Author: Mike Small & Martin Kuppinger

Buyer's Compass

Security Service Edge: Broadcom

Chapter 1

The Challenge

Digital transformation and cloud-delivered services have led to a tectonic shift in how applications and users are distributed. Protecting sensitive resources of the increasingly distributed enterprise with a large mobile workforce has become a challenge that siloed security tools are not able to address effectively. In addition to the growing number of potential threat vectors, the very scope of corporate cybersecurity has grown immensely in recent years. This has led to the challenges described below:

Increased Cyber Threat Level

The level of cyber threats from both state-sponsored activities and cyber criminals is extremely high. At the same time, all industry sectors have become more dependent upon digital services and this has increased the potential business impact of these threats. These two factors have made cyber resilience an essential element aspect of digital transformation. In today's distributed environment and with this level of cyber threats single-point controls are insufficient and multiple levels of controls across the network, applications, storage and endpoints are needed and these must be coordinated to act in unison.

Network Threats

The majority of cyber threats involve the network. These include inbound threats where the threat actors attempt to gain access to organizational systems and outbound threats where insiders access risky network assets such as malicious websites or export data to insecure cloud services. There are many potential weaknesses in IP communications that can be exploited by threat actors. These include open ports and open protocols. For example, web browsing uses HTTP and HTTPs protocols over TCP on ports 80 and 443. These ports should only be open for those protocols and other ports on a web server should be closed to external access. The following paragraphs describe some of the more important network-based threats.

Distributed Denial of Service

A common network-based attack is Distributed Denial of Service (DDoS). In this, the attacker attempts to overwhelm an organization's network, service or applications by sending a large number of requests from a wide range of endpoints (Botnets) under the attacker's control.

Botnets

Networks of infected computers or „bots" controlled by an attacker. Botnets are used to launch coordinated attacks, such as DDoS attacks, spam campaigns, or malware distribution.

Cross-Site Scripting (XSS)

These attacks inject malicious scripts into web pages viewed by users. The script runs in the context of the user's session, allowing attackers to steal cookies, session tokens, or other sensitive information displayed on the page.

SQL Injection

This attack targets databases through web applications by injecting malicious SQL statements into a query. It exploits a vulnerability in the application code that fails to check user input and can lead to unauthorized access to sensitive data, data breaches, and loss of data integrity.

ARP Spoofing (Address Resolution Protocol Spoofing)

This technique misleads a network by associating the attacker's MAC (Media Access Control) address with the IP address of another host, such as the default gateway, enabling the attacker to intercept, modify, or block communications to that IP address.

DNS Tunnelling

This uses the DNS protocol to communicate non-DNS traffic over port 53. It can be used to bypass network security measures to exfiltrate data or command and control callbacks.

Lateral Movement

Once an attacker has gained access to an organization's network, they will attempt to find a route to access the sensitive resources that are their target by moving between network subsegments. This is called lateral movement and depends upon weak controls that allow network traffic to flow in unexpected ways.

Social Engineering and Phishing

The threat actors often use social engineering to trick users into downloading malware that gives them access and then move around the network to access and exfiltrate sensitive data. Malware is software which is designed to disrupt the normal operation of an endpoint upon which it is installed to achieve the aims of a threat actor.

A common tactic is "Phishing" where the threat actor sends emails or social media messages that appear to come from a legitimate source and need immediate action. The message will often contain a URL which, if clicked, will ask the user to authenticate to a fake website in order to obtain their login credentials. The message may also contain attachments such as a PDF file or a macro-enabled office file, which, when opened, will run malicious code on the end user's device.

A more subtle variant of this is "Spear Phishing" where the threat actor has identified specific people as targets and sends messages that are tailored to their interests or job function.

Zero-day Exploits

These attacks exploit vulnerabilities in software or hardware that are unknown to the vendor or for which no patch has been released yet. Attackers can use zero-day exploits to bypass security measures and gain unauthorized access or cause damage. These pose a particular risk and often their existence can only be inferred by anomalous behaviour patterns.

Compromised Credentials and Ransomware

Ransomware is a threat where the threat actor encrypts organizational data to render it inaccessible and / or exfiltrates the data and threatens to leak it unless the organization pays a ransom.

The most common way ransomware gets into victim organizations today is via compromised credentials. Ransomware perpetrators buy access to compromised credentials on the dark web and then come in through VPN. The second most common path is through phishing emails. Tactics have changed and it is less common now that users pick up ransomware through browsing or freeware.

