Silver leaf

Cybersecurity Solutions

Agenda

- What is Cyber Security
- Next-Generation Firewall
- Data Loss Prevention (DLP)
- Web Application & API Protection
- End Point Detection & Response (EDR)
- Multi Factor Authentication (MFA)
- Secure Remote Access
- Load Balancing Solutions
- VAPT Assessments
- Cloud Access Security Broker (CASB)
- Network Access Control (NAC)
- Security Information & Event Management (SIEM)
- Contact Us

What is Cybersecurity | An Introduction

Cybersecurity is a set of Solutions & Strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. It maintains the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers.

What are the threats to Cybersecurity?

Threats to Cybersecurity can come in different forms. A common threat is malware, or malicious software, which may come in different variations to infect network devices, including:

- Ransomware
- Spyware
- Viruses

Types of Cybersecurity Solutions:

- Network Security
- Endpoint Security
- Cloud Security
- Application Security
- Internet Security

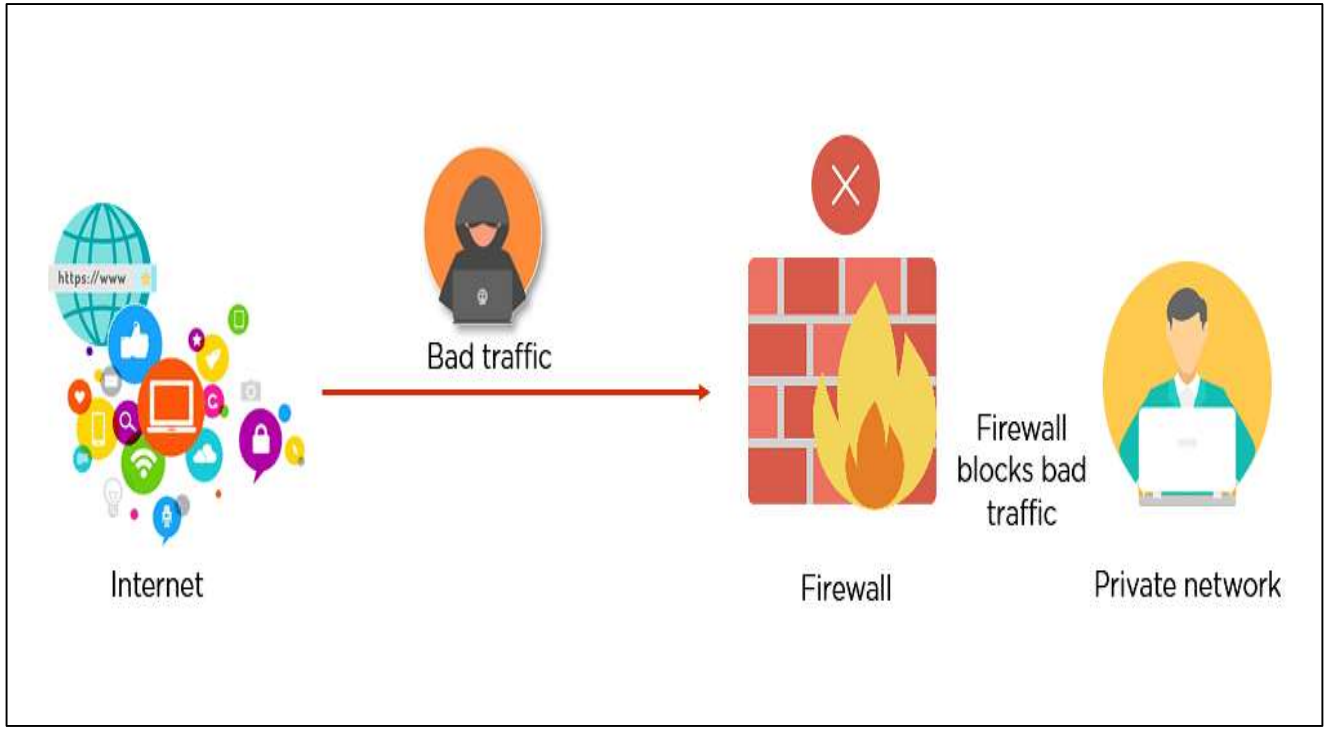
Next-Generation Firewall (NGFW)

Next-Generation firewall (NGFW) is an advanced network security device that combines the features of traditional firewalls with additional capabilities to provide enhanced security and threat protection.

