Cloud Security: A Buyer's Guide

Forcepoint

Brochure

What's Inside:

Evaluation Criteria: What to Look For in Your Solution

As with any technology, cloud security vendors tout a wide range of attributes and features. It's often hard to distinguish between what's worth considering and what's simply noise. Here are 15 points to keep top-of-mind while evaluating solutions and determining the best fit for your organization.

Support and Services

Whether you're looking to improve Office 365 performance at branch offices, safeguard employees' use of web content while working remotely, or protect the use of cloud apps and data, having the right solutions with the right team behind them makes all the difference. Don't settle for a patchwork of point products cobbled together from multiple vendors. Look for partners who can provide integrated connectivity and security solutions that can be deployed smoothly and supported efficiently.

Ease of Use

It wasn't so long ago that "enterprise" products were designed for experts who saw complexity as a badge of honor. Today, no IT organization has the time or personnel to spare on siloed products that get in the way of efficient operations. While some solutions may appear to be quick to set up and use, especially in demo situations, look at what they will take to operate at true enterprise scale. That's where you'll be spending the vast majority of your time and where the biggest impact on your organization will be felt.

Pricing

Cloud security can be as simple as a few firewalls and as complex as a 1,000-site rollout of integrated network intrusion prevention, web security, and cloud application control with data protection. Look for solutions that are priced in a straightforward way without dinging you for every little feature. Enterprise License Agreements can make it easier still, enabling technologies to be consumed as needed for a single per-user fee.

Ease of Implementation

The ability to integrate with your existing environment is critical. Your firewalls, web gateways, and cloud application security brokers should all be able to use your existing infrastructure to pull identity information from Active Directory or send log data to your SIEM. Just as important is the ease with which you can create security policies that implement your real-world business processes. Look at how quickly you can add or update policies across hundreds or thousands of sites. Even if your organization isn't this large yet, systems that are designed for global scale can help you grow and can free your operations teams to focus on moving your business forward.

Customization/Flexibility

No two organizations are the same and one size never fits all. While you undoubtedly have certain security policies that apply globally, you probably have additions and exceptions at almost every level of your enterprise—across geographic, organizational, and functional lines. Make sure the solutions you evaluate let you handle your unique needs, whether it's in selectively limiting access to various parts of your network, guarding the use of different types of content on the web, or controlling the way your own custom cloud applications and data are used.

Direct-to-cloud Connectivity

Digital transformation initiatives often begin by replacing internally hosted applications with cloud-based software as a service (SaaS) that can be used from anywhere. However, many traditional hub-and-spoke networks, especially those built on MPLS, often can't keep up. In addition, they're easily overloaded and can be prohibitively expensive to upgrade. That's why organizations around the world are connecting their offices and branch sites directly to the cloud using local broadband internet links managed by software-defined wide-area networking (SD-WAN). This approach to connectivity can dramatically cut network costs, improve users' productivity (especially for modern cloud apps like Office 365), and reduce operational burdens. But, keep in mind that while SD-WAN solutions typically provide encryption for protecting data sent over them, that's only half the picture.

Securing the Use of SD-WAN

Using SD-WAN to connect sites directly to the cloud instead of backhauling traffic to centralized security gateways requires a new approach to security. You need to keep intruders out of your remote sites (such as with firewall appliances or firewall-as-a-service) and protect what your people do on the internet. That includes safeguarding the use of web content (usually via cloud-based web security services) and preventing the misuse or exposure of cloud apps and data (the most common uses of CASBs). To reduce the number of products and vendors you have to deal with, look for solutions that integrate SD-WAN and branch security (often called Secure SD-WAN) as well as web security and cloud access control.

Visibility

Security is rarely black and white. People use managed and unmanaged devices, sanctioned and unknown apps. Things always happen in the gray areas. To keep on top of it all, operations teams have to rapidly understand what is happening throughout your environment. Look for solutions that go beyond data logs. Interactive dashboards help you quickly visualize what's going on so that you can focus on insights—not data—and have the technology adapt to you instead of the other way around.

Safe Access to Internal Applications

The shift to working from home has highlighted the ongoing challenges of providing access to internal apps. VPNs have been begrudgingly relied upon but their costs and complexity limit their scalability, and they often leave networks exposed. Fortunately, there are new approaches such as Zero Trust Network Access solutions that provide private access over the internet to internal apps as an alternative to using VPNs for non-administrative users.

Protection for Data in the Web and Cloud

Most organizations already protect their web and cloud users against internet threats. That keeps the bad stuff out, but you need to keep the good stuff (your data) in, too. Look for web security and CASB solutions (the more integrated, the better) that also offer true enterprise-class data protection. This will help you keep control of regulated data and sensitive intellectual property no matter where people work.