Missing Security Patches

End user devices running older versions of software, such as operating systems, browsers, plugins, and business applications, may contain vulnerabilities that have not been patched which makes them susceptible to compromise by cyber attackers. The same risks apply to physical and virtual resources such as VMs that have not been patched. This increases cyber risk since all these devices provide a potential route of access into organizational systems.

Unsecured Devices (BYOD)

End users may be allowed or encouraged to use their own devices to access organizational systems and these devices are particularly vulnerable to cyber-attack. The user may not have enabled security features such as device encryption, firewalls, anti-virus, and service passwords, which are essential to protect sensitive data, guard against malware, and comply with industry regulations on their personal devices.

Unknown devices

Many, if not most of the devices that access an organization's organizational systems may not feature in a formal inventory. This makes it hard to distinguish between those which are legitimate and those which are potentially malicious. A cyber attacker may have obtained a legitimate access credential and masquerade as an authorized user using an external unknown device. They may also have gained access to a known host but are using this to make unusual lateral access. These examples illustrate the need to authenticate not only the user but also the device.

Insider Mistakes and Malice

Users with legitimate access to the organizational system may act to compromise security through mistakes as well as malice. By mistake, a user may use email to send sensitive data to external third parties, often due to the email client prefilling the wrong email address. A malicious user may use their legitimate access privileges to gather sensitive or regulated data, which they then copy to external systems or removable storage devices.

Weak Authentication

Access to organizational systems by remote users is especially vulnerable where user authentication is based on username and password. While VPNs provide a secure access tunnel through the network, username / password authentication provides a significant risk. However, deploying MFA with VPNs increases administrative complexity and makes VPNs more difficult to manage.

Excessive Privilege

Users and systems need access privileges in order to perform their legitimate functions; however, where these privileges exceed those that are needed, they represent a risk. A cyber attacker can exploit unnecessary privileges to navigate through the organizational network to access, decrypt, and exfiltrate sensitive data. Virtual devices such as cloud virtual machines are a special case that must also be considered. These need access privileges to enable them to interoperate with the customer's other cloud elements needed to deliver a business application for example. These cloud elements may be assigned excessive privileges by developers to ensure that the application functions.

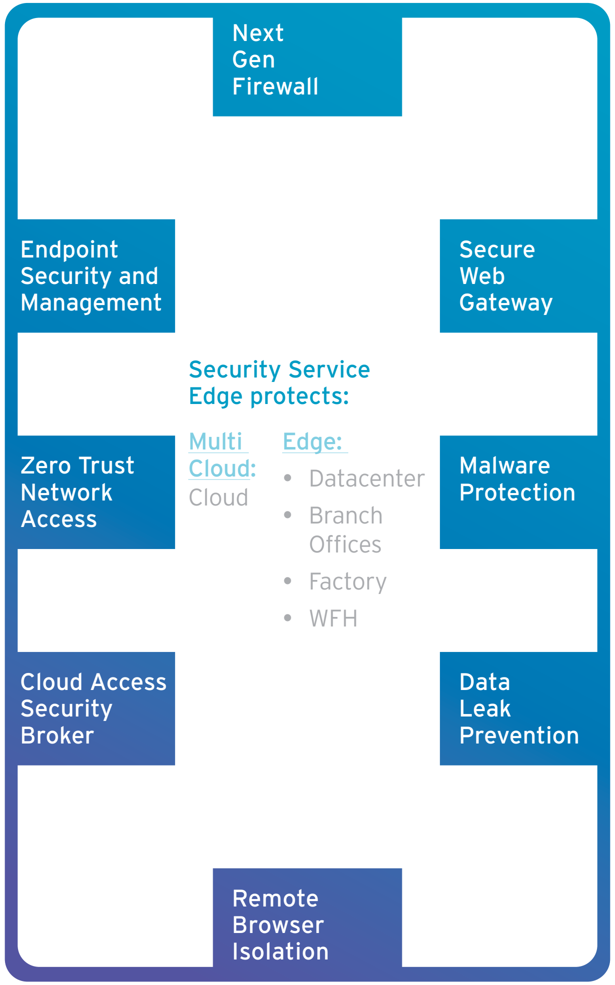
Chapter 2

The Solution

Security Service Edge (SSE) is a term describing technologies that intend to secure access to the web, cloud services, and private applications. It comprises several different security technologies designed to improve security posture as well as to secure connectivity for remote offices, cloud services, contractors, and remote employees.

