SEMOR

Next-Generation Cybersecurity
Focus to Secure

GUARDINSIGHT

Security, Events, Monitoring, Orchestration, and Response

Overviews are delivered in a common and consistent framework, canvassing the organization's in-scope systems in a logical way.

GUARDINSIGHT continuous around-the-clock security monitoring. Monitors the entire extended IT infrastructure – applications, servers, system software, computing devices, cloud workloads, and the network - 24/7/365 for signs of known exploits and for any suspicious activity.

The core monitoring, detection, and response technology monitors and aggregates alerts and telemetry from software and hardware on the network in real time, then analyze the data to identify potential threats.

Log data generated by every networking event – is a subset of monitoring that's important enough to get its own paragraph. While most IT departments collect log data, it's the analysis that establishes normal or baseline activity and reveals anomalies that indicate suspicious activity. In fact, many hackers count on companies not always analyzing log data, which can allow their viruses and malware to run undetected for weeks or even months on the victim's systems.

Threat detection is the indication of actual cyber threats and hacker exploits from the false positives – and then triages the threats by severity. Our solutions include artificial intelligence (AI) that automates these processes and 'learns' from the data to get better at spotting suspicious activity over time.

Incident response. In response to a threat or actual incident, to limit the damage.
Actions can include:

- Root cause investigation, to determine the technical vulnerabilities that gave hackers access to the system, as well as other factors (such as bad password hygiene or poor enforcement of policies) that contributed to the incident
- Shutting down compromised endpoints or disconnecting them from the network
- Isolating compromised areas of the network or rerouting network traffic
- Pausing or stopping compromised applications or processes
- Deleting damaged or infected files
- Check with Microsoft AD for an email account and passwords for internal and external users.
- Integrating with XDR solutions enable automate and accelerate these and other incident responses.

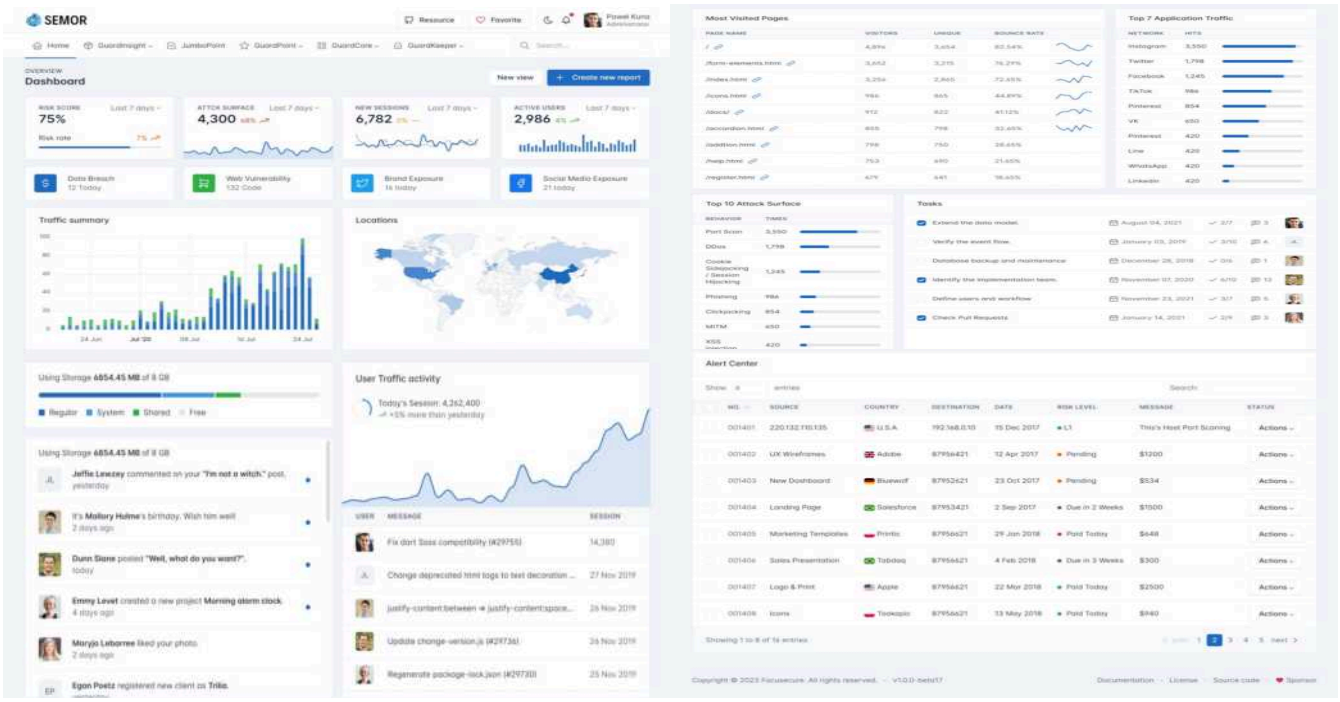
It's important that reports to executives convey as much information as clearly and quickly as possible.

