KuppingerCole Report

MARKET COMPASS

By Alexei Balaganski

March 09, 2021

Cloud-delivered Security

The KuppingerCole Market Compass provides an overview of the broad market of cybersecurity solutions delivered from the cloud, focusing primarily on Zero Trust and Secure Access Service Edge (SASE) functional capabilities and user experiences targeted towards employees and other end users.

By **Alexei Balaganski**
ab@kuppingercole.com

Content

1 Management Summary

The KuppingerCole Market Compass provides an overview of a market segment and the vendors in that segment. It covers the trends that are influencing that market segment, how it is further divided, and the essential capabilities required of solutions. It also provides ratings of how well these solutions meet our expectations. This Market Compass covers a variety of security solutions that help organizations protect their users from a broad range of cybersecurity threats without the need to deploy additional on-prem appliances or software agents, greatly reducing the cost and complexity of corporate security infrastructures.

As businesses embrace the Digital Transformation and become increasingly cloud-native, mobile, and interconnected, the corporate network perimeter is gradually disappearing, exposing users to malware, ransomware, and other cyber threats. Traditional perimeter security tools no longer provide adequate visibility, threat protection, and scalability, nor can they offer convenience and productivity for users on the go.

Protecting sensitive resources of an increasingly distributed company with a large mobile workforce is becoming a challenge that traditional security tools are no longer able to address. The most obvious challenge is the growing number of potential threat vectors, so a simple firewall is no longer sufficient: a proper security gateway has to combine a large number of specialized technologies to cover just the most dangerous ones.

However, an even more crucial problem is the general lack of full visibility across disjointed heterogeneous environments that makes the daily job of a security expert painfully complicated. Beyond the usual security challenges, this leads to a massive compliance problem: the “Shadow IT”. As soon as employees start using their personal devices and unsanctioned cloud services to perform their jobs, this introduces massive potential impacts not just on compliance but may directly lead to a data breach.

An increasingly popular alternative to traditional on-premises security gateways, which are costly, complicated to operate, and create a performance and productivity bottleneck for mobile users, is a security gateway operating directly in the cloud or rather a whole “security cloud” consisting of multiple breakout points across different geographical regions.

With such a solution, every user or device outside of the corporate perimeter can continue using the Internet without any performance penalties and changes in user experience, yet constantly remain protected from the latest cyber threats the same way they used to feel at their office workplace. This way, a secure cloud gateway can be considered the first line of defense in a multilayered “defense in depth” security infrastructure, providing visibility into all internet activities, enforcement of the most important security and compliance policies, and identifying and mitigating cyber-attacks.

The market now offers a substantial number of cloud-based security solutions that vary in their functional

scope, platform coverage, and operational complexity. One crucial distinction among these solutions is the range of network protocols and services that they can intercept, analyzing and mitigating threats in real-time – some solutions may only focus on web traffic, others only on e-mail security, and so on. Relying on a specific interception technology may further limit a solution's ability to protect against specific threats.

In this report, we are looking at available managed cloud-delivered security platforms and ranking them by their protection scope and reliability, coverage and scalability, and, of course, their impact on user productivity. The only key requirement for inclusion in this Market Compass is that the service does not require customers to deploy any hardware on-premises or to make any changes in their existing network infrastructures.

2 Market Segment

In this Market Compass, we attempt to cover the broad market of cybersecurity solutions delivered from the cloud from the end user's perspective, focusing primarily on functional capabilities and user experiences targeted towards end-users: employees, partners, or sometimes even customers. Protecting sensitive resources of an increasingly distributed company with a large mobile workforce is becoming a challenge that traditional security tools are no longer able to address. In addition to the growing number of potential threat vectors, the very scope of corporate cybersecurity has grown immensely in recent years.

To protect multiple remote offices, enterprises must either supply each location with a full stack of security appliances or route all local traffic to a central gateway, which dramatically increases hardware costs and bandwidth losses. Often, smaller locations and mobile users are left completely unprotected. The COVID pandemic has introduced additional challenges for organizations around the world. For years, strict segregation of work and personal activities has been enforced by security and compliance policies, even for BYOD.

Nowadays, when so many employees resort to using their home PCs for remote work, this approach no longer works, and corporate IT and cybersecurity teams are forced to expand their focus towards not just their remote workers but their home devices and even their family members. Unsurprisingly, the demand for cloud-based security solutions increased sharply, and for many companies that were reluctant to try such services earlier making the switch has become the matter of survival of their businesses.