How the solution works

The distinctive feature of SSE currently offered by vendors is the integration of several capabilities that were previously offered as standalone products. These most often include Secure Web Gateways (SWGs) which are network proxies used to consolidate and control user and app web utilization. Endpoint Security tools discover and prevent exploitation of vulnerabilities and execution of malware, provide application controls, and URL/ content filtering. Next-Generation Firewalls (NGFWs) are application and (in some cases) identity-aware firewalls. Firewall as a Service (FWaaS) are cloud-hosted NGFWs. Cloud Access Security Brokers (CASBs) enable shadow IT discovery, Network Access Control (NAC) points, and Data Leakage Prevention (DLP) Policy Enforcement Points (PEPs) for cloud-hosted resources. Another key element is Zero Trust Network Access (ZTNA), which is foundational for a complete solution. Capabilities such as Remote Browser Isolation (RBI) complete SSE offerings.



Secure Web Gateways (SWGs)
Secure Web Gateways provide web traffic policy enforcement, URL filtering and classification, malware detection, and content inspection. SWGs are network proxy services that manage a variety of internet and web traffic, applying policies in conjunction with customers' IAM and Network Access Control solutions.

Next-Generation Firewalls (NGFWs)
Next-Generation Firewalls and Firewall-as-a-Service provide features to protect networks, offices, data centers, cloud instances, and other resources from Denial of Service (DoS), DNS, and application layer attacks. NGFW services include packet filtering, Deep Packet Inspection (DPI), Encrypted Traffic Analysis, application awareness (including the ability to route and filter based on traffic types), and network segmentation. NGFWs may perform traffic decryption for security analysis, or in a few cases, examine encrypted traffic using advanced Network Detection & Response (NDR) methods such as JA3/JA3S, Mercury, etc. The firewall/ NDR components, in conjunction with Endpoint Protection Detection & Response tools (described below), if present, usually can take mitigating actions such as process termination, connection termination, node isolation, blocking of IPs/URLs, and initiating packet capture on endpoints, gateways, and in the cloud.

Zero Trust Network Access (ZTNA)

Zero Trust has arisen over the past decade and has become a primary means of addressing access control use cases. Often expressed as „Never trust, always verify", ZTNA is an embodiment of the principle of least privilege, and at its core mandates that every access request be properly authenticated and authorized. Thus, IAM (Identity and Access Management) is a foundational element for ZTNA. Most SSE solutions are identity-relying parties, accepting Open ID Connect (OIDC) and Security Assertion Markup Language (SAML) assertions for federated authentication to their resources. In the latter scenario, the choice of authenticators depends on the customers' existing IAM or IDaaS. Strong and Multi-Factor Authentication (MFA) options are recommended.

Risk Adaptive Authentication

Risk-adaptive and/or continuous authentication features for ZTNA. Although in many cases SSE customers use identity services outside of the SSE solution, the solution can harvest authentication and session data to perform risk-adaptive and continuous authentication and authorization.

Remote Browser Isolation (RBI)

This can protect end-user devices from compromise from malicious content from the web and email. RBI is generally hosted by SSE vendors in their clouds and allow customers to use the most widely deployed browsers with few configuration changes. Acquisition, scanning, and execution of remote content happen in the vendors' RBI environments, with inert results passed to users. Remote Browser Isolation should be able to be applied by user and resource types. Pixel rendering is an older but slower method for RBI. DOM rewriting is a newer and faster RBI method. Pixel rendering is theoretically safer for end users but has high latency. DOM rewriting may miss some malicious content in web traffic. A few vendors are deploying newer technologies in this area that do not conform to the models described here. Some SSE solutions rely on 3rd-party products for RBI functions.

Data Leakage Prevention (DLP)

Data Leakage Prevention functions include data discovery and classification, and definition and enforcement of security policies with controls over how data can be accessed and where data can move. Enforcement may be through endpoint agents or network-based controls. DLP systems typically look for common data types such as Personally Identifiable Information (PII), credit card numbers, Social Security Numbers, and other government identifiers, etc. Customers should be able to create their own data types for DLP mechanisms to enforce. Some SSE solutions rely on third-party products for DLP functions.

Cloud Access Security Brokers (CASBs)

Cloud Access Security Brokers discover and control cloud service usage, discover and classify data, and enforce data security policy compliance in the cloud. In this context, cloud includes major SaaS services such as Microsoft O365 and Teams, Google Workspace, Salesforce, Slack, Concur, ServiceNow, JIRA, etc. Access control models for user/group to resource entitlement management and Role-Based Access Control (RBAC) are those most commonly used. However, Attribute-Based Access Control (ABAC) is preferred. Regarding data discovery, classification, policy definition, and enforcement, DLP and CASB should be functionally similar across vendor solutions. Enforcement actions include controls over the uploading of files to sites, attaching files to email, reading data, copying content to clipboard, downloading files, and moving or copying files to other devices.

