/7 IT Operations Team
Landing Page Development and Management	• Product Manager • Joint CSM who will also handle the Managed Secure Access component of this engagement. • Solutions Architect • Shared Platform Engineering Team.

6. Standard Service and Support

6.1 Service Management

6.1.1 Cisco/Gruve Obligations

Cisco/Gruve will:

- Provide your Authorized Operational Contacts with access to the ITSM platform (SecurityHub365).
- Manage Service Requests and Incidents as set out in this Service Description
- Perform necessary maintenance on the service infrastructure during a maintenance window.
- Maintain an inventory of the Service Requests, including tracking and recording changes to the configuration of the Service
- Provide a monthly report on the status of all Service Requests and Incidents received by the IT Operations Team, and performance against Service Level Targets

6.2 Security Incident Management

6.2.1 Scope

The IT Operations Team will manage the lifecycle of an Incident through to resolution.

Where the IT Operations Team considers that an Incident is attributable to a Service Exclusion, the team will notify the Customer that the Incident is outside the scope of the Service. Where this occurs, the IT Operations Team is not responsible for the Incident and, where Customer requests to resolve the Incident, the IT Operations Team reserves the right to charge for any services provided on a time and materials basis.

6.2.2 Event and Alert Reporting

The IT Operations Team will monitor the dashboards of the SIEM platform. Periodic reporting of the volume and nature of events and alerts will be provided via the Security365 customer portal. Dashboards will also be visible in the SecurityHub365 platform.

6.2.3 Security Incident Management

Cisco/Gruve will:

- Log all incidents and determine the priority.
- Inspect and adjust incident priority as necessary based on risk to the organization.
- Respond to and provide remediation recommendation for incidents in accordance with the Service Level Targets.
- Update the Customer service portal, Security365 regarding the status of incidents.
- Consolidate and provide reports to Customer leadership monthly.

6.2.4 Security Incident Priorities and SLAs

Cisco/Gruve will assess the Impact of an Incident using the below criteria:

Impact / Risk		Definition
1	**Critical: Extensive/ Widespread**	An Incident which has major business risk to Customer assets or operations.
2	**High: Significant/ Large**	An Incident which has significant business risk to Customer assets or operations.
3	**Medium: Moderate/ Limited**	An Incident which has minimal risk to Customer assets or operations.
4	**Low: Minor/ Information**	An Incident which has little or no risk to assets or operations. This can include information notifications.

Cisco/Gruve will meet the following SLAs:

Mean Time to Notification (MTTN)

Time from event detection to ticket establishment.

Severity	Definition	MTTN
1	**Critical** Notification of incident must happen as soon as possible.	15 Minutes
2	**High** High priority incident but not as critical as a Sev1. Notification will come in an expedited manner.	30 Minutes
3	**Medium** There is limited urgency for incident notification, and so notification will be provided in a timely manner.	1 Hour
4	**Low** There is no urgency, and the Incident is not time-critical to fix so notification will be provided on a standard schedule.	2 Hours

Note: These values can be updated based on the customer requirements.

Mean Time to Respond (MTTR)

Time from event detection to ticket restore.

Severity	Definition	MTTR
1	**Critical**	1 Hour

	The Incident restored with as soon as possible with the highest priority.	
2	**High** The Incident is of a higher priority however can take some additional time to restore.	2 Hours
3	**Medium** There is no urgency, and the Incident can be fixed at a scheduled time later (or a workaround is available).	4 Hours
4	**Low** There is no urgency, and the Incident is not time-critical to fix. The containment requirement is low or not required.	8 Hours

Note: These values can be updated based on the customer requirements.

6.3 Active Incident Response

During an active threat or attack scenario, the IT Operations Team will supply response actions and direction based on the nature if each scenario. The IT Operations Team will not directly change configurations on Customer assets outside of Cisco Secure Access, unless via the automated response actions that have been defined as part of the service. These automations will be developed and deployed with prior approval from the Customer team.

When additional managed add-on services have been purchased, such as Firewall managed services, the IT Operations team will perform the required incident remediation activities on those managed products/devices when required. Remediation actions on devices/application not included for management in the Managed Security Service are the responsibility of the customer.