- Key Findings
- Security Risk Monitoring Summary
- Cyber Incident Summary
- Cyber Threat Summary
- Remediation Recommendations

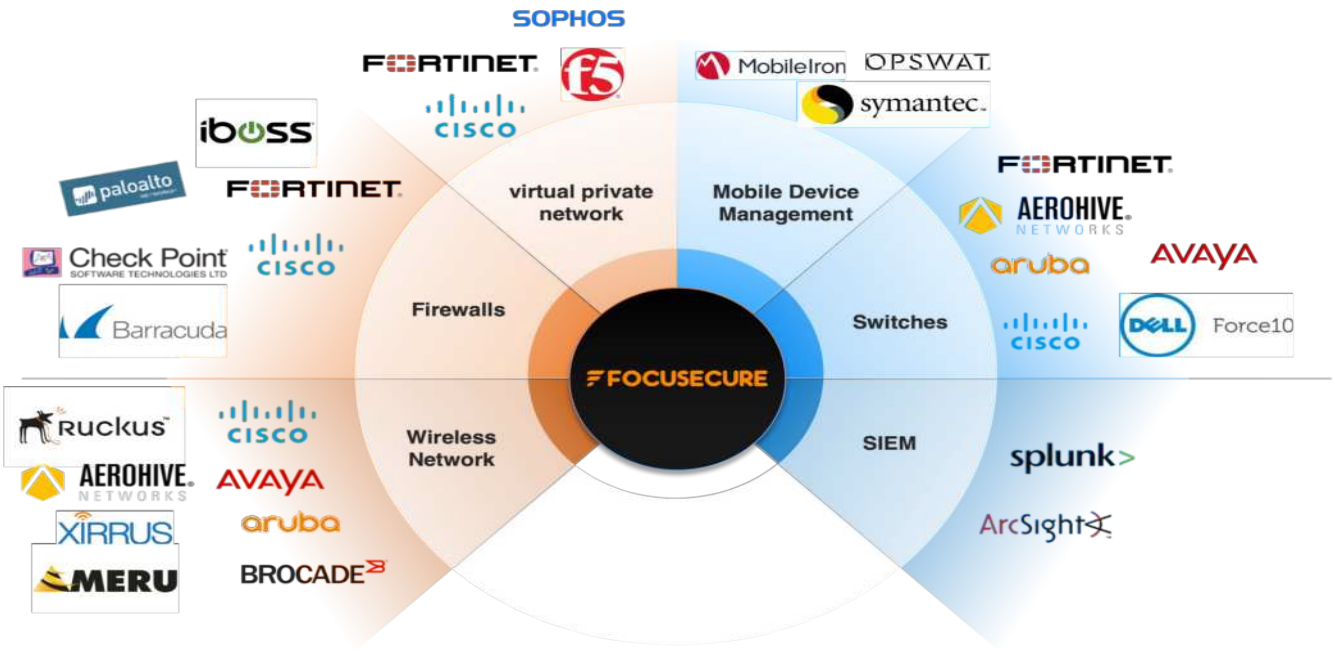
Elastic Correlation Analysis Reports

- Manager Layer – Overall key findings and summary
- Analysis Layer – Real-Time analysis dashboard
- Operation Layer – Maintenance index dashboard
- Maintenance Layer – Day/Month/Quarter reports

Monitoring and Analysis



Enriching and Integrate Your Existing Infrastructure



SEMOR

Agentless
Gain a unified, real-time inventory of network-connected assets including their security and risk posture.

Accurate-Effective
Automatic device detection to classify every device to gain context for building proactive security and compliance policies.

Efficient
Gain real-time assurance that security tools and compliance controls are working properly.

We deliver unparalleled insight into every effectively connected asset through deep integration into your environment from a small to a large heterogeneous network fabric.