Scalability

Whether you're a Global 2000 enterprise, a nationwide government agency, or a mid-sized business, your organization is constantly shifting—growing larger in some places and smaller in others. The ability to automate key processes such as spinning up (or down) new locations, adding large numbers of new users, or updating security policies across the world when seconds count is key. Look for solutions that are designed to handle the rigors of global operations. This type of efficiency will free you up to focus on growing your business—even if you aren't a multinational conglomerate.

Recognition/Credibility

Technology adoption life cycles go through phases: At first, solutions get awards and accolades based on the features they have and how they might be different from the status quo. Ultimately, however, attention shifts to what other customers are saying. Look at who's using the solution and why. This will help you more rapidly find the technologies and people that are best suited to your individual needs.

Analyst Performance

Analyst reports such as Gartner Magic Quadrants, Forrester Waves, and product tests such as those performed by NSS Labs often provide a starting point for finding solutions. But no two analysts or tests will see a solution the same way. Rather than focus on absolute rankings, look at the questions they ask and the way they frame their evaluations. This can help you find what's most relevant to you.

Hybrid IT Environments

Securing the use of the cloud from the cloud is one of the hallmarks of a comprehensive cloud security solution. However, in today's world where applications exist everywhere— in multiple clouds, as well as on premises—there are many situations in which enforcement may still need to be done at specific locations. Whether it's streamlining compliance or meeting data sovereignty requirements, modern enterprise IT environments are hybrid in nature. Your security has to be wherever your people and data are, which means hybrid security solutions are likely going to play an important part of keeping your organization safe and your auditors happy.

Innovation

One of the most important attributes to look for in a solution provider is whether they are trying to make a quick sale and move on or are laying the foundation for a long-term partnership with you. Look at the vision they have for cybersecurity. Are they focused on key industry trends such as the use of behavior intelligence and new approaches such as Gartner's Secure Access Service Edge (SASE) and Forrester's Zero Trust models? In the end, the best partners will work with you to tailor their innovations to make your business more productive, efficient, and secure—giving you a pathway to the future you want for your business.

Charting Your Options

	FORCEPOINT	ZSCALER	SYMANTEC	PALO ALTO	FORTINET	CISCO	NETSKOPE
Web Security	●	●	●	○	○	●	○
Direct-to-cloud SD-WAN	●	—	—	—	●	●	—
NGFW	●	○	—	●	●	●	○
CASB	●	○	●	○	●	○	●
Email Security	●	—	●	—	—	●	—
DLP for Cloud Applications	●	—	●	—	—	—	●
Hybrid Enforcement	●	○	●	○	—	●	○
RBI	●	●	●	—	—	—	—
Protection of Unmanaged Devices	○	○	○	○	○	○	○
Pathway to Behavior-based Security	●	—	—	○	—	—	—

● = supports ○ = partially supports — = minimally/doesn't support

Zscaler – Founded as a cloud-based web gateway, Zscaler has been branching out, adding new capabilities such as basic firewalling, some CASB, and now remote browser isolation (RBI). They are aggressively claiming to already be a secure access service edge (SASE) solution, even though Gartner analysts state there are no real SASE products yet.

Symantec (Bluecoat) – Symantec offers a wide range of security solutions, from web security appliances and cloud services, DLP, and CASB to email security. However, they do not offer NGFW, which limits the visibility and control they can provide within your network. Since their acquisition by Broadcom, they have decided to focus solely on the Global 2000, leaving all other enterprises and mid-market businesses to find alternate solutions.

Palo Alto Networks – Founded as a "next-generation" firewall point product vendor, Palo Alto Networks has been branching out through acquisitions to create a security platform company. In 2019, they acquired behavioral intelligence technology and will likely try to follow Forcepoint into offering behavior-based security. They are pursuing SASE with their Prisma product.

Fortinet – Originally founded as a lower-cost provider of next-generation firewalls, Fortinet has expanded their business through acquisition but still has a reputation for lacking manageability at scale and providing collections of features that don't necessarily work together.

Cisco – As the dominant networking company, Cisco captured a large share of the security market by adding security into their networking sales—the technology version of "Would you like security fries with that network burger?" Their security products often don't work together and they've frequently been criticized for not offering customers a clear path forward. They are pursuing SASE with their Umbrella product.

Netskope – Founded as a CASB point product vendor, Netskope has solid data protection for cloud apps. They recently expanded their offering to include web security and will be adding further capabilities in pursuit of SASE.

Sample Questions to Highlight in RFPs

When looking at cloud security products, many enterprises find it useful to ask vendors for input in the early stages or for details at later stages. Such Requests for Information (RFIs) or Requests for Proposals (RFPs) can highlight key capabilities that can shape the ways in which products and solutions are used.