6.4 Requesting Service

6.4.1 Scope

Cisco/Gruve will manage Service Requests.

Some Service Requests may *not* be included within the cost of the Service. Any additional charges payable for fulfilment of a Service Request are dependent upon the type of Service Request and will be set forth in the Service Request catalogue or advised in writing by The IT Operations Team.

Where the IT Operations Team considers that a Service Request may affect the Team's ability to deliver the Service or meet a Service Level Target, Cisco/Gruve may reject the Service Request and recommend alternatives to fulfil the Service Request (subject to conditions).

6.4.2 Service Requests

Customer Authorized Operational Contact must submit all Service Requests to the email address identified as the Service Request special point of contact or via the SecurityHub365 Portal. Email templates are available within the SecurityHub365 portal.

Cisco/Gruve will:

- Review the Service Request and determine whether the Service Request is a Standard Service Request or Non-Standard Service Request.
- Advise whether the Service Request is accepted and any impact that the Service Request may have on the Service.
- Respond to and fulfil accepted Service Requests in accordance with the process, pricing and timeframes will be determined by the IT Operations Team and accepted by the customer.

6.4.3 Service Change Requests

Customer may request change to the service in writing on a regular basis. Changes may include changes in response procedures or additions of additional telemetry sources. Cisco/Gruve reserves the right to review and specify where a requested change falls outside the scope of the purchased service.

Standard change service requests are based on typical Customer IT security control point lifecycle management; these include:

- Telemetry source credentials changes
- Security control point policy changes
- Software or firmware updates to integrated telemetry sources

Non-standard or emergency change service requests will require immediate attention from both Customer and the IT Operations Team. Cisco/Gruve expects Customer to make all required resources available to the IT Operations Team to mitigate or address the situation. These include:

- Changes because of active threats or incidents in the Customer environment
- Changes because of power failures or other environmental conditionals

Customer Responsibilities

It is understood that Customer may intentionally make changes to their IT infrastructure including endpoint, network, cloud, email, and identity/access control points that may impact the Service.

These changes may impact the service and the IT Operation Team's SLAs and related Service delivery commitments. For this reason, Cisco/Gruve requires that Customer notify the IT Operations Team of these changes forty-eight (48) business hours in advance of planned change implementation. These requirements will be discussed with the customer during the onboarding process.

- Reconfiguration of telemetry sources.
- Reconfiguration of IT infrastructure.
- Changes to internet service impacting reachability from the Customer environment to the SIEM platform.
- Product or tooling migrations.

6.5 Customer Responsibilities

6.5.1 General Responsibilities

To enable the IT Operations Team to provide the Service, in addition to any other obligations set out in the Agreement, the customer must in a timely manner:

- Maintain appropriate security, access controls, protection and backup of your data, unless expressly identified as an obligation of Cisco/Gruve as part of the Service.
- Allow access for the SIEM platform to telemetry sources such as agents and probes to enable the IT Operations Team to actively monitor the Service.
- Provide access to Cisco Secure Access for service delivery (only required if the customer chooses to own the license).
- Provide list of users which will require access to Secure Access Landing Page/SecurityHub365.
- Provide an escalation matrix.
- Provide the asset/application list and network diagrams. The IT Operations Team will provide a template through SecurityHub365 which can be utilized to share the relevant asset/application information with the team.
- Participate in regularly scheduled project review meetings or conference calls.
- Provide internal resources to support the service initiation.

6.5.2 Additional Scope

Any request by you to vary the scope of the Service, including for upgrades to the Service to take advantage of new features or functionality supported by the Service, will be subject to a separate quotation.

Specific Add-on services, outlined in this document, can be purchased at the start of the engagement or throughout the duration of the Managed Security Service.

The Agreement will be varied to reflect any agreed change to the scope of the Service and a contract term beyond the Committed Term may apply to the purchase of additional end points or devices (Extended Term).

7. Billing and Payment

NOTE: This billing and pricing section outlines the billing options for this service. The final pricing for this service will eventually be calculated using the methodologies described below. Final pricing will be provided once additional scoping details have been collected from the customer.

Pricing will be based on agreed upon contract terms and conditions. Pricing will include two high level components.