Endpoint Protection Detection & Response (EPDR)

Endpoint Protection Detection & Response (EPDR) tools are designed to identify malware or malicious behavior and prevent damage, control application access, filter URL/content; and detect and remediate malware or other security incidents on desktops, servers, laptops, and mobile devices. There are four approaches that vendors can take to EPDR as part of SSE:

- EPDR functions bundled in the SSE agent and included in the subscription. No vendor currently offers EPDR and SSE together.
- EPDR available from the same vendor but licensed and instantiated separately.
- Partnership with one or more EPDR vendors.
- In some cases, SSE vendors do not offer as built-in or partner with EPDR vendors but rather leave the choice to the customer about how to procure, deploy, and manage endpoint security.

Unified Endpoint Management (UEM)

UEM provides asset management, device vulnerability, and security posture assessments. SSE endpoint agents have access to detailed device information. Some vendors integrate with full UEM solutions in their wider suites; some vendor products provide interoperability with third-party UEM solutions via APIs; and others do not leverage device information outside of the Device Posture Checks that they perform for network access control.

Chapter 3

Top Use Cases

Working From Home

VPNs have supported Work From Home (WFH) and other drivers for more than two decades. The Covid pandemic necessitated widespread WFH, and the technologies that remote work relies upon have proven to be highly effective. However, in many cases, the performance of traditional VPNs has been strained. Scalability has been insufficient. Managing network segmentation in conjunction with VPN access has become exceedingly difficult in large enterprises. SSE provides capabilities that help to manage these challenges.

Work from Anywhere

Many organizations accept that Work from Anywhere (WFA) will be the norm going forward. The need for Secure Access is greater than ever, with fraud, ransomware, and corporate espionage on the rise. Remote worker access, including employees and contractors, needs to be properly secured with strong authentication services and granular access controls. Moreover, assurances that end-user devices are not compromised must be part of the Secure Access equation. Remote workers and contractors now do much of their work in the cloud as well as by accessing resources in corporate data centers. Security Service Edge provides capabilities that facilitate secure remote working.

Cloud Access Control

Most organizations now depend upon a wide variety of cloud-delivered business-critical services. By their very nature, access to these services is over a network, and this access needs to be secured. Access to cloud-delivered business applications must be authenticated to prevent access by threat actors while making this access easy for authorized users. Security Service Edge provides capabilities to enable people within the organization to use sanctioned cloud services while preventing the use of unsanctioned services.

Data Protection

Data is the most valuable asset of the modern organization and it must be available to authorized users when they need it and at the same time protected against leakage, loss, as well as ransomware. Laws and regulations also stipulate where certain data must be held which adds further challenges when using cloud services and other forms of distributed computing. Security Service Edge provides capabilities to improve the protection of data across the distributed enterprise.

Enhanced Security

As organizations have gone through digital transformation, they have become more vulnerable to cyberattack. Digital transformation by definition increases external connectivity by enabling greater access to organizational systems. This, together with increased use of cloud services, also increases the potential attack surface. Security Service Edge provides capabilities to enhance the cyber security posture of the digital enterprise.

Chapter 4

Top Functional Selection Criteria

Policy Based

The solution should provide the capability to set and apply consistent cyber security controls across a wide range of technologies and network types using policies that are technology-independent. This should include Policy Based Access Controls as well as other forms of policy-based security to ensure that cyber controls are instantiated as physical and virtual resources are created and deployed.

ZTNA

The solution should support a "Zero-Trust" approach to network security. This includes the capabilities for authentication and authorization of end users, administrative users, applications, devices, and resources. The preference is for MFA, federation, and attribute and / or policy-based access controls. The solution should support interoperation with IAM/IDaaS solutions beyond identity federation, such as Privileged Access Management (PAM).

Endpoint Protection

The solution should provide endpoint security and management or integrate with EDPR / UEM capabilities from other vendors. These should cover a wide range of endpoint device types and operating systems.

Network Security

The solution should provide capabilities for detecting and responding to threats at the network level, such as DDoS, command & control traffic, botnet traffic, reconnaissance by adversaries, lateral movement, and data exfiltration attempts. These functions are typically managed by the Next-Generation Firewall and Firewall-as-a-Service components. However, in some vendor solutions, these functions may be implemented in the SWG components.