2.1 Market Description

In a traditional perimeterized environment, the role of a central security enforcement point is usually taken by a security gateway that controls all network traffic passing from and to the corporate network. What once was a simple firewall has now evolved into a range of specialized security appliances – malware scanners, content filters, or intrusion detection systems – and to stay on top of the modern threats, companies often have to deploy massive stacks of those just to cover the most dangerous threat vectors.

Such on-premises gateways are expensive and difficult to manage and operate. Even bigger, however, is that their protection does not extend to any user or device outside of the perimeter. In a large company with multiple remote offices, the cost of deploying a full stack of security appliances in every location will be prohibitive. Thus, users outside of the corporate network either have to use a slow VPN connection backhauled to their office or be inevitably left unprotected.

Protection from external threats, however, is not the only challenge in a heterogeneous and de-perimeterized IT environment. The costliest data breaches are often caused by malicious or simply

negligent insiders – internal administrators, contractors, third-party vendors. In fact, nowadays a developer, a business user, or even a C-level executive can have enough privileges to cause a major loss of sensitive information (or even have a corporate bank account drained of funds).

This is why real-time monitoring and analysis of network traffic between users and cloud services is a crucial capability: only when you know with confidence what's going on everywhere in your corporate network and beyond does it become possible to mitigate malicious activities before they turn into a data breach. Cloud Access Security Brokers deployed on-premises have been in use for quite some time; next-generation security platforms are expected to deliver this functionality directly from the cloud.

The last but not least of the challenges most organizations are currently facing is the strong increase in complexity and severity of compliance regulations that deal with managing sensitive personal information as well as data residency requirements. While solutions with large, geographically distributed cloud infrastructures can address these challenges easily by concentrating customer data processing in a local region, all cloud-based security solutions must explicitly incorporate multiple additional data protection and privacy controls to remain compliant with regulations like GDPR or HIPAA.

In this report, we are thus focusing on managed, entirely cloud-based security gateway solutions that offer consistent protection for the mobile workforce regardless of their location inside or outside of a corporate perimeter. Whether large vendors maintaining their global "security clouds" or smaller companies running their platforms in a public cloud infrastructure – the key requirement is that the service does not require customers to deploy any hardware on-premises or to make any changes in their existing network infrastructures.

- Fully managed cloud-hosted security platforms that intercept and secure all or partial network traffic between user devices and the Internet to detect and block cyber threats.
- Efficient, scalable, and ubiquitous access to prevent customers from ever experiencing a performance bottleneck and a negative impact on productivity.
- A broad range of supported network protocols and services, including the ability to analyze encrypted traffic according to corporate policies.
- Rich alerting, reporting, and auditing capabilities to support forensic analysts and compliance auditors.
- Configurable policies to comply with local privacy regulations and other legal frameworks.

For obvious reasons, we are not covering products that require additional hardware or software installation or are primarily delivered for on-premises deployment. Also, we have decided to limit the scope of this Market Compass only to cloud platforms providing security to end-users and their devices, excluding specialized solutions for protecting applications, cloud workloads, IoT devices, or any other class of products we may cover in separate reports. Finally, solutions where security capabilities are not the primary scope (for example, general-purpose SD-WAN platforms).

2.2 Market Direction

The idea to deliver security solutions from the cloud is nearly as old as cloud computing itself. The first generation of such tools was dominated by established security vendors essentially repackaging their existing security appliances as virtual machines deployed on public cloud infrastructures. However, customers have quickly realized that this approach is not sustainable and does not solve most of their challenges, such as scalability, manageability, or additional latency.

In later years, the market has grown and evolved towards cloud-native solutions that can benefit from cloud elasticity and distributed nature to deliver reliable high-performance and low-latency user experience regardless of the end user's location around the world. In that regard, perhaps the most curious phenomenon that could be observed is the convergent evolution of several different approaches taken by different vendors. While manufacturers of traditional security products continued improving their solutions' deployment, management, and analytics capabilities in public clouds, companies previously known as content delivery networks or other types of "edge platforms" have integrated security capabilities into their architectures.