NGFWs are designed to defend against modern, sophisticated threats and provide more granular control over network traffic.

Features:

1. Application Awareness
2. Intrusion Prevention System(IPS)
3. User Identification and Control
4. Content Filtering
5. Advanced Threat Protection
6. VPN Support
7. Centralized Management and Reporting



Strategic OEM –

CHECK POINT

Other OEMs:

Fortigate Cisco SonicWALL

Net Gear Palo Alto Sophos

Data Loss Prevention(DLP)

Data loss prevention (DLP) is a set of techniques and technologies designed to prevent the unauthorized or accidental loss, leakage, or theft of sensitive data from an organization. It involves identifying, monitoring, and protecting sensitive data throughout its lifecycle, both within the organization's network and outside of it

Features:

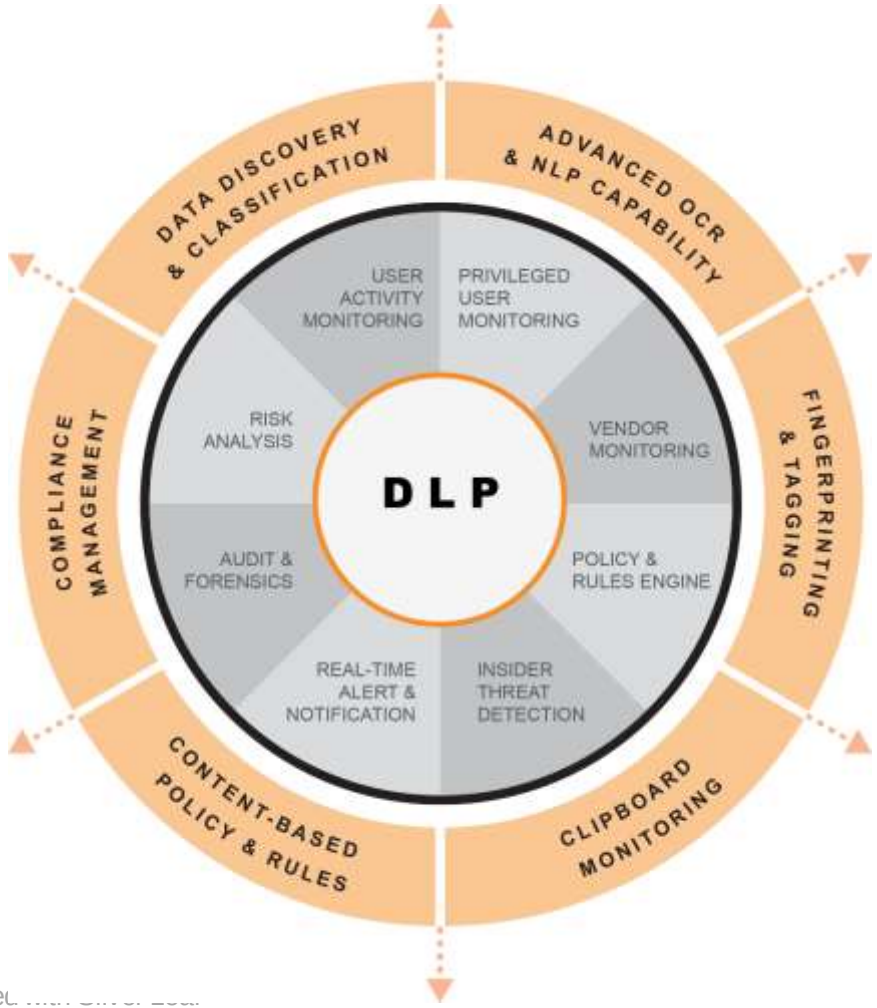
1. Data Discovery and Classification
2. Data Monitoring and Control
3. Policy Enforcement
4. Endpoint Protection
5. Incident Response and Reporting

Strategic OEM:

FORCEPOINT

Other OEMs:

- ✓ TrendMicro
- ✓ Trellix
- ✓ Symantec
- ✓ Sophos



Web Application & API Protection

Web Application and API Protection (WAAP) is a set of security measures and technologies designed to safeguard web applications and APIs from various threats and vulnerabilities. It involves implementing security controls and best practices to mitigate risks, protect data, and ensure the availability and integrity of web applications and APIs.