1. Development/Onboarding
2. Managed Services

From time to time during the duration of the agreement, there may be changes or additions to the service as agreed between Cisco and Gruve which will result in new or modified contractual service pricing; service contracts will be updated accordingly.

7.1 Development/Onboarding Costs

Development/Onboarding costs will be provided as a flat rate. This rate will depend on the total number of features required for the Landing page. This will also depend on any additional customer requirements the customer may have. If requested, these onboarding costs can be paid upfront, or they can be divided up and paid alongside the managed service costs.

7.2 Managed Service Costs

Managed Service costs cover the 24/7 availability monitoring for the Landing Page and 24/7 monitoring and incident response for the Secure Access architecture. This includes all support required to maintain and operate both the Secure Access solution and the landing page. Manage Service Costs can be accounted for in one of two ways:

1. Consumption Model
2. Flat Rate

7.2.1 Consumption Model

In a consumption model services will be paid for on a quarterly or monthly basis. This price will include a base rate and a consumption rate. The base rate will be determined as 25% of the maximum overall utilization expected by the customer as determined by Secure Access license consumption. The consumption rate will be determined based on the average number of daily consumed Secure Access Licenses. Based on this daily average the customer will pay a per license per month or a per license per quarter cost. License consumption counts will be tracked via the Secure Access Landing page and can be monitored by the customer. Then based on the consumption the customer will pay the base rate plus the costs accrued based on consumption.

Cost Component	Cost Definition	Cost Calculation
Base Rate	This the base cost paid every payment period. This cost is by taking 25% of the estimated maximum users the customer	Total Maximum # of Users * 25% * per Secure Access license per month cost.

	expects and multiplying it by the Secure Access license per pay period (month or quarter) cost. If the total number of consumed Secure Access Licenses exceeds the maximum utilized to determine the base cost, the base cost can be reevaluated.	
Consumption Rate	This cost is paid every payment period. This cost is determined by taking the average number of daily consumed Secure Access licenses and multiplying it by a discounted per license per pay period cost.	Average # of Daily Concurrent Users * 75% * per Secure Access license per month cost.

7.2.2 Consumption Model

In a flat rate model, the monthly cost is determined based on the total number of expected daily concurrent users. The customer will share their estimate at the beginning of the project as this value will be utilized to determine the cost per month or quarter. If the customer exceeds this user count by 10% for more than three (3) consecutive months Cisco/Gruve have the right to reevaluate the pricing.

Cost Component	Cost Definition	Cost Calculation
Rate	**This the base cost paid every payment period. This cost is determined by taking the estimated average daily Secure Access license consumption count and multiplying by a per license per pay period cost.** **If the total number of consumed licenses exceeds the value utilized to determine this cost, this price can be reevaluated.**	Total Maximum # of Daily Consumed Secure Access license * per user per pay period cost.

Strategic Delivery Options:

7.3 Flexibility for CVS Health

Cisco recognizes that a project of this magnitude requires not only the right technology but also the right delivery model. To ensure total alignment with CVS Health's operational preferences, we are pleased to offer two distinct paths for the implementation of the 3rd Party Landing Zone (3PLZ).

Regardless of the path chosen, **Cisco Secure Access** remains the core connectivity engine, and **Presidio** - Cisco's strategic partner of choice - will serve as the primary interface for procurement, lifecycle management, and ongoing account support.