The increasing demand for secure network access management solutions and the rising popularity of the "Zero Trust" approach has led to the emergence of an entirely new class of software-defined perimeter (alternatively, Zero Trust Network Access) products. As opposed to traditional VPN solutions, these dispose with a network-centric approach towards securing access to applications or services and focus instead on maintaining encrypted, authenticated, and monitored point-to-point connections between clients and services. Increasingly, such solutions not only have their control planes entirely in the cloud but incorporate in-line security and compliance functions as well.

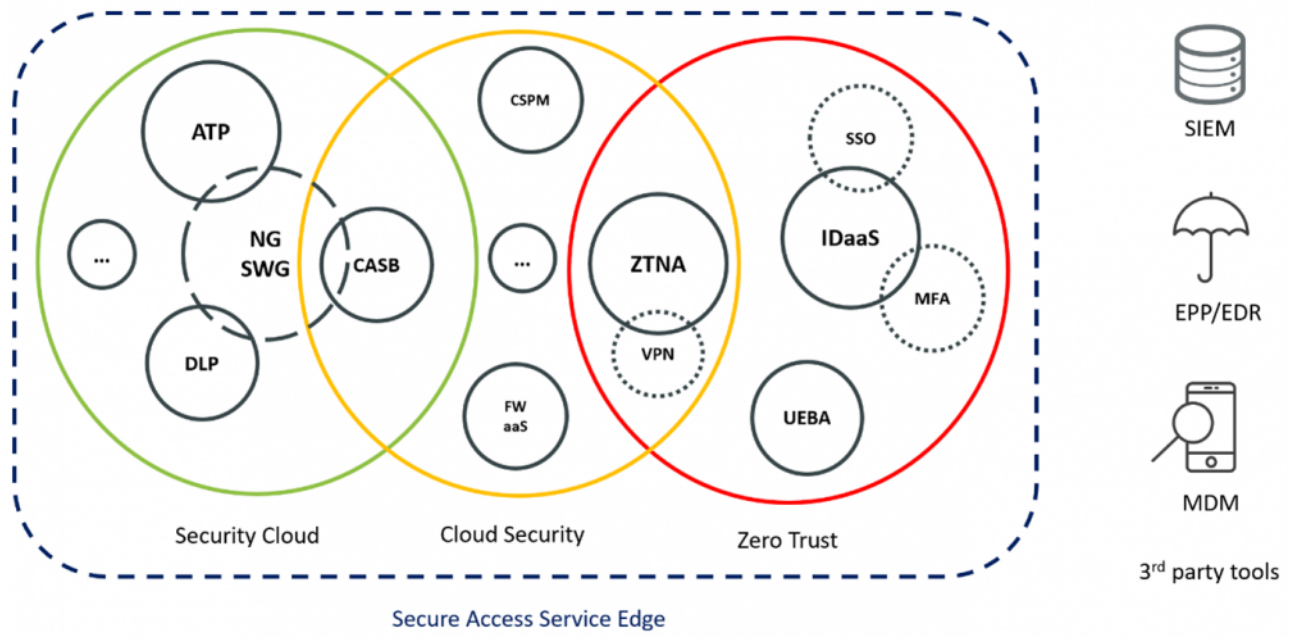


Figure 1: The market for cloud-delivered security solutions is complex, heterogeneous, and difficult to navigate.

This proliferation of a wide variety of access management, threat protection, and activity monitoring tools that are partially or completely based on cloud infrastructures, on one hand, is undoubtedly beneficial for organizations and their employees. On the other hand, however, the abundance of new technologies often marketed under multiple acronyms makes navigating this market quite complicated and confusing. The fact that products with supposedly distinct capabilities, like Cloud Access Security Brokers (CASB), Secure Web Gateways (SWG), and Zero Trust Network Access (ZTNA) can now offer substantially overlapping functionality, makes architecting and budgeting new IT infrastructures even more difficult.

Perhaps the latest attempt to unify this market segment under a single common banner was made recently by Gartner analysts, who have introduced the concept of Secure Access Service Edge (SASE). The idea behind the term is to integrate managed network security capabilities with Software Defined Networking for Wide Area Networks (SD-WAN) and, crucially, Identity as a Service (IDaaS) in a single platform that could address all needs for an organization to enable consistent, dynamic, secure access to sensitive data and applications on an Internet scale. All these capabilities, such as strong authentication, traffic encryption, real-time threat and data loss prevention, as well as continuous monitoring and risk assessment, are expected to be delivered from the cloud in an integrated and managed manner based on a “cloud-native” consumption-based licensing model (although, for obvious reasons, volume- or bandwidth-based licenses are not recommended for any kind of security tools).