Web Security

This is distinct from network security and covers the Secure Web Gateway and Remote Browser Isolation capabilities provided. In most cases, these functions are cloud-hosted but, depending on the vendor's architecture, may also be present in the on-premises gateway appliances. In a few vendor solutions, RBI functions are outsourced but integrated.

Data Protection

The solution should provide capabilities such as the ability to define access control policies centrally, and to discover, classify, and enforce data access control policies on endpoints and the cloud. Discovery should be automatic and data classification automated and controls should be based on the classification and sensitivity of the data as well as regulatory compliance obligations.

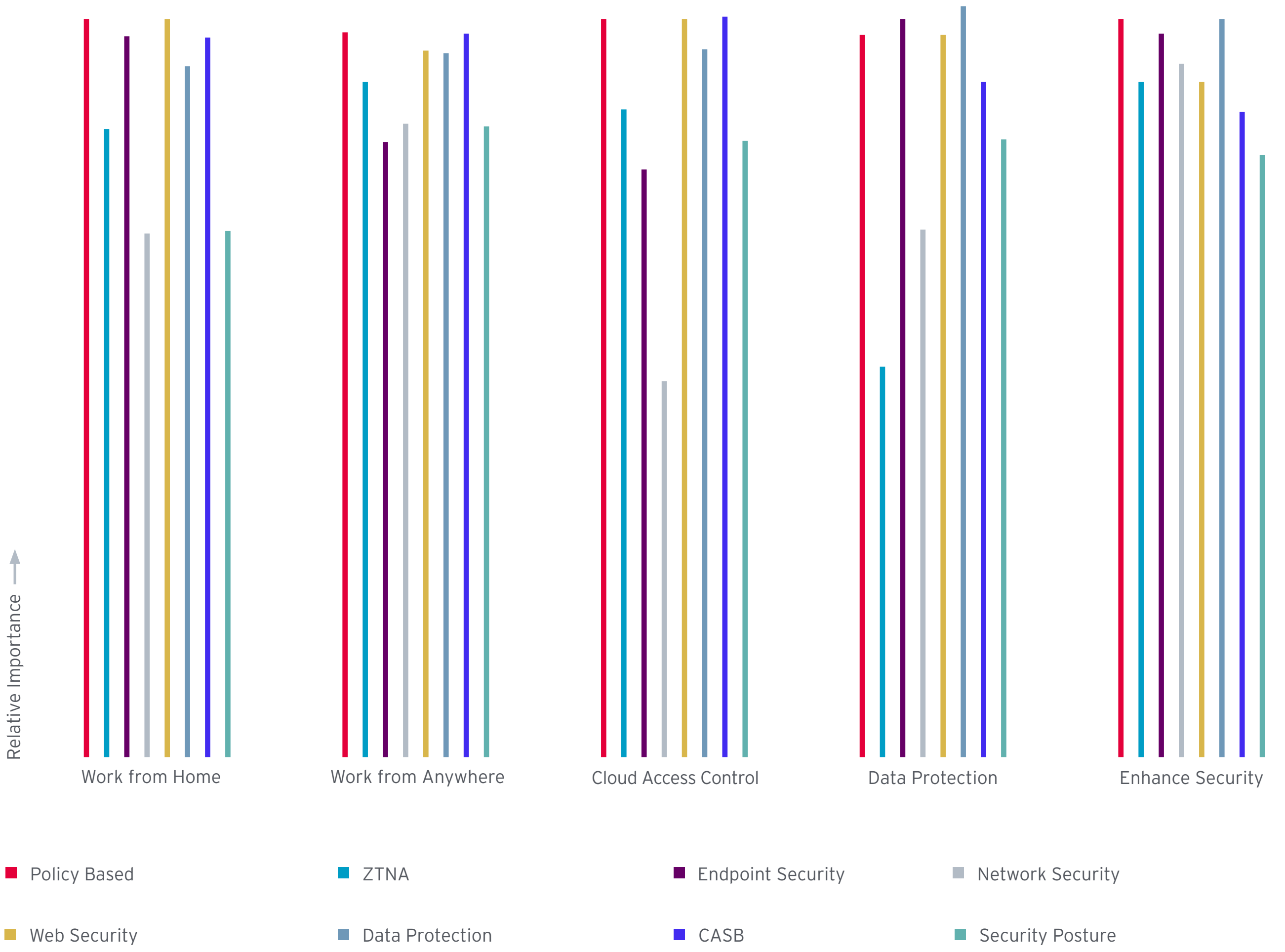
CASB

The solution should provide capabilities to control which SaaS services organizational users can access. It should also discover shadow IT usage and prevent access to unsanctioned services that the organization considers to be too risky. It should integrate with the major SaaS services to implement fine-grained controls over how sanctioned services can be used. It may also integrate with DLP (Data Leakage Prevention) solutions to control which data can be moved to which cloud services.

