www.phoenixit.lk

WELCOME TO PHOENIX IT LANKA

Phoenix IT is an information technology firm focusing on cyber security via its dedicated Managed Security Services (MSS Provider) business unit. This business unit was established in collaboration with SecureOps, Montreal, Canada to provide industry standard security services and solutions to South Asian Small Medium Business (SMB) customers. We believe very organization irrespective of size is a target and should have access to the most suitable cyber security services and solutions to safeguard their operations.

VISION

"Secure the uninitiated"*

MISSION

"Our mission is to educate our customer base, build capacity in every country we operate in and make cyber security affordable to all."

* Those who believe they will never be a target

OUR SERVICES

MANAGE SECURITY SERVICE

SURVEILLANCE SOLUTION

DESKTOP/WEB/MOBILE APPLICATION DEVELOPMENT

CYBER SECURITY

AWARENESS TRAINING

IT CLOUD INTEGRATION

"We, at Phoenix IT, are committed to ensuring a secure future through application development using secure software development processes, specialist cyber security services, and managed security services.

Our partnership with SecureOps provides us with instant access to over 20 years of cybersecurity experience across large multinational organizations which we distill down to meeting our unique customer requirements.

As a group of Sri Lanka's foremost cyber security professionals we are committed to building capacity in Sri Lanka and contributing to the national goal of being a regional premium technology services hub.

We believe our approach to cyber security will help you understand your unique needs and look forward to being of service to your organization."

CHIEF EXECUTIVE OFFICER

OUR CERTIFICATIONS

VALUED PARTNERS/PRODUCTS

virsec	thycotic	Synology	asustor ASUSTOR Inc.	RAPID7
OneSpan Be bold. Be secure.	onelogin	DARKTRACE	LogRhythm	Radar
netskope	imperva	HIKVISION	alhua TECHNOLOGY	GTB Technologies Next Gen Data Protection
FORTINET	Check Point SOFTWARE TECHNOLOGIES LTD	paloalto NETWORKS	Harmony	EKRAN
CYBONET	CyberCyte	SOCRadar	radware	A10
	SecuPi	tripwire	Guardicore	

SOLUTION SUMMARY

virsec

- Patented AppMap™ Technology.
- Automated Protection Without Learning, Tuning, or Noise.
- Full-Stack Application Protection.
- Runtime Visibility and Protection.
- Protecting the World's Most Critical Applications.
- Highly-Scalable, Enterprise-Ready.

thycotic

- Privileged Access Management

Synology

- Photos. Protect, organize, and share memories.
- Audio Station. Keep your favorite tunes organized.
- Video Station. Manage your collection of movies and TV shows.
- Drive. Sync and access files anywhere.
- Cloud Sync. Sync with the cloud.
- Presto. Accelerate file transfers.
- Hybrid Share for C2 Storage

asustor

ASUSTOR Inc.

- Sign In Page
- Searchlight
- 2-way Backup
- Mission Mode
- Cloud Connect
- Seamless system migration
- Detection Tool
- Service LED Indicator
- HTTPS encrypted connections

RAPID7

- high-speed asset discovery
- configuration auditing
- target profiling
- malware detection
- sensitive data discovery
- vulnerability analysis

OneSpan

Be bold. Be secure.

- Electronic Signature.
- Digital Signature.
- Professional Plan.
- Enterprise Plan.
- eClosing.
- ID Verification & Authentication.
- Qualified Electronic Signatures.
- Virtual Room.

onelogin

- Cloud Directory.
- Unlimited SAML and OIDC Authentication.
- Single Directory Integration.
- Windows Domain Authentication.
- Mobile Single Sign-On.
- Password Policy Management.
- Prebuilt integrations to the OneLogin App Catalog.
- Multiple Languages

DARKTRACE

- Augment and empower security teams with autonomous, always-on, AI-driven capabilities