It is important to stress that the definition of SASE does not provide any substantial details about the technical implementation or architecture of such a platform. However, it aligns well with the ongoing trend of integration of previously disparate cloud-based security technologies and consolidation of existing solutions through acquisitions of smaller specialized vendors by large veteran security companies. Thus, we can already observe a substantial amount of hype and marketing efforts around the concept and it will

undoubtedly continue to fuel the further development and consolidation of the cloud-delivered security market for the next several years.

Another trend that is very hard to ignore is the post-pandemic reality that forces the majority of business line employees to work from home, outside of whatever still remains as the corporate security perimeter. Although cloud-native security platforms were already steadily increasing in adoption in recent years, the surge in demand starting in early 2020 has been unprecedented, with some vendors even temporarily struggling with scaling their infrastructures to meet it. However, it is the scalability and elasticity of true cloud-native architectures that have allowed the vendors to address these challenges quickly and even be able to offer their services for free during the worst periods of the pandemic lockdown.

So, even though the market for cloud-delivered security solutions is still in a quite early phase of its evolution, it is already growing rapidly and steadily in size, while undergoing continuous changes and consolidation in terms of technologies and capabilities. While it could be argued that vendors that can offer fully integrated SASE solutions are yet to emerge, the market is heading in that direction. However, we expect that it will still take years till it reaches complete homogeneity, and for the foreseeable future, we'll see multiple options for organizations to either opt for multi-functional "security cloud" platforms powered by large cloud or edge infrastructures, focus on designing their own architectures from "best of breed" technological components like NG-SWG or ZTNA or simply to consume specific managed services to address their most burning challenges. It is worth stressing that cloud-delivered security is not limited to secure access and threat protection for web applications. Other potential attack surfaces like APIs, OT and IoT protocols, and even email and instant messaging platforms can and should be covered by such solutions, not to mention protecting specialized cloud workloads.