- Discover your entire asset inventory that reveals coverage gaps across your digital terrain, providing a real-time view of your attack surface
- Automate asset classification and build comprehensive profiles with threat intelligence, including known risks and vulnerabilities.
- A captive portal for registration and remediation.
- Continuously assess an asset's status, risk posture, and policy compliance without needing an agent to be installed, which is essential for protecting IoT, IoMT, and OT assets.
- Multiply your forces while minimizing human error with automated reporting on compliance posture and cyber-risk exposure, letting you focus your efforts on what matters most.

DISCOVER

See devices the instant they connect to the network Continuously monitor as transient devices come and go Get a real-time asset inventory that uncovers visibility gaps.

IDENTIFY

Identify diverse types of IT, IoT, IoMT, and OT devices Harness the power of Device Cloud for full device context Improve auto-classification efficacy, coverage, and speed.

ACCESS

Identify security exposures and compliance gaps. Assess adherence to internal and external mandates and gain situational awareness of cyber and operational risk.

Customize discovery and monitoring techniques for your environment

Leverage the flexibility of active and passive monitoring techniques across wired, wireless, VPN, and virtual/software-defined networks so you can avoid disrupting assets that are sensitive to active scanning techniques.

Guard Point Solves For:

- Visibility gaps are caused by siloed teams and disparate security tools.
- Operational and business risks due to error-prone manual processes.
- Incomplete device intelligence hinders the execution of security policies.
- Security gaps when agent-based tools are not up to date or functioning properly.
- Undetected rogue devices or MAC spoofing.
- Non-compliance can quickly emerge between point-in-time scans.

DISCOVER

Real-time deep discovery

- Physical and SDN infrastructure including switches, routers, wireless access points, and controllers
- Laptops, tablets, smartphones, BYOD/guest systems, work-from-home devices
- IoT assets in campus networks, data centers, branches, remote sites, and edge networks
- Public and private cloud instances across Amazon Web Services, Microsoft Azure, and VMware environments
- Operational technology (OT) and industrial control systems including HMIs, SCADA, PLCs, building management systems (BMS) and building automation systems (BAS)
- IoMT devices in hospitals and healthcare delivery networks (HDO) like infusion pumps and diagnostic equipment

ACTIVE TO INFRASTRUCTURE

Network infrastructure polling

Public/Private cloud integration
- VMware
- AWS
- Azure
- AliCloud

Query directory services (LDAP)
Query web applications (REST)
Query databases (SQL)

PASSIVE TO ASSET

SNMP traps

SPAN traffic Flow analysis
- NetFlow
- Flexible NetFlow
- IPFIX
- sFlow

DHCP requests
HTTP user-agent
TCP fingerprinting
Protocol parsing
RADIUS requests

ACTIVE TO ASSET

Agentless Windows inspection
- WMI
- RPC
- SMB

Agentless macOS, Linux inspection
- SSH

NMAP
SNMP queries
HTTP queries

IDENTIFY

Intelligent auto-identification

Implementing security policies without full asset context can lead to undesirable outcomes that may put operations at risk. FOCUSECURE, GUARDPOINT has one of the largest repositories of device intelligence gathered from over 80 million devices and automatically provides a comprehensive context for every connected asset. Our multidimensional identification taxonomy identifies device function and type, operating system and version, and vendor and model.

This includes:

- More than 1,500 different operating system versions.
- Over 8,400 different device vendors and models.
- Healthcare devices from over 410 leading medical technology vendors.
- Thousands of industrial control systems and automation devices are used across manufacturing, energy, oil and gas, utilities, mining, and other critical infrastructure industries.

Auto-identification

The world's largest repository of asset intelligence that provides the most complete and accurate understanding of asset risk within any organization.

GUARDPOINT

Flexible Authentication | High Availability | Auto Registration

IDENTIFY DEVICE

Function	Operating System	Authentication	Vendor
➢ Wireless Access Point ➢ Tablet ➢ Printer ➢ VoIP Server ➢ HVAC System ➢ Point of Sale ➢ Medical Devices	➢ Windows ➢ Windows Server ➢ Android ➢ IOS ➢ MACOS ➢ Linux	➢ LDAP ➢ RADIUS ➢ OAUTH2 ➢ SAML	➢ Palo alto ➢ Fortinet ➢ Checkpoint ➢ Barracuda ➢ Cisco ➢ Ruckus ➢ Aruba ➢ MobileIron ➢ Splunk

ACCESS

Agentless posture assessment

Discovers assets and immediately assesses the configuration, posture, and risk indicators of the asset to understand whether they adhere to compliance mandates and security policies. Policies can help better quantify risk by assessing compliance conditions such as:

- Is the security software installed, operational, and up-to-date with the latest patches?
- Is the asset critical to business operations?
- Are any assets running unauthorized applications or violating configuration standards?
- Are assets - especially IoT, IoMT, and OT systems - using default or weak passwords?
- Have rogue assets been detected, including those spoofing legitimate assets?
- Which of your connected assets are most vulnerable to the latest threats?