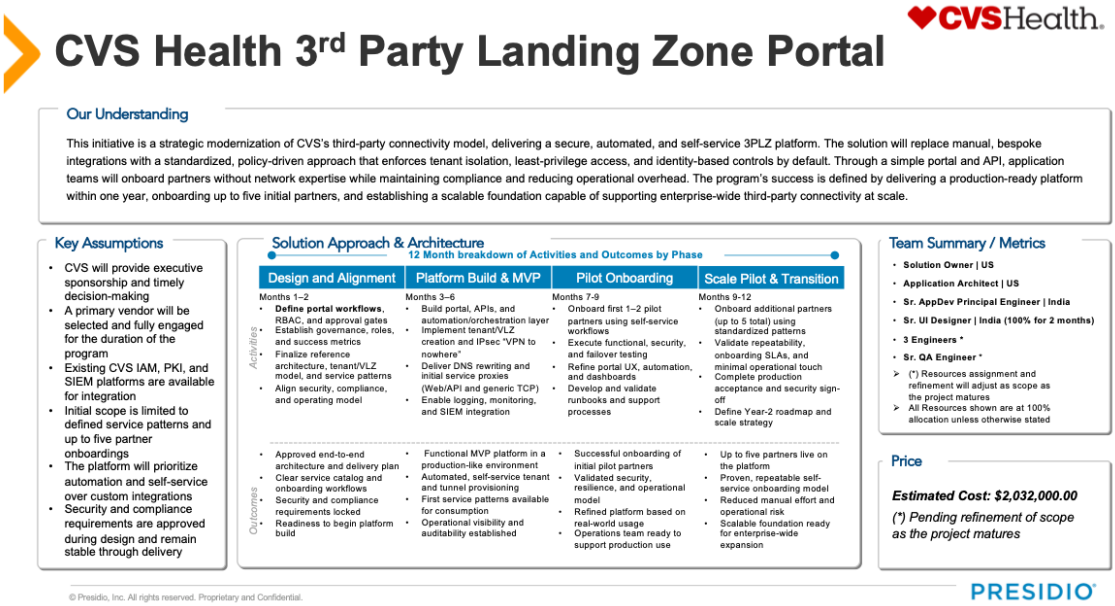
Option 1: The "As-a-Service" Accelerator (Cisco + Gruve.ai)

This is our primary recommendation for CVS Health. By leveraging Cisco's strategic investment in Gruve.ai, we provide a turnkey, "As-a-Service" frontend and fully managed security solution purpose-built to orchestrate Cisco Secure Access. This option combines a modern, automated user interface with Cisco's 24/7 Managed Excellence.

- Best for: Rapid deployment, reduced upfront development costs, and a SaaS-like user experience.
- Managed Operations: Includes 24/7 proactive monitoring, incident response, and threat hunting, removing the operational burden from CVS internal teams.
- Key Advantage: Direct API integration between the Gruve portal and Secure Access, enabling the "Version 1.0" vision by the end of 2026.

Option 2: The Lifecycle-Driven Platform (Cisco + Presidio)

Complementing our accelerated managed service model, Cisco and Presidio offer a Lifecycle-Driven Platform. This 12-month strategic initiative leverages Presidio's deep institutional knowledge of the CVS environment to design and build a bespoke 3PLZ portal and operational runbook. This path is specifically structured to prioritize a phased development cycle with the goal of an eventual transition to CVS internal ownership and management.



The Cisco Commitment

Cisco's primary objective is the successful modernization of CVS's third-party connectivity model. Whether CVS chooses the **as a service offering with Gruve.ai** or the **CVS managed Presidio platform**, Cisco will provide the underlying Secure Access technology, and Presidio will provide the strategic oversight and transactional stability required for a project of this scale.