Security Posture

The solution should provide capabilities to provide a way to continuously identify, visualize, and manage an overview of the existence and effectiveness of the controls that it provides against the risks and customer's compliance obligations.

Use Case / Capabilities Mapping



Chapter 5

Vendor Spotlight

Broadcom, with its roots in the semiconductor field, has emerged as a leading software vendor, specifically in the cybersecurity and IAM (Identity & Access Management) space. Through the acquisition of CA Technologies, the enterprise division of Symantec, and VMware, Broadcom has built a strong portfolio of solutions for cybersecurity, including Symantec Network Protection as their offering for SSE, including ZTNA capabilities. Network Protection covers all areas of what is expected within SSE.

Symantec, after the acquisition of Vontu for DLP (Data Leakage Prevention) back in 2007, which now helps strengthen the ZTNA offering by controlling outgoing data flow, has acquired several other cybersecurity companies over the past decade that add to their SSE offering. These include, for instance, Blue Coat for SWG, threat inspection, and sandboxing, Luminate for the core ZTNA offering, or Fireglass for remote browser isolation. These solutions also have become part of the Symantec Enterprise Cloud, which provides cloud-delivered protection, but also integrates with on-premises protection.

It builds on a unified agent and utilizes various common services such as threat prevention services, the Symantec Global Intelligence Network for threat intelligence, and analytical services. Symantec SSE can leverage any SD-WAN solution, including direct integration with VeloCloud SD-WAN, for a full SASE solution.

Symantec SSE comes with a broad set of functional areas:

- Cloud-based Secure Web Gateway with proxy-based architecture
- CASB, delivering insight into web applications and allowing administrators to decide which should be blocked
- Threat Detection with deep file inspection and sandboxing
- Cloud firewall for non-web traffic, allowing filtering according to user and layer 4 port
- Full web isolation/remote browser isolation for securing web access
- Edge SWG for on-premises environments, protecting them from fraudulent web access
- ZTNA for secure communications over the web without the need for a VPN
- Intelligence Services based on the Symantec Global Intelligence Network, delivering insights into threats based on continuous analysis of Internet traffic
- Management Center and Reporter as the solution for centralized management and reporting across all components of Symantec SSE

These are available as Web Protection, which focuses on SSE except ZTNA and a few other features such as full web isolation/remote browser isolation, and as Network Protection or “Full SSE”, which integrates these capabilities as well. With the inclusion of ZTNA, Network Protection is, to our perspective, the recommended option, unless there already exists another vendor’s ZTNA solution.

A major advantage of the Symantec SSE solution is that it goes beyond SSE by having an out-of-the-box integration with the Symantec Endpoint Security solutions. Due to that, there is only one agent needed for all capabilities, including Endpoint Security, DLP, ZTNA, CASB, and SWG. This can massively simplify the deployment and operations of the solution compared to other vendors’ offerings. Deploying and maintaining agents on the endpoint causes significant overhead. By reducing the number of agents, overhead as well as potential incidents such as outdated agents and updating issues can be reduced.

Symantec SSE supports the common SSE use cases such as enabling remote work and work from anywhere including safe browsing, cloud access control including full traffic visibility and web filtering, data protection for outgoing traffic with their DLP capabilities, and enhanced security with comprehensive threat protection, application visibility and other functions.