MONITOR

Compliance Insights

Gain actionable insights from out-of-the-box dashboards that quickly pinpoint, prioritize, and proactively mitigate risks across your digital terrain. Customizable dashboard views help security analysts and SOC teams

- Detection of Abnormal Network Activities
- Proactive Vulnerability Scans
- Security Agents
- Windows Management Instrumentation (WMI)
- Statement of Health
- Remediation Through a Captive Portal
- Isolation of Problematic Devices

EXTENSIBLE / EASILY CUSTOMIZABLE

Guard Point has a couple of extension points where you can override Guard Point's default behaviour with a little bit of Perl code. The API has been designed to be easy to understand with only a couple of high-level entry points. Several examples are already there in the source code but commented. Also, when upgrading, Guard Point doesn't replace the files in the extension points, this way you keep your modified behaviour on upgrades.
The captive portal templates are also easily customizable with HTML and CSS knowledge. They are built using Perl's Template Toolkit.

ADMINISTRATION

Command-Line and Web-based Management

Web-based and command-line interfaces for all management tasks. Web-based administration supports different permission levels for users and authentication of users against LDAP or Microsoft Active Directory.

EXPIRATION

The access duration to the network can be controlled with configuration parameters. It can either be an absolute date (eg. "Thu Jan 20 20:00:00 EST 2011"), a window (eg. "four weeks from first network access"), or as soon as the device becomes inactive. On expiration registered devices become unregistered. With a little customization, it is also possible to do this on a device category basis. Expiration can also be manually edited on a per-node basis.

PKI AND EAP TLS SUPPORT

Guard Point does support EAP-TLS for certificate-based authentication. Guard Point provides a small PKI solution that can be used to generate a TLS certificate for each device or each user. Guar dPoint also integrates with Microsoft's PKI solution. Guard Point will make use of the Simple Certificate Exchange Protocol (SCEP) to talk to
Microsoft's Network Device Enrolment Service (NDES) to create the appropriate certificate during an endpoint onboarding process.

DEVICE MANAGEMENT

Guard Point provides device management and provisioning capabilities through its integration with complementary solutions. These solutions which normally include an agent, allow compliance checks, settings being pushed, and more on endpoints connected to your network. Guard Point can make sure the agents (or clients) are installed during the registration process, and afterward for every new connection. Guard Point supports the following solutions:

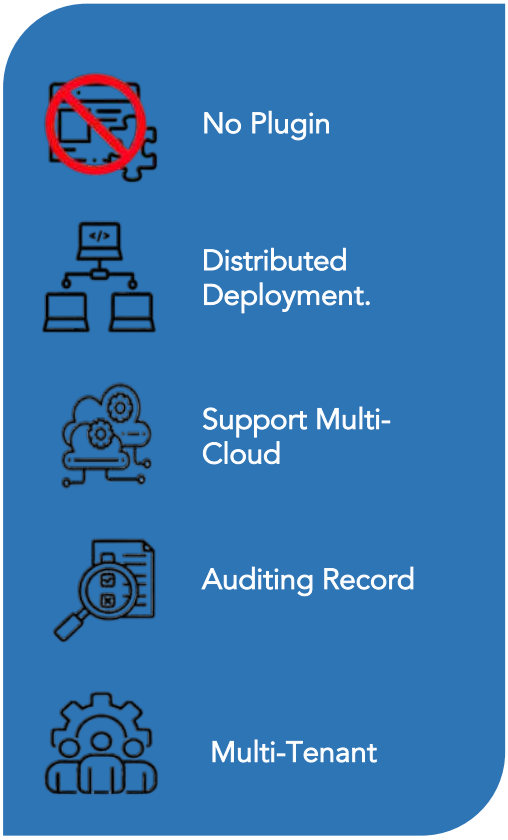
- MobileIron
- OPSWAT Metadefender Endpoint Management
- Symantec SEPM
- Guard Point provides its own configuration agents for Android, Apple, and Windows-based endpoints.