SOLUTION SUMMARY

LogRhythm

- Response
  - Threat Intelligence
- Records
  - Incident
  - Logs Incident Reports
  - Resource Usage
- Management
  - Incident Alerts
- Network Management
  - Activity Monitoring
  - Asset Management
  - Log Management
- Incident Management
  - Event Management
  - Automated Response
  - Incident Reporting
- Security Intelligence
  - Threat Intelligence
  - Vulnerability Assessment
  - Advanced Analytics
  - Data Examination

netskope

- adaptive access control
- cloud encryption
- cloud threat exchange
- data protection
- deployment options
- SSL/TLS Inspection
- Third party risk
- Threat Protection
- web content filtering
- Zero Trust Network Access

imperva

- Web Application Firewall. Blocks attacks with precision.
- Advanced Bot Protection. Prevents automated attacks.
- Runtime Protection. Disrupts supply chain attacks.
- Client-Side Protection.
- API Security.
- Server less Protection

GTB Technologies
Next Gen Data Protection

- Zero False Negatives
- Zero False Positives
- Off-network Universal Policy Enforcement
- Drip DLP
- OCR - Network, Endpoint & Discover
- Value delivered immediately using GTB's single agent cloud solution
- Real-time security, at scale and adaptable
- Single-tenancy models offering stronger isolation

HIKVISION dahua TECHNOLOGY

- Full-color image output.
- Support H.265+/H.265 video compression.
- Support rapid focus.
- High-quality imaging.
- Excellent low-light performance by Dark Fighter technology.
- 25x optical zoom, 16x digital zoom.
- Up to 200 m IR distance.
- Accurate human and vehicle target classification

Harmony

- Harmony Endpoint identifies ransomware behaviors such as file-encryption or attempts to compromise operating system backups, and safely restores ransomware-encrypted files automatically. Zero-Phishing® technology identifies and blocks the use of phishing sites in real time.

SOLUTION SUMMARY

CYBONET

- Protections from advanced malware threats within emails and attachments with sandboxing module.
- Strong protection from spam and viruses.
- Compliance ready solution with easy to search message archiving.

A10

- Local Server load balancing / Globe Server load balancing / DDOS

EKRAN

- Full Cycle Insider Threat Management

CyberCyte

- Ransomware Protection. Protect your organization in minutes from malicious applications including ransomware.
- Protection From Phishing E-mails. Enable the discovery and automatic deletion of malicious e-mails.
- Protection from Zero-Day Attacks.

SOCRadar

- Threat Fusion.
- Use Cases. Credentials & Data Leak Detection Dark & Deep Web Monitoring Phishing Domain Detection VIP Protection Supply Chain Visibility & Protection IOC Enrichment & SOAR Integration. Roles.

Check Poir
SOFTWARE TECHNOLOGIES

- VPN and mobile device connectivity.
- Identity and computer awareness.
- Internet access and filtering.
- Application control.
- Intrusion and threat prevention.
- Data Loss Prevention

paloalto NETWORKS

- Application-based policy enforcement (App-ID. ™
- User identification (User-ID™)
- Threat prevention.
- URL filtering.
- Traffic visibility.
- Networking versatility and speed.
- Global Protect.
- Fail-safe operation.
- malware Analysis and reporting
- VM-Series Firewall
- Management and panorama

Radar

- Ingest vast amounts of data from on-prem and cloud sources.
- Applies built-in analytics to accurately detect threats.
- Correlate related activities to prioritize incidents.
- Automatically parses and normalizes logs.
- Threat intelligence and support for STIX/TAXII.
- Integrates out-of-the-box with 450 solutions.
- Flexible architecture can be deployed on-prem or on cloud
- Highly scalable, self-tuning and self-managing database

radware

- Real-time network attack prevention protecting application infrastructure against network & application downtime
- application vulnerability exploitation
- Malware spread
- Information theft and more.
- Protects against known and emerging network attacks.
- **DefensePro** provides automated DDoS protection from fast-moving, high-volume, encrypted or very-short-duration threats and is part of Radware's attack mitigation solution. It defends against IoT-based, Burst, DNS and TLS/SSL attacks to secure organizations against emerging network multivector attacks, ransom DDoS campaigns, IoT botnets, phantom floods, and other types of cyberattacks.
- **AppWall** - Radware's Web Application Firewall (WAF), ensures fast, reliable and secure delivery of mission-critical Web applications and APIs for corporate networks and in the cloud. AppWall is an NSS recommended, ICSA Labs certified and PCI compliant WAF that combines positive and negative security models to provide complete protection against web application attacks, access violations, attacks disguised behind CDNs, API manipulations, advanced HTTP attacks (slowloris, dynamic floods), brute force attacks on login pages and more.