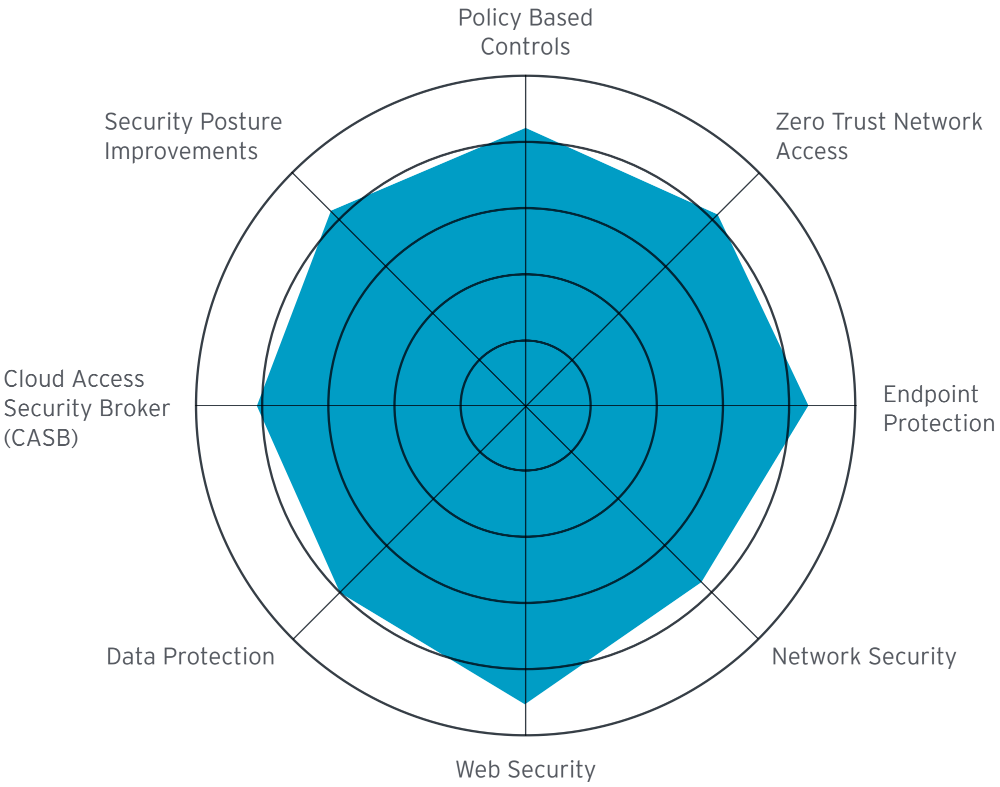
Some of the specific strengths of the solution include

- Full visibility into all traffic with leading-edge SSL/TLS decryption
- Flexible yet non-intrusive, proxy-based SWG architecture, supporting a variety of actions on web traffic from passing to blocking, quarantine, alerting, and others
- Integration of the Symantec Global Intelligence Network, processing huge amounts of Internet traffic per day and having proven its strength by discovering multiple major APTs (Advanced Persistent Threats) including Stuxnet and Dragonfly
- Multi-layered threat analysis for any deployment model, with edge security and cloud security working in neat integration
- Strong performance by building on a global cloud-native footprint, utilizing the private Google backbone
- Full hybrid support with cloud and on-premises components, supporting any type of organization and use case

The latter is important for many if not most organizations, which aren't cloud-native, but run a hybrid IT environment. For these, edge capabilities in addition to cloud-delivered and cloud-focused capabilities are essential.

Symantec SSE is well positioned in the SSE market across all areas. The solution comes with a wide range of features, covering all major areas of SSE in breadth and depth. Its architecture allows for supporting complex, hybrid customer environments. It is backed by leading-edge cyber intelligence services. Symantec SSE is an integrated solution, delivered via the Symantec Enterprise Cloud, but also providing edge components where needed, as well as a unified endpoint agent that also integrates with the Symantec Endpoint Security features. This makes Symantec SSE a solution that should be included when looking for an SSE solution.

Symantec SSE delivers strongly to the key functional areas of SSE solutions



Chapter 6

Considerations

Architectural considerations

Deployment
Consider which deployment model is most appropriate for your use case. What permutations of distributed sites, remote workers, contractors, and cloud resources does your SSE need to support?

Most SSE solutions are delivered as SaaS but some components may be available as appliances or include software that can be deployed where required. Some vendors offer SSE as part of their complete SASE solution which includes a Software-Defined Wide Area Network (SD-WAN) with SSE delivered from the Points of Presence (PoPs). Other vendors utilize one or more public IaaS providers across multiple data centers for scalability and performance.

Another consideration is whether it is necessary to deploy agents, and if so, whether multiple agents are needed for the solution. Does the vendor offer a single deployable agent bundle that covers Endpoint Protection Detection & Response (EPDR) and Unified Endpoint Management (UEM) with the SSE agent?

Consider whether the vendor offers or partners with systems integrators to provide deployment and maintenance services to offload this work.

Integrations and interoperability
Look for support for standards that facilitate interoperability with other components in the security and IAM architecture. Relevant standards in IAM include FIDO, JWT, OAuth, OIDC, and SAML. Standards for security are concerned with inter-application information sharing and include CEF, REST API, SNMP, STIX, syslog, TAXII, etc. SSE solutions all generally support REST APIs for management interoperability, and a few support the newer GraphQL.