Features:

1. Web Application Firewall (WAF)
2. API Security
3. Bot Protection
4. Secure Development Practices
5. Threat Intelligence and Monitoring
6. Logging, Auditing and Compliance

Strategic OEM:

Other OEMs:

- ✓ Cloudflare Spectrum
- ✓ Fortinet Forti Web
- ✓ Imperva WAF
- ✓ AWS WAF

End Point Detection & Response (EDR)

Endpoint security, or endpoint protection, is the cybersecurity approach to defending endpoints – such as desktops, laptops, and mobile devices – from malicious activity.

It is a centralized management console from which administrators can connect to their enterprise network to monitor, protect, investigate and respond to incidents.

Features -

- Application control
- Device Control
- Web Protection
- Data Loss Prevention
- Endpoint Detection and Response

Strategic OEM –

CROWDSTRIKE

Other OEM -

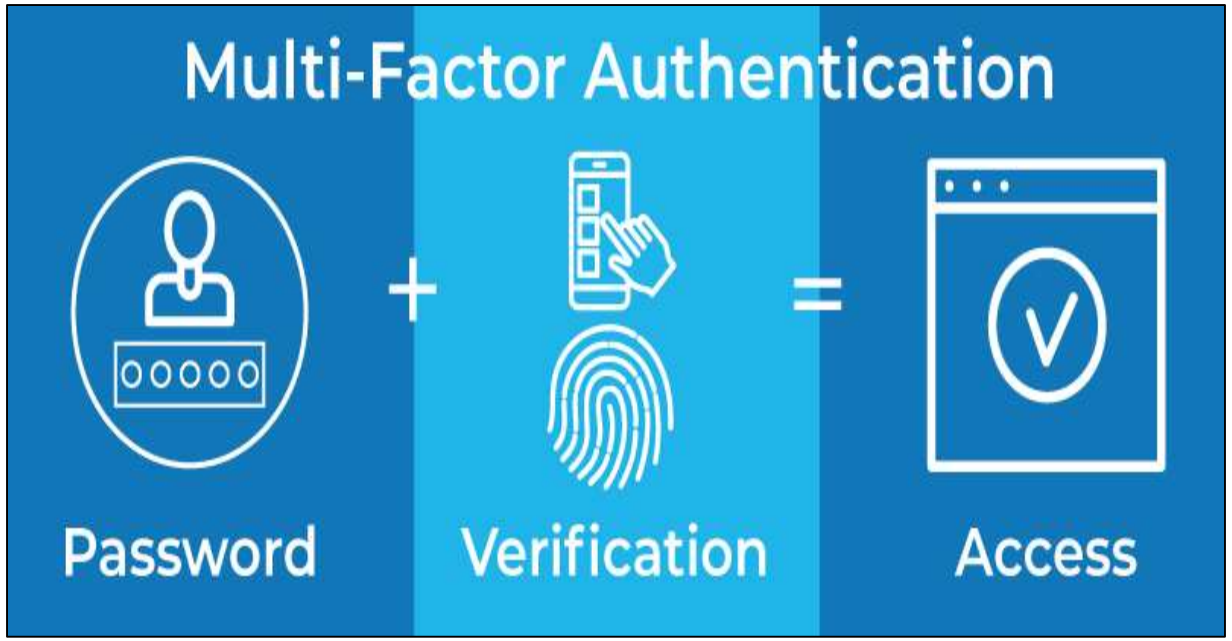
- ✓ Trend Micro Apex One
- ✓ McAfee Endpoint Security
- ✓ Broadcom Symantec Endpoint Security
- ✓ Checkpoint Harmony Endpoint
- ✓ FireEye Endpoint Security
- ✓ SentinelOne Singularity XDR

Multi Factor Authentication

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.