While full RFPs often have hundreds of questions, here are some examples that might be useful to ask:

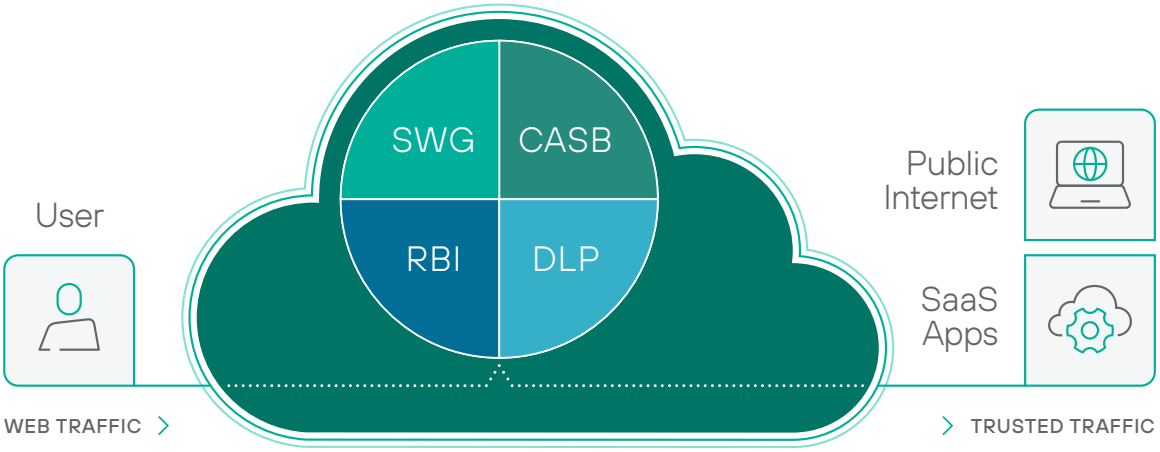
How can sites and users connect to the solution?

QUESTIONS	WHAT THIS QUESTION CAN TELL YOU
How is the solution deployed (as a cloud service, on-premises appliance, hybrid of the two)?	Some solutions force you into a one-size-fits-all approach: cloud-only or appliance-only. However, most enterprises have a mixture of cloud and datacenter-based applications which can have different security requirements. Hybrid approaches, in which enforcement can be in the cloud as well as on-premises, help you address requirements for local enforcement that specific sites might have (for data sovereignty or audit compliance).
How do remote sites connect to the solution (VPN back to a central hub, industry-standard GRE and IPsec to cloud service, other)?	Modern solutions make it easy for each site to connect directly to the cloud without having to set up complicated VPNs or complex tunneling.
How do roaming users connect to the solution (VPN back to a central hub, manual proxy files, automated agent)?	Security should follow users whenever they go off the enterprise network (at hotels, visiting customers, etc.) without requiring manual or slow mechanisms like connecting back through a central office.
How are roaming users who are behind other organizations' defenses (e.g., at hotels, other companies, etc.) still protected?	Security solutions that aren't designed for roaming users often break or require manual connections over VPNs when users are at sites that enforce other security controls.
Does the solution include SD-WAN connectivity for remote sites or require it from a separate vendor?	Requiring separate products or services for SD-WAN, especially from other vendors, can lead to added costs and complexity.
Can the solution provide content localization for each user at each location?	Many security solutions only let users see web content in the language of the country where the security service is running rather than where the user actually is.
Can the vendor provide enough throughput to support the types of applications you need to use?	Some vendors lack the flexibility to scale up the bandwidth they can provide to each customer.

What controls are provided for securing use of web sites and content?