Pre-deployment considerations

Identifying primary use cases
It is important to understand which are the main use cases for SSE in your organization. The answers to this will determine the environments with which SSE will need to integrate and the standards and best practices that it will need to support.

Integrations
You should consider how the solution will integrate with your target environments. Ideally, the solution should support integrations out of the box. One critical area will be integration with existing security tools and identity and access management.

- Which agents do you need to install to get the required coverage and functionality?
- How do you integrate the solution with the environments, and tools that are used?
- What APIs do you need to integrate with other services and security tools?
- If some functionality that you require is not present in the vendor’s solution, do they have APIs, partnerships and/or API-level connectors with third-party products and services that can provide it?

Chapter 6

Questions to Ask Vendors During RFPs

Do you specialize in serving specific industries?
Large vendors will have customers across most industries. Some smaller vendors may focus on specific industry sectors, such as retail, media, healthcare, finance, etc. In some circumstances, vendors with experience and focus on the industry that is specific to your organization may provide more value.

What are your key differentiators?
Understanding the key differentiators between the vendors is essential. Ask the vendor what their unique capabilities are. For example, content disassembly and reconstruction for increased protection, DLP features to prevent data exfiltration, and inbuilt EDPR.

What certifications and attestations have you obtained for the solution?
Certification of the solution against security standards as well as industry regulations not only confirms compliance; it also demonstrates the vendor's commitment and conveys trust. Security certifications such as ISO27001 and attestations such as SOC 2, US FedRAMP, UK Cyber Essentials, and German C5 as well as the relevant industry regulations and standards should be considered. Note that the solution itself should be covered, not just the cloud service that is used to deliver it.

Does your solution help customers with regulatory or standards compliance?
Depending on geography and industry sector, organizations are often subject to a wide range of regulations. These regulations usually include obligations to protect financial data, such as PCI-DSS, and personal data protection such as GDPR, California's CCPA and HIPAA for US healthcare providers. There are also upcoming regulations for cyber resilience such as the EU NIS2 and DORA. How does the solution help your organization meet to meet its obligations under the relevant laws and regulations?

How does your solution achieve scalability and high availability?
Does the solution scale sufficiently to meet the needs of your deployment? What are the limits that you need to consider? How can the solution be configured to meet the levels of availability that your organization requires? How does the service help to manage incidents that are detected?

How does your solution support a hybrid multi-cloud strategy?
Organizations are exploiting multiple clouds as well as on-premises and edge computing. How does the solution help to support the mixture of environments in your organization, as well as your prospects for cloud migration?

What is on your short-term and long-term roadmap?
The list of features on a vendor's roadmap is a good indicator of their innovativeness and the vendor's ability to support emerging use cases. What features are expected in the near or long term (e.g., 3, 6, or 12 months out)?

What are the emerging trends that you are seeing?
Threat actors are constantly innovating, and security solution providers are usually aware of their changing tactics. If the SSE vendor has special expertise in finding and deterring the kinds of cyber threats your organization is experiencing, then this topic merits further discussion.

Can I speak to some reference customers?
Finally, it is usually enlightening to speak to one or more reference customers. It is most helpful when the reference customer is in a similar industry and region.

Recommendations

Organizations adopting a work-from-anywhere model supported by business applications delivered through a distributed and multi-cloud hybrid IT infrastructure need to deploy an integrated set of security tools to manage the current elevated level of cyber risks. It is recommended that they should consider adopting a Security Service Edge (SSE) solution to secure access to the web, cloud services, and private applications.

Related Research

Leadership Compass

- SASE Integration Suites
- Unified Endpoint Management (UEM)
- Managed Detection and Response (MDR)
- Cloud Security Posture Management
- Attack Surface Management
- Email Security
- Zero Trust Network Access
- Endpoint Protection Detection & Response
- Network Detection & Response

Advisory Note
Implementing SASE

Whitepaper

- Security Operations in the Age of Zero Trust
- The Role of Identity for Zero Trust

Copyright

All conclusions, recommendations and predictions in this document represent KuppingerCole´s initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

For further information, please contact clients@kuppingercole.com.

KUPPINGERCOLE ANALYSTS AG
Wilhelmstraβe 20 – 22
65185 Wiesbaden | GERMANY
P: +49 | 211 - 23 70 77 - 0
F: +49 | 211 - 23 70 77 - 11
E: clients@kuppingercole.com.
KUPPINGERCOLE.COM