Features:

- Push notifications
- SMS notifications
- One-time passwords
- Email notifications



Strategic OEM:

accops

Other OEMs:

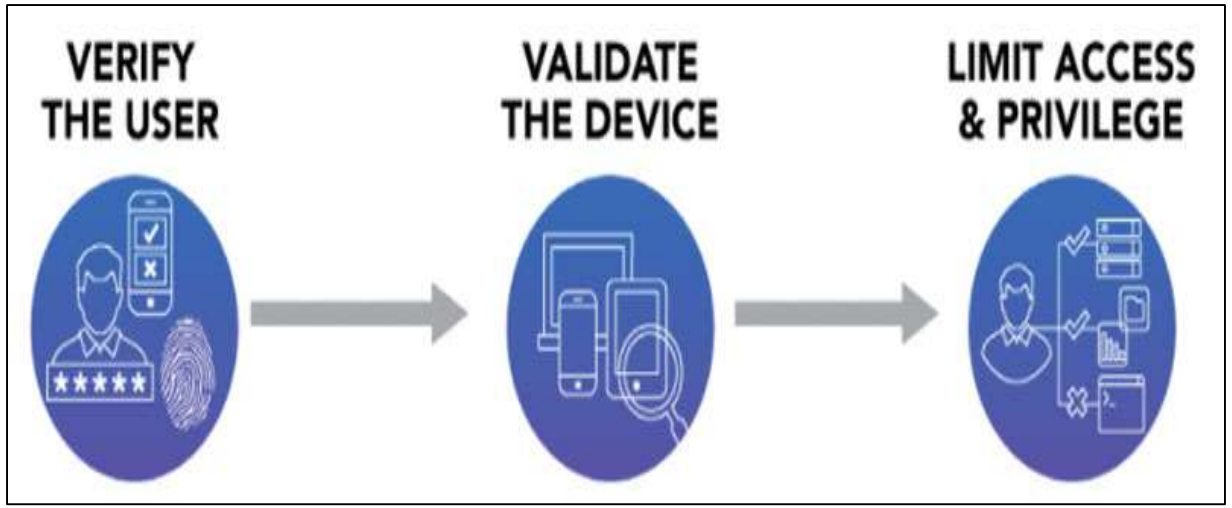
- ✓ RSA SecurID Access
- ✓ Salesforce Authenticator
- ✓ Azure Multi-Factor Authentication
- ✓ Forti Authenticator
- ✓ Okta Adaptive Multi-factor Authentication

Secure Remote Access

Zero Trust Network Access (ZTNA) is a category of technologies that provides secure remote access to applications and services based on defined access control policies.

Features:

- Secure Remote Access
- Single Sign On
- Strong Endpoint Control
- Device Audit/Detailed Users
- User Activity Logs
- MFA



Strategic OEM –

accops

Other OEM:

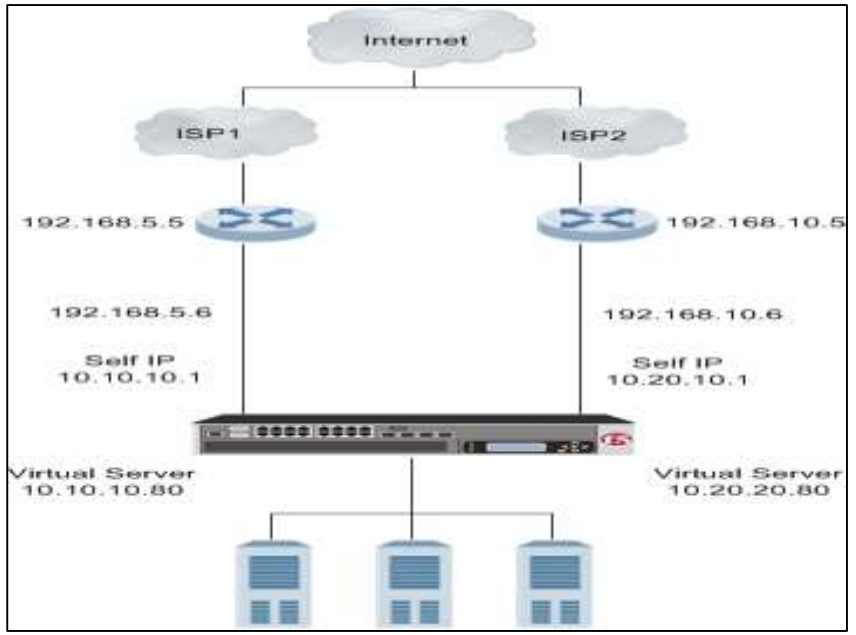
- ✓ Palo Alto
- ✓ Zscaler
- ✓ Akamai
- ✓ Perimeter 81