FLOATING NETWORK DEVICES

A Floating Network Device is a Switch or Access Point (AP) that can be moved around your network and that is plugged into access ports. Once configured properly, Guard Point will recognize your Floating Network Devices and will configure the access ports appropriately usually allowing multiple VLANs and more MAC addresses. At this point, the Floating Network Device can also perform network access through Guard Point or not. Once the device is disconnected Guard Point will then re-configure back to its original configuration.

UNIQUE POINT

- GUARDPOINT offer:
  - Multiply vendor Integration
  - Intrusion Detection
  - Full integration with MDM Solution
  - IDS Reporting
  - Vulnerability Reports



Our Privileged Access Management (PAM) Complying with the 4A Protocol of Operation and Security Auditing, with 4A required, We offer a full-function platform with security and audit checks to help users/service vendors to maintain the system/service well and all system/service with lower risk impact from any direct connection/attack.

- Controls, Manages, and Audits remote privileged access to critical IT systems by authorized employees and third-party vendors. No VPN is required.
- Provides visibility and control over access to sensitive and business-critical systems and data, including cloud infrastructure, and web/thick application.
- Ensuring employees, third-party vendors, and other insiders don't have free access to systems while accessing the network remotely.
- Provide an appropriate level of access to each role needs to complete their work. This ensures privileges aren't left unchecked and prevents users from becoming entry points for attacks.

Privileged Remote Access gets you closer to a true zero-trust strategy by applying granular privileged access controls across the enterprise. This includes insider and outsider access. With a zero trust approach, ensure all access is appropriate, managed, and documented—regardless of the defined perimeter.

Our Privilege remote access provides visibility and control over third-party vendor access, and internal remote access, and extends access to important assets without compromising security.

Here are the features that make this possible.

- **Privileged Access Control**
  Enforce the least privilege by giving users the right level of remote access to do their jobs, not anything more.

- **Advanced Session Monitoring**
  Control and monitor sessions using standard protocols for RDP, VNC, HTTP/S, and SSH connections.

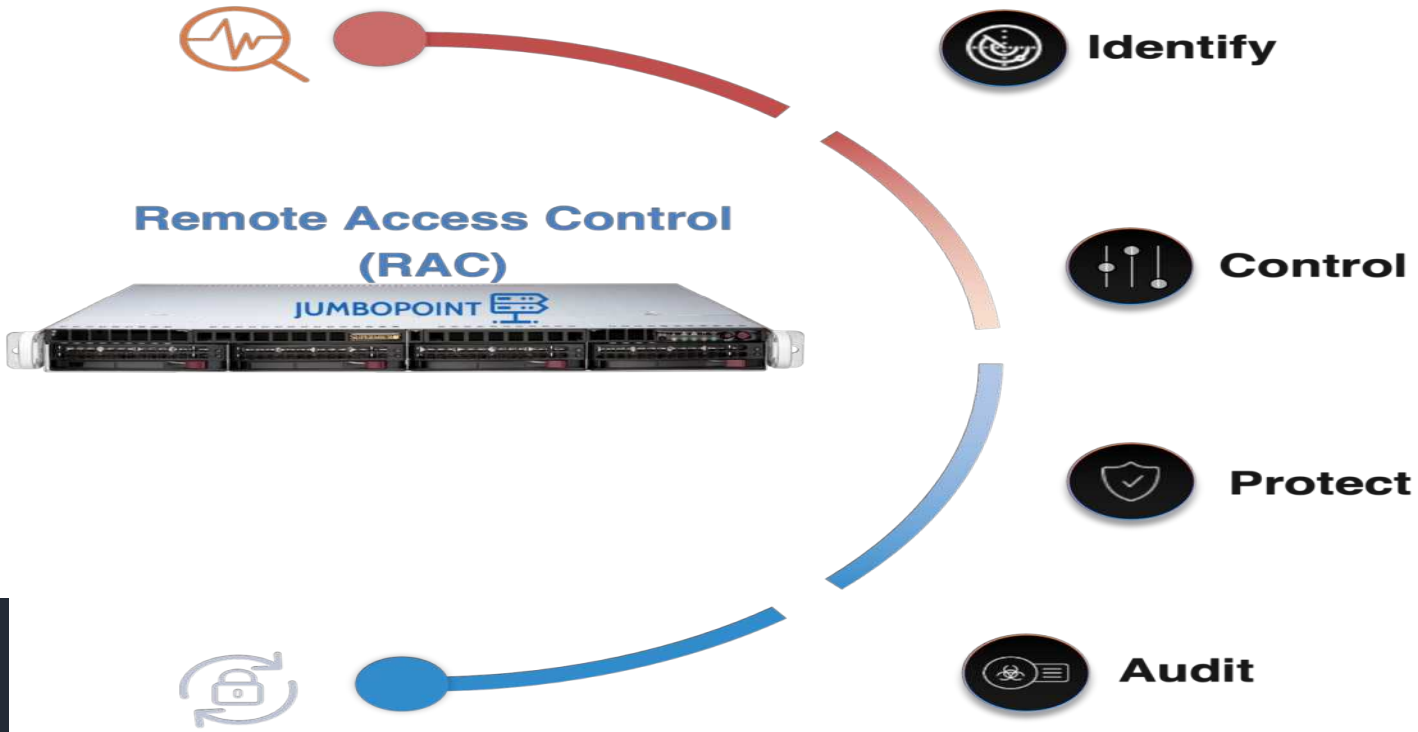
- **Attach Surface Reduction**
  Reduce attacks by consolidating the tracking, approval, and auditing of privileged accounts in one place and by creating a single access pathway.