tripwire

- File Integrity Monitor
- Vulnerability Management
- Event Monitoring

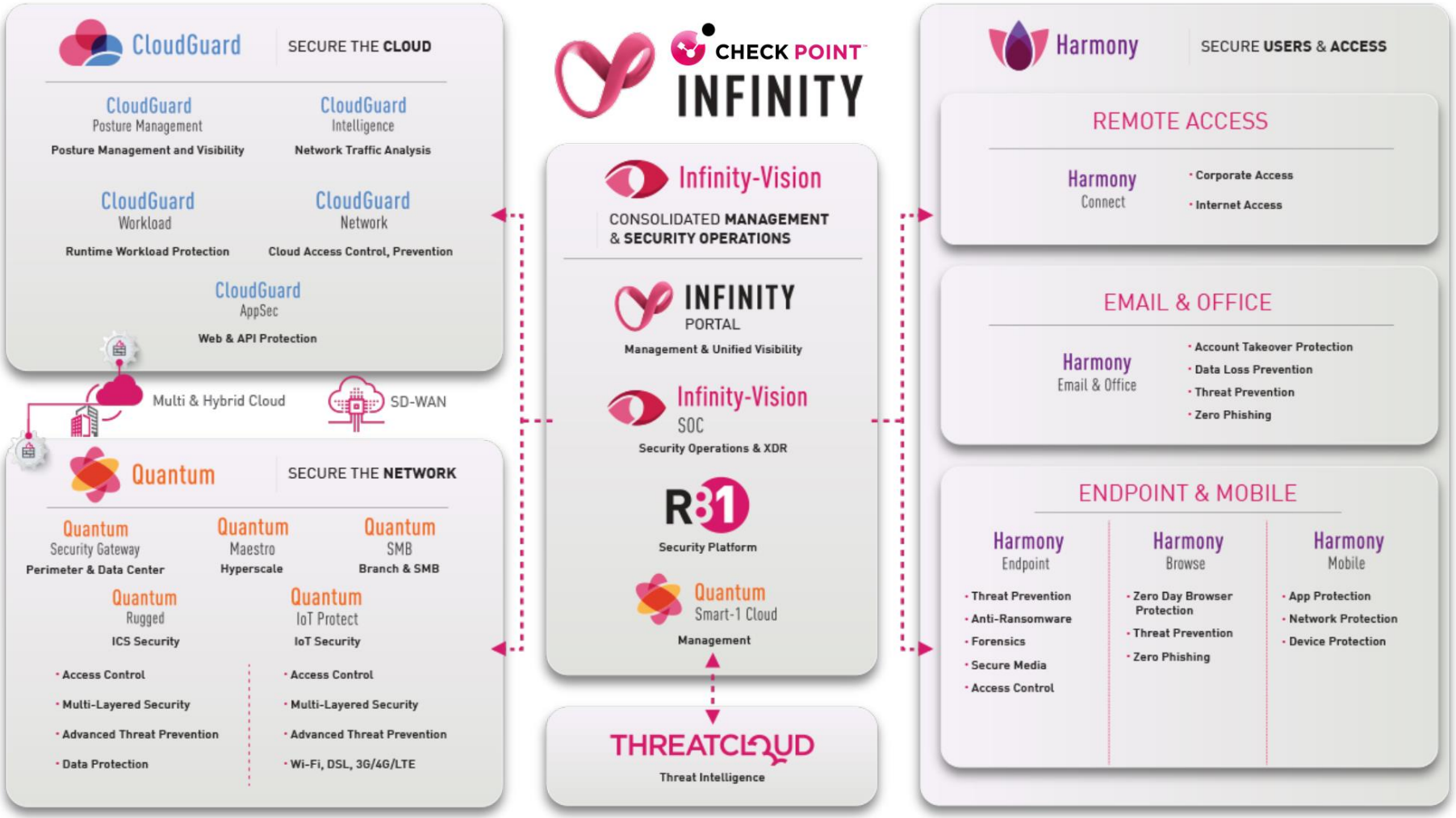
SecuPi

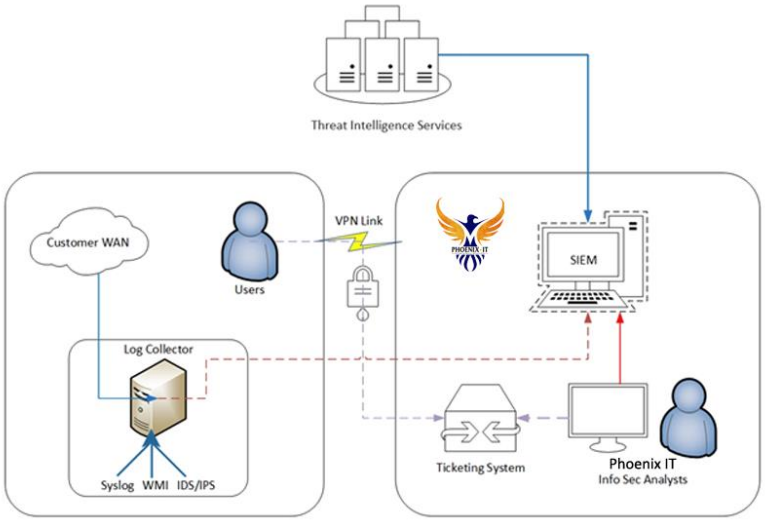
- Discovery Integration
- User behavior Analytics
- Monitoring & Auditing
- Dynamic Consent Controls
- Dynamic Data Masking
- Soft/hard Deletion

Guardicore

- Micro Segmentation
- Visualizing Infrastructure & Risk
- Accelerating Threat Detection & Response

CHECKPOINT INFINITY ARCHITECTURE AND SERVICES





Cloud-Based, Shared Environment

This service model is based on the fact that most customers do not want to own or manage their own SIEM or Security Logging infrastructure. A Log Collecting appliance (or several, depending on data load and redundancy needs) is sent to the customer and log sources are then pointed to send their logs to it. This