Appendix

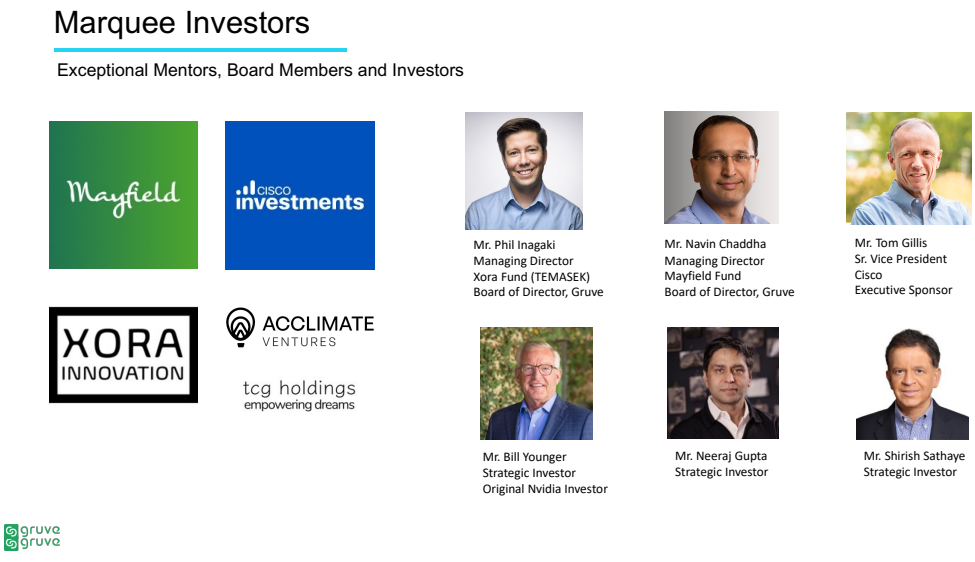
Terminology Definitions

Term	Definition
Committed Term	The contractually agreed upon service duration
MTTN	Mean-time-to-Notify
MTTR	Mean-time-to-Restore to a detected alert
Managed Security Service	Managed Extended Detection and Response delivered by the IT Operations Team via the SecurityHub365 portal and the SIEM platform.
EDR/EPP	Endpoint Detection and Response / Endpoint Point Protection Platform.

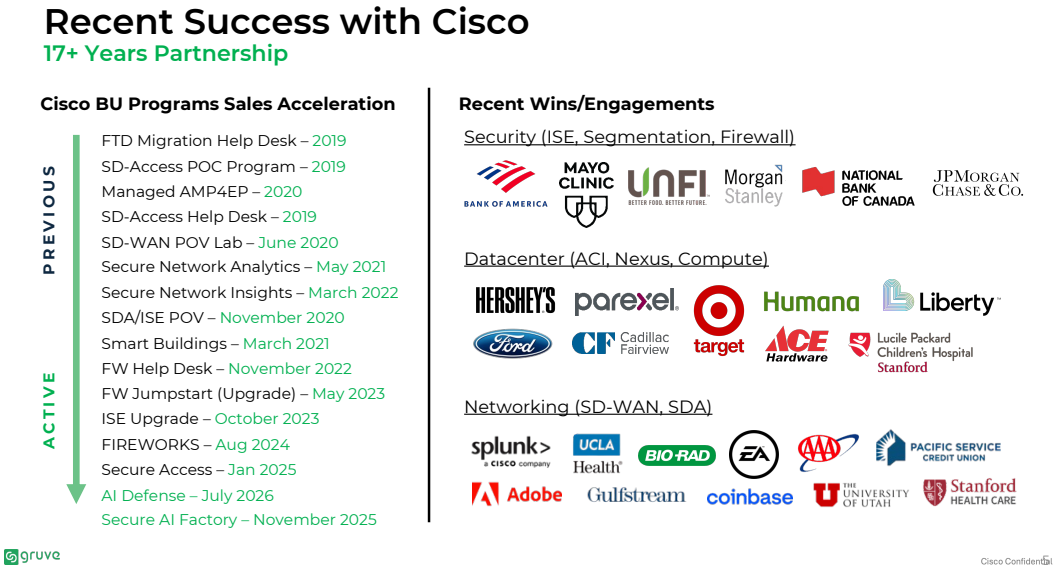
Gruve and Cisco Partnership Overview

Gruve and Cisco have a long-standing partnership and have effectively delivered IT services to a wide range of customers. Gruve is a Global Services Partner with Cisco and delivers IT services on behalf of Cisco and as a Cisco partner throughout the world.

While Gruve was founded in 2024, Gruve acquired three long standing Cisco services partners, SecurView Inc, Lumos, and NetServ. These companies have a combined 25+ year history delivering IT services for and through Cisco. The acquisition and integration of these firms into Gruve has created a powerful services partner, delivering services across the Cisco Cybersecurity, Data Center, and Enterprise Network portfolio. Cisco seeing the potential of the Gruve as a partner has directly invested in Gruve's Series A round of funding with Tom Gilis acting as the executive sponsor.



Gruve and Cisco have extremely close relationship with Gruve delivering programs and services directly for Cisco. As a trusted expert partner Cisco will bring Gruve in to support larger internal initiatives related to their highest internal priorities. Gruve's involvement in Cisco programs is shown in the graphic below.