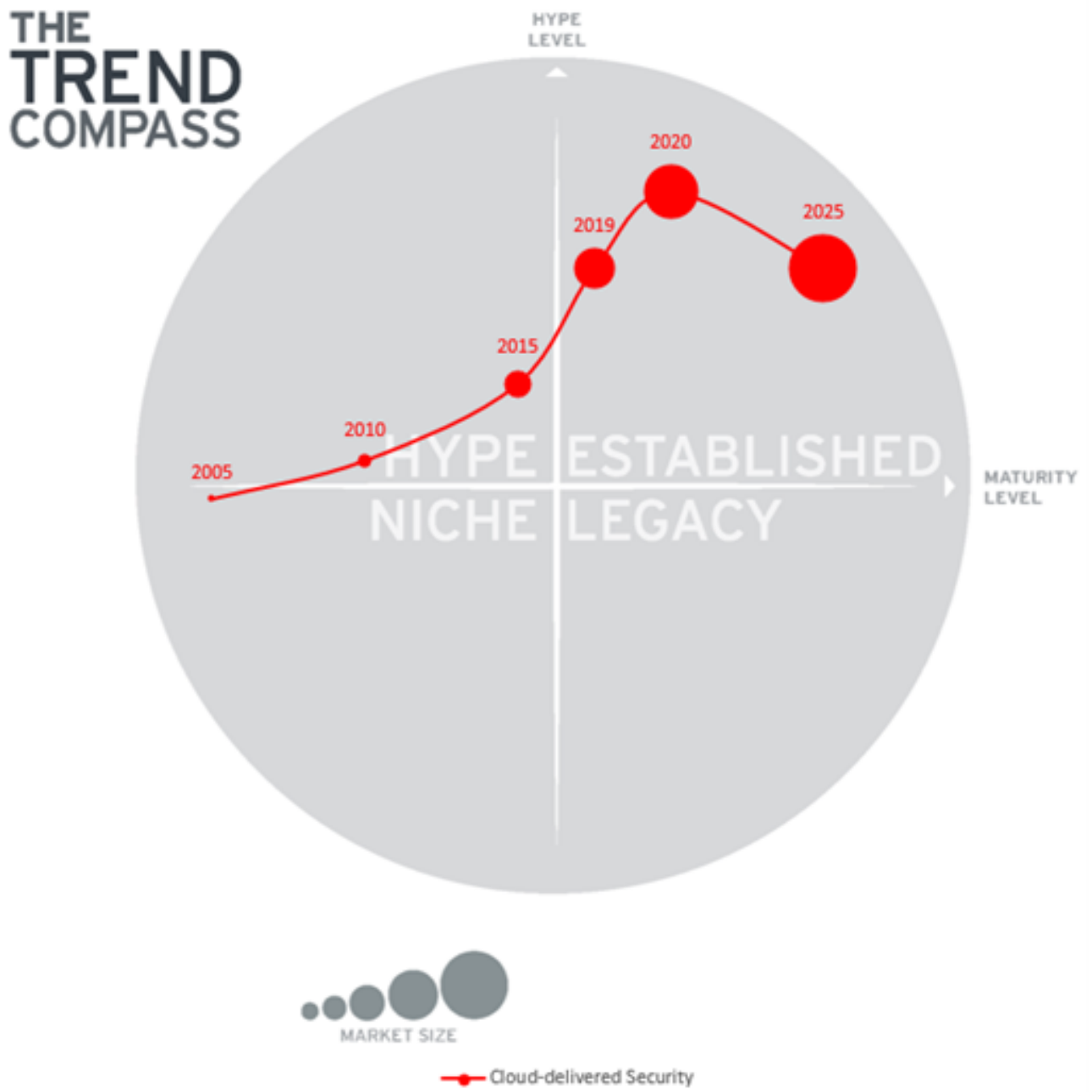


Figure 2: Trend Compass

2.3 Capabilities

Since the market for cloud-delivered security solutions is still far from maturity, and the terminology used by vendors is inconsistent at best, comparing currently available products and understanding their ability to solve specific problems can be a challenge for customers. This is especially challenging in the times of a pandemic crisis when many companies have neither time nor resources to follow proper RFP processes and perform full-scale trials.

This is why KuppingerCole's recommendation has always been to look past product labels and categorizations, focusing instead on identifying the capabilities required to address specific problems and requirements and evaluate products according to their ability to provide those capabilities.

2.3.1 Basic capabilities

Regardless of technology or focus of cloud-delivered security tools, they are expected to provide certain basic capabilities to even qualify as such and to fulfill the most common customer requirements.

Capability	Description	Relevance
Globally distributed cloud infrastructure	The solution must offer availability, resiliency and consistent high performance with low latency across all key geographical regions. As the most critical component of your network infrastructure, it should never become the single point of failure.	Critical
Centralized deployment, management, and operation	The solution must be fully managed and not require on-prem hardware setup or changes in existing infrastructure. Administrators should be able to provision, configure and monitor all services and devices in a central console.	Critical
Compliance with data residency and data protection regulations	In addition to the guaranteed ability to keep all analyzed data within a specific geographic region, this may involve additional configuration options: customers should be able to exclude specific sensitive traffic flows from analysis partially or completely, etc.	Essential
Support for a broad range of endpoints	The solution should provide consistent connectivity and protection capabilities across desktop computers and servers, mobile devices such as smartphones and tablets, even embedded and IoT devices – preferably in a uniform, agentless manner.	Essential
Support for multiple protocols and services	The solution is expected to support multiple methods of capturing or redirecting network traffic for analysis suitable for different platforms and environments. Additionally, it should be capable of blocking any type of malicious or unwanted communication, not just a web session.	Essential
Inline traffic inspection with SSL support	The platform must be capable of fully transparent real-time analysis of network traffic, including encrypted connections (whenever allowed by compliance policies). It's expected not to introduce noticeable latency for users.	Essential

Capability	Description	Relevance
Architecture open for 3rd party integrations	A cloud security platform should be able to integrate with existing on-premises security tools to augment their efficiency as well as share security events with SIEM and other forensic systems. It should be able to provide additional security features and threat intelligence through API-based integrations.	Essential
Real-time monitoring, analytics and alerting	The management console should provide holistic and real-time views into the whole platform's security and compliance posture and inform administrators about operational issues, malicious and suspicious activities.	Essential
Extensible platform with pluggable services	A cloud security platform is expected to be extensible with additional inline security, privacy, compliance or other services, either licensed from the vendor or from 3rd parties through technology partnerships.	Recommended