approach minimizes the cost by sharing the expensive SIEM appliance between the outsourcer and its customers. In extremely cost sensitive cases, it is possible to minimize costs even further by doing away completely with the Collector Appliance and using software agents instead. This may impact log collection reliability. Please note that the diagram shown here only has 1 Collector appliance, but it is possible that redundancy and the log quantity require several Collector appliances

Pros: Lowest Cost Solution Minimal setup on the customer side

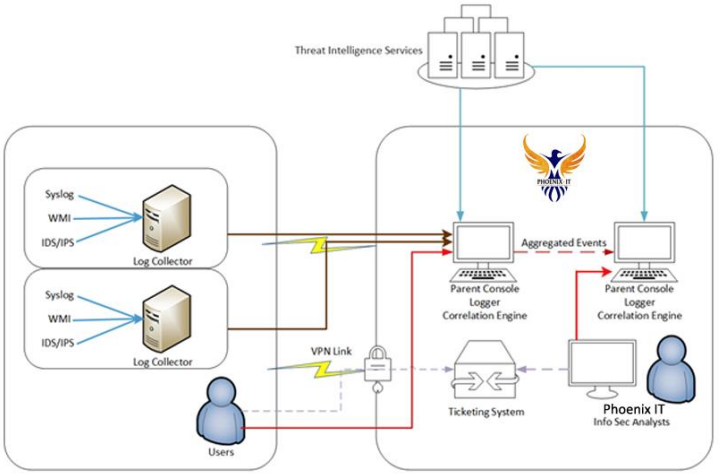
Cons: No visibility into the actual monitoring or SIEM Difficult or limited customization Raw Data is sent to a third party (compliance issues?) Data isolation between customers requires trust (security and compliance issue?)