Load Balancing Solutions

A load balancer is a device that acts as a reverse proxy and distributes network or application traffic across several servers.
Load balancers are used to increase capacity (concurrent users) and reliability of applications.

Features:

- Flexibility
- Scalability
- Redundancy
- Reduced Downtime



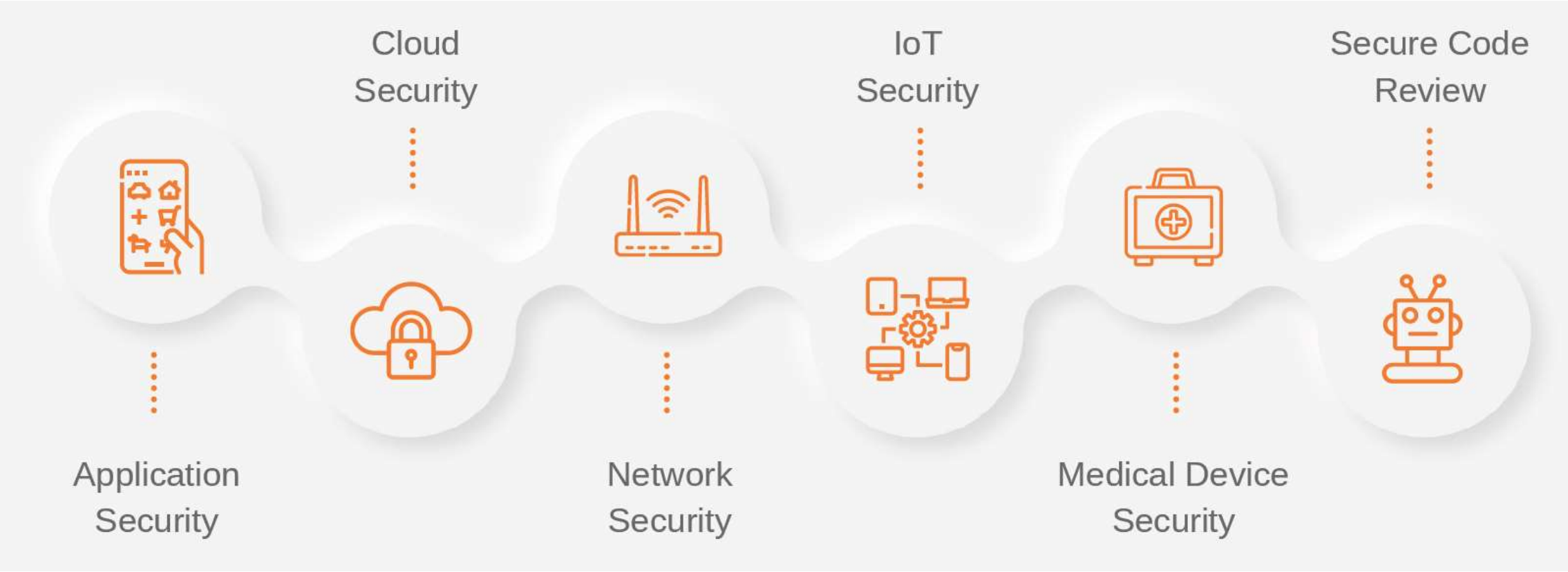
Strategic OEM:

Other OEM:

- ✓ Azure Application Gateway
- ✓ Kemp Load Master
- ✓ Azure Traffic Manager
- ✓ Citrix ADC
- ✓ Barracuda Load Balancer ADC
- ✓ Radware Alteon

VAPT Assessment

Under our VAPT service, we test complete IT infrastructure (Mobile/Web App, Servers, Networks, Desktops/Laptops, APIs, CRM/ERP) of an organization. We recommend solutions against all the vulnerabilities and do re-testing after the organization's engineering team patches all those vulnerabilities.