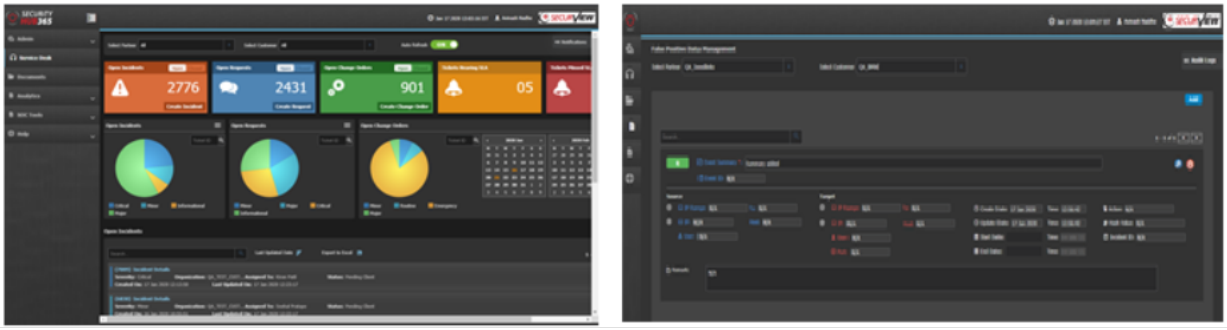
The combined Cisco and Gruve partnership will bring combined expertise and long-standing partnership to the customer, delivering expert services via cutting edge Cisco solutions. This will ensure smooth operations for the customers and the highest standard of service.

SecurityHub365 Overview

SecurityHUB365 serves as a cloud-based service-delivery Managed Security Service (“MSS”) platform and Information Technology Service Management (“ITSM”) platform. It provides a unified interface to the Security Operation Center (“SOC”) to analyse the reports/patterns. It helps the SOC team “operate” the Managed Security Services from a central location supporting multiple “Points-of-Presence”. It also serves as a single pane-of-glass to the SOC engineers/analysts/managers to operate various aspects of the service.

A few salient features of the SecurityHUB365 platform tool are as follows:

- Multi-channel service delivery
- Hierarchical Partner/Customer provisioning
- User Management
- Active Directory Integration for Authentication
- AD driven security policies
- Inbuilt Ticketing
- Support for all types of tickets – Incidents, Change Orders, Requests
- Customizable workflows
- SLA Monitoring & Alerts
- Integrated SIEM Interface
- Asset Management
- Customizable white labelling

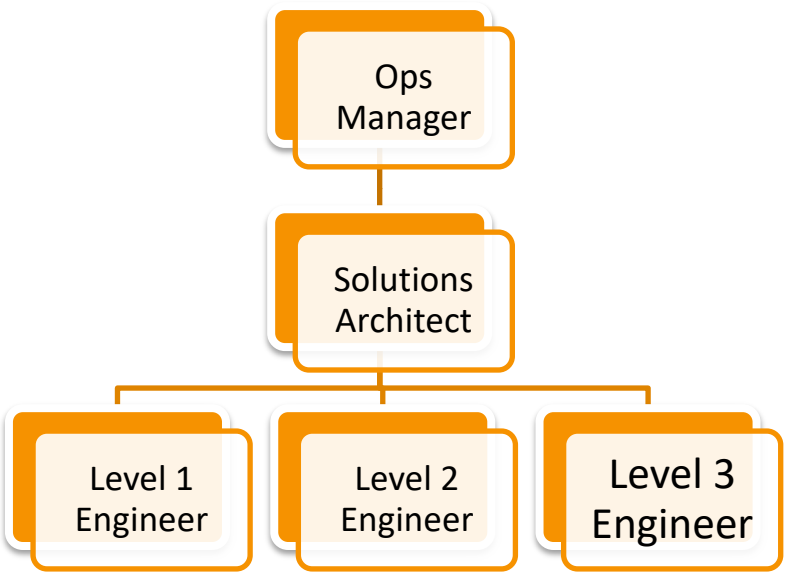


Note 1: There is no user limit for SecurityHUB365 portal access. It can be provided to 4-5 members or more easily, if required. No additional charges will be involved.

Note 2: The SecurityHub365 Licensing Cost is bundled into the Managed Security Service Pricing

Personnel Overview

This section describes the details on the provision of the operation team. The IT Operations Team is structured as follows:



LEVEL 1 Engineer (L1)

The primary function of an L1 Engineer is to implement P3 and P4 change requests and carry out scheduled upgrades. L1 Engineer's will also review P2 and P1 change requests and provide some context prior to escalating the ticket to a Level 2 Engineer or Solutions Architect.