QUESTIONS	WHAT THIS QUESTION CAN TELL YOU
How many categories of websites does the solution automatically distinguish? Can it categorize new or unknown sites in real time?	Automated categorization of websites greatly streamlines your operations and is critical for protecting against or controlling access to websites you hadn't heard of before.
How granularly can access to sites and categories be controlled (times, quotas, users/groups, etc.)?	Some solutions take an all-or-nothing approach to allowing or blocking connections. For more flexibility, look for controlled access to websites that you don't want to block outright or limiting controls to specific groups of users.
How are encrypted (SSL/TLS) sites decrypted and inspected while maintaining user privacy? Is the process automated or manual?	Now that most web access is encrypted, the ability to inspect content from such sites is crucial. However, many organizations have strong policies against decrypting users' personal data received from banks, healthcare providers, and other such sites. Automation is critical for protecting users' privacy.
Can internal applications be accessed by remote users without a VPN?	Most organizations still have applications that aren't directly accessible from the internet—in internal data centers or isolated cloud enclaves. New Zero Trust Network Access (ZTNA) capabilities provide private access to internal apps seamlessly, without the complexities of VPNs.
Can remote browser isolation (RBI) be used to insulate use of select categories of websites?	Rather than blocking access to unknown or possibly suspicious sites, remote browser isolation enables users to see information without putting their computer or the enterprise network at risk.
What types of data loss prevention (DLP) controls are provided for protecting uploads to websites?	One of the largest differences among security solutions is the range of filtering provided for files that are uploaded to websites. Often performed both in the cloud and on the endpoint, comprehensive and automated DLP is crucial to preventing theft or accidental loss of data.
What types of sandboxing for protecting against zero-day or unknown threats does the solution provide (such as application/OS/CPU emulation)?	Deeper emulation is necessary for defending against advanced threats such as root kits or attacks that detect and avoid common emulation products.
What role will new approaches to security such as behavioral intelligence and Zero Trust play in future versions?	Old, static ways of manually expressing security policies across a wide range of conditions are giving way to new forms of automation that tailor enforcement to individual users' own actions. This will dramatically improve the effectiveness and efficiency of enterprise security systems.
What role will SASE and Zero Trust play?	Just as the disparate security "stacks" of the past have been consolidated into more-integrated products of the present, connectivity and security are converging in the cloud to enable organizations to work more efficiently than ever before.

Today's Inside-out Reality and the Forcepoint Difference



Digital transformation is driving tremendous changes in today's enterprises. People, applications, and data used to be located or connected behind security gateways. This created a barrier—a perimeter—to insulate enterprise systems from the rest of the world. But then the world changed in several key ways:

People

Organizations are becoming more distributed than ever before, often with branch offices spread around and people working all over.

Apps/Data

Many applications and data have moved into the cloud.

Connectivity

Naturally, connectivity between people, apps, and data have moved into the cloud as well.

Essentially, today's enterprise is turning itself inside out. Most of its business, and the information and transactions that drive it, are happening outside the perimeter, beyond the security walls that it depended on for so long. Something HAS to change.

Security only works when it's close to the things it's protecting. Having security follow people, apps, data, and connectivity into the cloud makes it possible for organizations to truly reap the benefits of being in the cloud—greater productivity, reduced costs—while managing risk and complying with ever-expanding privacy mandates.

Beyond just a buzzword, digital transformation is one of the biggest disruptions in the history of computing. The way edge protection is done is undergoing a seismic shift. Technologies are converging and traditional expectations are getting upended.

Forcepoint's unique background and range of capabilities are depended upon around the world to connect and protect highly distributed enterprises and government agencies. We are the only vendor to combine defense in both breadth and depth and are leading the industry toward a new generation of behavior-based security automation.

What Makes Forcepoint Edge Protection Solutions Different

Security Breadth
Web, Network, App, and Data Security in one

Hybrid Depth
Visibility and Control across Cloud, Network, Endpoint

Risk-Adaptive Protection
Automated enforcement powered by behavioral intelligence (coming)

Getting Started with Forcepoint: Features and Benefits We Provide

1. **Single-vendor converged solution –** Enterprise edge and cloud security platform encompassing network connectivity (SD-WAN, VPN), network security (NGFW), web and cloud access security with threat protection and data loss prevention (Cloud Security Gateway).
2. **Global scalability –** Used by enterprises of all sizes, all around the world.
3. **Hybrid enforcement –** Visibility and control spanning cloud, network, endpoint.
4. **Behavior-centric security –** Understanding the context of user actions on endpoints (such as which programs and users are accessing which resources across the network) and rich user and entity behavioral analytics (UEBA) inform a new style of automation. By triangulating actions at the individual user lever and gleaning more accurate insights into what's happening everywhere, security remains out of users' way until intervention is necessary.
5. **SASE and Zero Trust –** Forcepoint has a unique breadth and depth of protection technologies that will enable us to deliver a new generation of security that makes it dramatically easier to safeguard data and critical intellectual property.

How You Benefit

Greater Productivity – faster performance for modern cloud apps and greater agility for opening new locations

Lower Costs – fewer boxes and consoles to buy and manage, lower operations burdens

Reduced Risk – stronger security, including a pathway to behavior-centric security, that's extensible to adapt to customers' growing needs

Streamlined Compliance – unified visibility and control across cloud, network, and endpoint to accelerate incident response and remediation

Are you ready to learn more about how Forcepoint's converged enterprise edge and cloud security solution can safeguard your users and data while fulfilling operational imperatives?

Connect with one of our experts to start talking about your unique needs.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[Cloud-Security-A-Buyers-Guide-Brochure-EN] 21July2020