VAPT Assessment

We follow the industry's best security standards like:

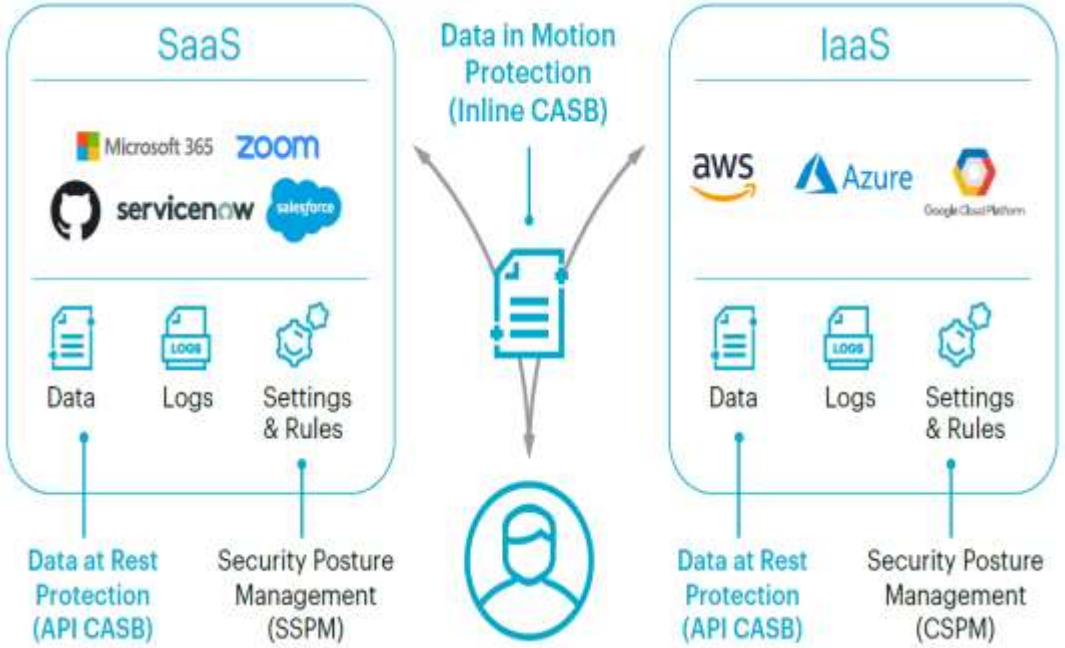
OWASP10 ------ SANS25 ------ OSSTMM ------ NIST SP800-115 ------ CERT-in ------ CIS Benchmark

Cloud Access Security Broker (CASB)

With CASB, Organizations can confidently adopt cloud applications and services – without sacrificing security. Manage the unintentional or unapproved movement of sensitive data between cloud app instances and in the context of app risk and user risk with Netskope's industry leading cloud security solution

Safely enable users anywhere

- ✓ Eliminate blind spots: With Patented Netskope Cloud XD™, get deeper understanding to quickly target and control activities across thousands of cloud (SaaS and IaaS) services and millions of websites.
- ✓ Secure managed and unmanaged cloud services: Secure managed cloud services like Microsoft 365, GSuite and AWS, while safely enabling unmanaged, business-led cloud services without the need for blocking.
- ✓ Guard sensitive data with award-winning DLP: Netskope DLP and introspection enables the protection of sensitive content that matches DLP profiles. Includes pre-defined DLP profiles for regulatory compliance.
- ✓ Stop elusive cloud threats and malware: Protect against malware, advanced threats, and cloud-enabled threats with anti-malware, sandboxing, ML analysis, and more.



Strategic OEM –

netskope

Other OEMs –

- ✓ Zscalar
- ✓ Forcepoint
- ✓ Palo Alto

Network Access Control (NAC)

Network Access Control (NAC) is a security approach that enforces policies and controls to manage and secure access to network resources. It helps organizations ensure that only authorized and compliant devices and users can connect to their networks, while providing visibility and control over network access.