The secondary function of L1 Engineer's is to monitor the Client's environment on 24*7 basis and identify resource availability and utilization issues. Once an issue is identified the L1 Engineer will perform a first responder assessment of the Alarm. Following determination of the issue this shall be escalated to the L2 Analyst for further investigation. In summary the L1 Engineer role is described as follows:

- Perform P3 and P4 Change Requests
- Review P2 and P1 Change Requests
- Perform Scheduled upgrades.
- Acknowledge, analyse, and validate alarms triggered from correlated events through SIEM solution.

- Acknowledge, analyse, and validate incidents received through other reporting mechanisms such as email, phone calls, management directions, etc.
- Escalate validated and confirmed incidents to relevant IT Operations Engineer (Either a Level 2 Engineer or the Solutions Architect).
- Undertake first stages of false positive and false negative analysis.

LEVEL 2 Engineer (L2)

The primary function of an L2 Engineer is to implement P2 and P1 change requests and carry out unscheduled upgrades and patches. L2 Engineer's will review all P1 and P1 tickets and provide some context prior to escalating the ticket to a Solutions Architect if required.

The secondary function of this team is to analyse issues and tickets escalated by L1 Engineers and undertake the detailed investigation of the issue or change. The L2 Engineer can determine whether higher priority tickets can be resolved or need to be escalated. They will be coordinating with the Client's IT team for throughout the resolution of the issue or implementation of the change. In summary:

- Escalate validated and confirmed P1 and P2 tickets when needed.
- Notify customer of incident remediation was successful post implementation.
- Fine-tune alerting rules and thresholds to reduce false positive and remove false negatives.
- Implement unscheduled upgrades and patches.
- Proactively monitor annual upgrade plan for managed devices.
- Develop and distribute information and alerts on required corrective actions to the organization.
- Consult with customer to create use cases for the development of customer specific correlation alerts.

LEVEL Engineer (L3)

The primary function of the team-lead is to maintain a co-ordination between the IT operations team and address any technical as well as team management issues for smooth operations during the shift. (This role can be jointly assumed by the Solutions Architect and Ops Manager depending on the scale of the engagement)

- Audit L1 & L2 work .
- Approve P1 and other emergency changes.
- Monitor unplanned upgrades and patching.
- Consult with customer to schedule change-windows.
- Conduct advanced analytics.
- Review the reports.
- Team Management to support the engineers in every shifts.
- Incident closure.
- Tracking SLA compliance.
- Service Management.
- Escalation Management

The following points provides the details of the roles and responsibilities for a L3 Engineers:

- Point of contact internally for information on Client's IT architecture.
- Conduct Exploratory Data Analysis (EDA), including acquiring, engineering, and exploring various data types and log sources for monitoring opportunities.
- Provide expert analytic investigative support of large-scale IT environments.
- Perform analysis of incident response mitigation options and support the implementation of these changes.
- Keep up to date with information security news, techniques, and trends.
- Monitor backup and schedule/design tests to validate the health of the backups.
- Perform system restores from backups with the support from the Solutions Architect
- Become proficient with third-party tools as required.

Solutions Architect

The Solutions Architect assigned to a managed service engagement acts as the Subject Matter Expert (SME) for the Client's network architecture. This engineer will be brought up to speed on the Client's network environment and be the primary escalation resource for both the Managed Service IT Operations Team and the Client's IT team.

- Client architecture SME
- Assume role of L3 engineer as needed.
- Managed Service Process Management.
    - Incident Response Management Process
    - Upgrade/Patching Process
    - Change Management Process
    - Backup/Restore Process
- Lead Quarterly Business Reviews (QBRs)
- Monitor the implementation of P1 and P2 changes and any emergency upgrades/patching.

Operations Manager (Ops Manager)

The Operations Manager will perform the platform management of the internal tools utilized by the IT Operations Team to deliver this service.

- Monitoring Platform management
- Prepare and test customer specific alerts.
- Creation of ad hoc dashboards for the customers
- Log archiving and management.