2.3.2 Advanced functionality

Capability	Description	Relevance
Advanced threat protection	The platform can offer its own or 3rd party capabilities for detection and blocking of advanced persistent threats, ransomware, botnets, browser exploits, etc. using capabilities like cloud sandboxing, machine learning or threat intelligence.	Recommended
Data Loss Protection	Capabilities like URL filtering, DNS filtering, deep packet inspection as well as specialized functionality for e-mail and communication servers can prevent sensitive data exfiltration.	Recommended
Application Control	Application-aware content filtering based on user identity, location or other attributes can help enforce corporate security, compliance and ethics policies.	Recommended
Cloud Access Security Broker	Through integrations with SaaS vendors, the platform can expand security and access management to cloud services and put an end to "shadow IT".	Recommended
Bandwidth management	Provide intelligent prioritization to business application traffic, reduce latency, improve user productivity	Recommended

Capability	Description	Relevance
Privacy enhancement and personal data protection	Sensitive data anonymization, segregation of duty for administrators and other privacy-enhancing functions to comply with regulations like GDPR and CCPA.	Recommended
Software-defined Perimeter / ZTNA	Fully authenticated, secured and policy-driven fine-grained access to applications and data sources regardless of user location helps implement Zero Trust architectures across corporate IT environments.	Optional
Cloud Security Posture Management	Extending security monitoring, auditing and threat protection to cloud workloads help enforce corporate policies uniformly across hybrid and multi-cloud environments.	Optional
E-mail security	By integrating traditional e-mail security capabilities with web-based protection functions (safe links, cloud-based attachment scanning, fraud, and BEC protection, etc.), the solution can significantly boost overall security posture.	Optional
Messaging and social media platform security	Expanding protection to instant messaging platforms, social media and other communication tools also boosts overall security, improves data loss and fraud protection, and strengthens brand reputation.	Optional

3 Vendors & Products

In this report, we have an interesting mix of vendors having different takes on providing fully managed security services delivered from the cloud. Some of these companies have started as providers of traditional security tools and then evolved towards the cloud, while others have started with cloud operations and added security capabilities later. Some have long-established names in the cybersecurity industry, while others have just branched out into this field recently through acquisitions. However, all these vendors offer comprehensive, scalable, and convenient tools to secure your workforce directly from the cloud.

3.1 Vendors Covered

Akamai is a content delivery network and edge service provider headquartered in Cambridge, Massachusetts, USA. Founded in 1998, the company is one of the veteran players on the market, providing a broad range of performance-, security- and even productivity-related services through their content delivery network (CDN), one of the world's largest distributed computing platforms.

Broadcom is a large US-based manufacturer of semiconductor products and supplier of infrastructure software solutions founded in 1961 and currently headquartered in San Jose, California. In 2018, Broadcom expanded into the cybersecurity market by purchasing CA Technologies and later acquiring the enterprise security of Symantec. Nowadays, the company offers a broad portfolio of security solutions under the Symantec brand.

Cisco is a multinational technology company headquartered in San Jose, California, USA. Founded in 1984 by the pioneers of the multi-protocol network router concept, the company has quickly grown into the world's largest manufacturer of networking hardware and telecommunications equipment. In 2015, Cisco acquired OpenDNS, a company that operates one of the world's largest Domain Name System (DNS) infrastructures and extends it with a cloud security product suite, which is now offered under the Cisco Umbrella brand.

Forcepoint is a cybersecurity corporation headquartered in Austin, Texas. Although established in 2016, the company traces its roots back to Websense, a major provider of network security solutions since the late 1990s. In 2015, the company became a subsidiary of Raytheon, a major US defense contractor, but became private again in October 2020. Forcepoint offers a range of "human-centric" data protection, network, and cloud security products.

Ivanti is a software company specializing in IT asset and service management, supply chain management, and IT security headquartered in South Jordan, Utah. Although established in 2017, the company's history can be traced back to the 1980s under the name LANDESK. In 2020, Ivanti acquired Pulse Secure, a

provider of secure access solutions ranging from VPN to ZTNA.

Mimecast is a company specializing in cloud-based email management and security. Founded in 2003 in London, UK, the company currently has over 10 local offices worldwide. With a massive global cloud infrastructure for storing and processing emails, Mimecast offers a range of services for mailbox continuity, archiving, email security, and threat protection, as well as web security, online brand protection, and security awareness training.

Palo Alto Networks is a multi-national cybersecurity company with headquarters in Santa Clara, California. Founded in 2005 by a former engineer from Check Point, the company was the pioneer of the “next-generation firewall” market and continues to be one of the leading providers of both traditional network security tools and modern cloud-native security solutions and services.