Features -

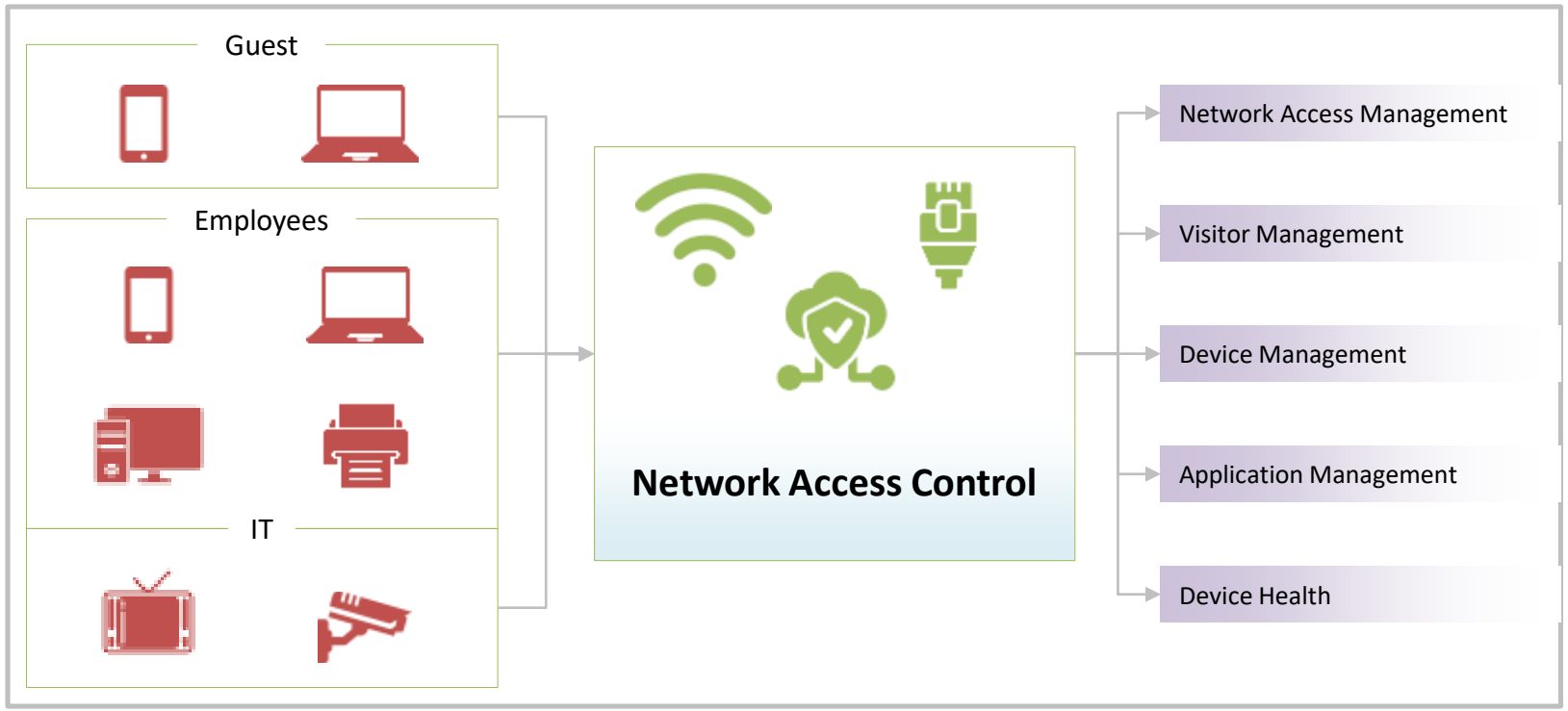
- Dot1x Authentication
- Device Profiling
- Device Health Check
- Policy based Access Control
- Guest Access Control

Strategic OEM –

aruba
a Hewlett Packard Enterprise company

Other OEMs -

- Forescout
- Fortinet
- Cisco



Security Information & Event Management (SIEM)

Security Information and Event Management (SIEM) is a centralized solution for security management that involves the collection, analysis, and correlation of security events and log data from various sources within an organization's network. SIEM systems provide real-time monitoring, threat detection, incident response, and compliance reporting capabilities.