- **Privileged Passwords Vaulting**
  Discover, manage and rotate privileged credentials for Windows platforms and seamlessly inject those credentials on demand.

- **Flexible Mobile & Web Consoles**
  Use mobile apps or web-based consoles to initiate access anytime, anywhere without circumventing security policies.

- **Audit & Compliance Features**
  Create audit trails, session forensics, and other reporting features by capturing detailed session data in real-time or post-session. Then, gain access to attestation reports to prove compliance.

- **Streamlined Privileged Session Management**
  Standardized, secure, and complete privileged session management solution that controls access to and from any platform in any environment. Eliminate manual credential check-in and check-out.



Our Privileged Remote Access controls access to critical systems and remote desktops without hindering the work privileged users need to perform.

You can closely define how users connect, monitor sessions in real time, and record every session for a detailed audit trail. Meanwhile, end users get a simple, easy-to-use console.

Here are the remote access features at the core of the solution.

- **Infrastructure Access for Devs & Engineers**

  Privileged Remote Access allows Developers and DevOps teams to access the systems they need to access to do their jobs. This functionality is enabled through a streamlined interface that promotes a protocol first and brings your own tool (BYOT) workflow.

  Not only can these users access existing systems, but APIs are available that allow instant access to ephemeral systems in multi-cloud environments.

- **Strong & Powerful Privileged Access Control**

  Enforce a policy of least privilege by giving users just the right level of access needed for their roles. For shared accounts, easily establish individual user accountability.

  Define what endpoints users can access, schedule when they can access them, and whitelist/blacklist applications for a comprehensive approach to privileged access. Control and monitor sessions via a secure agent or using standard protocols for RDP, VNC, Web, and SSH connections.

  Set authorization and notification preferences to be alerted when a user is accessing Privileged Remote Access. Administrators can use their mobile devices to approve requests and monitor access usage from anywhere.

- **Productivity Balanced Security**

  Privileged Remote Access increases user security without impacting daily workflows, and can deploy in just a few days. Automate processes with features like credential injection and SIEM integrations.

  Transfer files within the session, using the thick client or browser-based console.

- **Consolidated Access Pathways**

  Administrators and IT teams can consolidate the tracking, approval, and auditing of privileged accounts in one place.

  Require all connections to be brokered through a single access pathway. This substantially reduces the attack surface and provides a single list of authorized endpoints available for each user.

  Improve the end-user experience with the use of a single interface. Improve the service desk experience by reducing remote support ticket clutter with a new access request workflow.

- **Universal Cloud & Virtualization Security**

  Effectively manage privileged access to business assets that leverage web-based management consoles. This includes IaaS servers, hypervisor environments, and web-based configuration interfaces for core network infrastructure.

  - ❑ Amazon Web Services
  - ❑ MicrosoftAzure
  - ❑ Google Cloud
  - ❑ Alicloud
  - ❑ Huawei Cloud
  - ❑ VMWare xSphere
  - ❑ Citrix XenServer
  - ❑ Microsoft Hyper-V
  - ❑ Linux
  - ❑ MacOS

Singapore
8 Ubi Road 3 #03-27
Zervex Singapore 408538

Taiwan
No. 58, Section 3, Zhongshan North Road,
Zhongshan District, Taipei City 104 , Taiwan (R.O.C.)

Contact: +65 8819 6685
Email" ating@focusecure.com
Learn more at www.focusecure.com