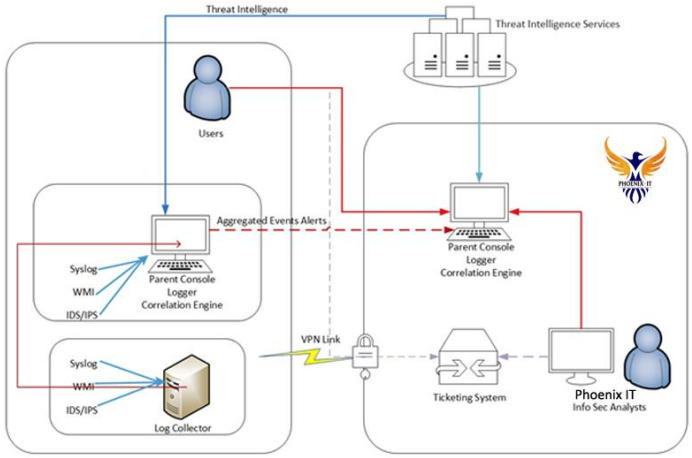
Cloud-Based, Virtual Private Environment

This second cloud-based architecture is similar to the first one but involves a more dedicated (usually virtual) infrastructure on the Managed Services Provider's cloud. This allows for better security, isolation, customization and visibility than the fully shared environment. Of course, this comes at an increased cost.

Pros: Low Cost Solution (but more expensive than fully Shared Environment) Very little setup on the customer side Leverage MSSP for maintenance and upkeep of the infrastructure Elastic infrastructure, MSSP can allocate more compute resources on-demand Increased visibility, security and data isolation

Cons: More expensive than shared environment Some Security and Compliance issues may still remain depending on actual requirements





On Premise SIEM, only metadata sent out to MSSP

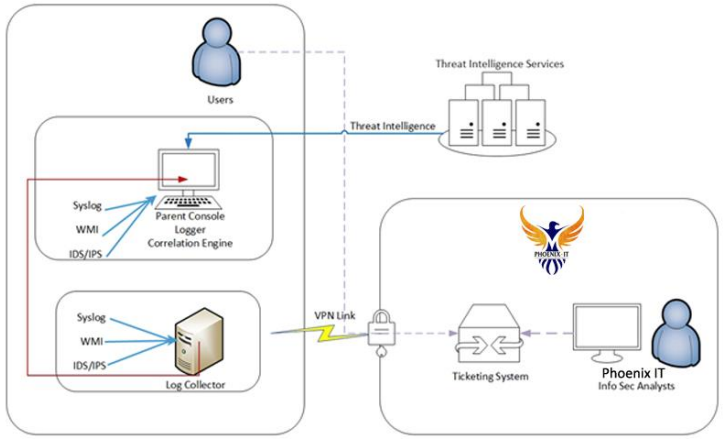
This monitoring architecture involves the customer having an on-premise logging infrastructure that is compatible with one of the MSSP's platforms. This infrastructure provides flexibility in terms of ownership. Many organizations will prefer to own their infrastructure while others prefer some other form of operational expense with the cost of the SIEM included as part of the service. This model is usually flexible in terms of management of the SIEM itself. The SIEM can be managed by the MSSP, Co-Managed between the MSSP and the client as well as fully customer managed.

Pros: Full (or shared) control over the SIEM Full Visibility into process, configurations Easier migration to another service provider/MSSP Logs Stay on-premise, can be spread out per jurisdiction for compliance (EU, Asia, etc.)

Cons: Increased infrastructure, configuration and maintenance cost Setup and integration time can be long and complicated

On-Premise SIEM, MSSP remotely connects

This engagement model is most often used with customers with extremely strict, detailed compliance requirements. In this case, the customer implements its own monitoring infrastructure and chooses not to send any data or metadata to the MSSP. All data resides under customer control. The MSSP connects remotely and exclusively uses customer equipment in order to perform its services. Since the scalability of the model is limited and the MSSP needs to customize all of its practices and procedures for a specific customer, this is by far the most expensive engagement model of all the listed options. Conversely, this is by far the most control any organization can attain over its security monitoring program. Compliance and governance issues are negated as the infrastructure and service is tailored exactly to customer needs. Given its lack of scalability, not all MSSPs are interested in supported this model.



Pros: Best Visibility Best Security and Compliance Most Control and Flexibility

Cons: The Most Expensive option Complex implementation Difficulty to obtain this type of service Phoenix IT Lanka in collaboration with SecureOps offers all of the above Security Monitoring engagement models as well as other customized solutions

REFERENCE CUSTOMERS

PHOENIX IT LANKA (PVT) LTD

Reg No: PV 00240684

10/C, Keppetipola Mawatha, Kolonnawa, Sri Lanka

sales@phoenixit.lk

(+94) 713 386 548

www.phoenixit.lk