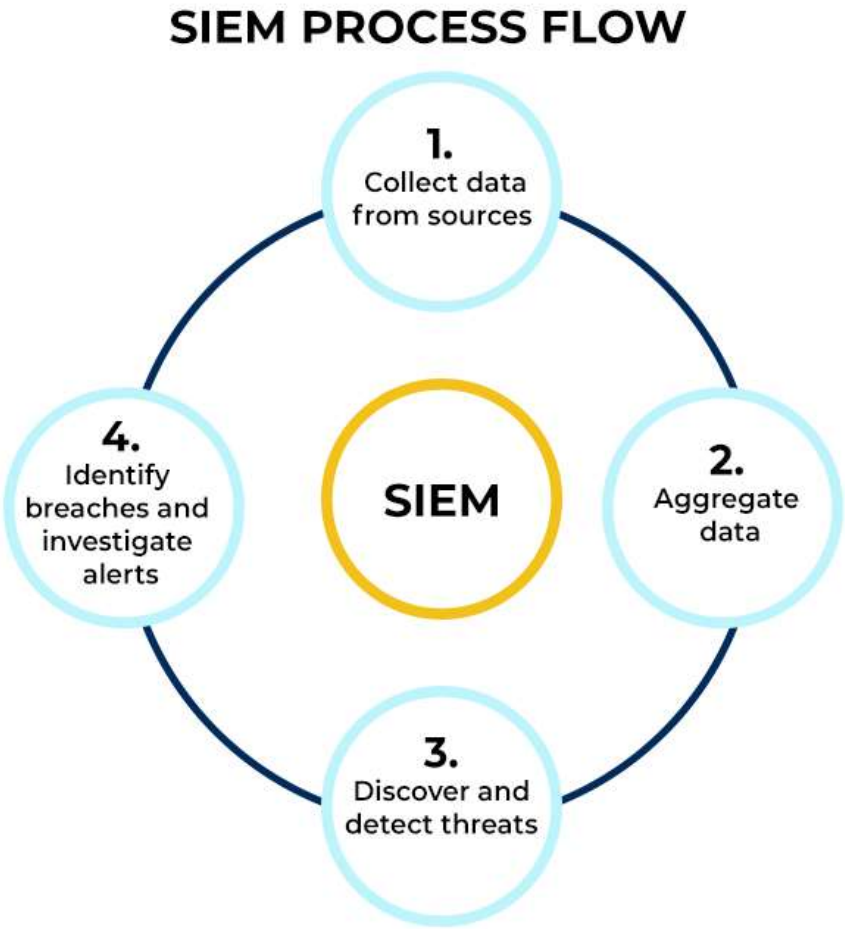
Features -

- Log Collection and Aggregation
- Event Correlation and Analysis
- Threat Detection and Alerts
- Incident Response and Workflow Management
- Forensic Analysis and Investigation
- Compliance and Reporting
- Integration and Data Enrichment

Strategic OEM: Trellix

Other OEMs:

- ✓ Qradar
- ✓ Splunk
- ✓ Sumologic



Contact Us @ info@silverleafsolutions.com

Gurgaon (HQ)	*510, Vipul Trade Center, Sector 48, Sohna Road, Gurgaon, Haryana, India 122018*
Mumbai	*C-1404 , 14th Floor, Kailas Business Park, Hiranandani Link Road, Vikhroli (West), Mumbai, India 400079*
United States	*Silver Leaf Solutions LLC* *1467 Onondaga PL, Fremont, CA 94539*
Australia	*Silver Leaf Solutions Australia Pty Ltd* *3 Corella Place, Cattai, NSW 2756, Australia*
Singapore	*Silver Leaf Solutions Pte. Ltd, 105 Cecil Street, #15-02 The Octagon, Singapore - 069534*
Germany	*Silver Leaf Solutions GmbH, c/o Paschen Rechtsanwailte, Kaiserin-Augusta-Allee 113, 10553 Berlin*