Retarus is a privately-owned company developing an enterprise-level cloud platform. Founded in 1992 and based in Munich, Germany, Retarus offers communication services for enterprises, focusing on business integration, process automation, as well as security and compliance for email and other channels.

Zscaler is a global information security company that provides an integrated cloud-based platform for Internet security, compliance, advanced threat protection, and other information security services. Founded in 2008, the company is headquartered in San Jose, California. Zscaler was one of the first vendors to introduce a notion of “security cloud”, currently operating one of the largest specialized cloud security platforms.

3.2 Featured Vendors

Before providing a detailed description of each participating vendor, we would like to highlight several companies for specific features or capabilities that might aid in selecting the most appropriate solution for your specific requirements.

Please note that being featured here does not represent any endorsement from KuppingerCole and does not automatically mean that these vendors are the best fit for every customer. A thorough evaluation of your requirements and risks and mapping available capabilities to address them is still necessary.

3.2.1 Featured for scale and performance: Akamai

Although the company’s history predates even the very notion of “cloud”, over the last two decades Akamai has evolved from a traditional CDN to a full-featured edge platform that not just competes with established cloud providers in multiple areas but complements them with a unified layer of defense and performance. Spanning over 4000 points of presence (POPs) globally, the company’s Intelligent Edge Platform is within direct reach of over 90% of Internet users around the world.

With this global footprint, Akamai can serve numerous large enterprise customers of all industries, including such demanding technology giants as Microsoft, Apple, or Facebook without ever facing performance or scalability bottlenecks. Harnessing the massive reach and performance of Akamai's network, the company's Enterprise Application Access provides consistent secure access to business apps across hybrid IT environments, while the Enterprise Threat Protector ensures that all users and devices are protected from external cyberthreats using the same cloud-based technology without additional performance overhead, administrative complexity, or investments into additional infrastructure.

Figure 3: Featured for Scale and Perormance

3.2.2 Featured for Zero Trust: Cisco

Zero Trust implementation starts with a long-term strategy, where multiple components are selected to be gradually introduced into the corporate network to make it more identity-aware, intelligent and automated, policy-driven, secure and compliant but above all less complex than before. Cisco's approach is to offer not just a set of core technologies to implement zero-trust principles for users, their devices, and the corporate network infrastructure but complements them with a broad range of additional security tools than can be combined as necessary to work together within a larger ecosystem open to third-party vendors as well.

The company offers such technologies as Cisco SD-Access, an intent-based networking solution that enables automated network segmentation for separating user, device, and application traffic without changing the underlying infrastructure; Cisco Secure Workload - the company's hybrid cloud workload protection platform, designed to secure cloud computing resources; Cisco Identity Services Engine (ISE) that provides a cloud-enabled approach to increase visibility into policy controls and zero-trust decision

points within the workplace; or Duo Security - a fully multi-tenant SaaS multi-factor security solution with a range of risk-based capabilities. Last but not least, Cisco Umbrella is a global, large-scale “security cloud" that can intercept and analyze network traffic in real-time to detect a large number of cyber-attacks, data leaks, and other threats.

Figure 4: Featured for Zero Trust

3.2.3 Featured for ease of deployment and use: Zscaler

As businesses become more interconnected, the traditional notion of a network security perimeter gradually ceases to exist. Protecting sensitive resources of an increasingly distributed company with a large remote workforce is becoming a challenge that traditional network-centric security tools are no longer able to address. Over a decade ago, Zscaler pioneered the migration from network-based security appliances towards a unified, cloud-native security platform.

Today, the Zscaler Zero Trust Exchange combines high-performance and scalable zero trust access with integrated data protection and threat prevention, cloud workload protection, and comprehensive network monitoring in a single fully integrated cloud platform. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world’s largest in-line cloud security platform.

Yet, with all this additional functionality, Zscaler is still committed to its original focus: there is no hardware or software to deploy and manage, as well as no network bottlenecks or traffic backhauling to struggle with. All services, policies, and access controls are managed in a single cloud console and changes are propagated instantly across all locations, devices, and users.

Figure 5: Featured for Ease of Deployment and Use

3.3 Vendors to watch

Besides the companies covered in detail in this document, we observe other vendors in the market that have comprehensive security capabilities delivered from the cloud but were for various reasons unable to participate in our rating. We still believe the companies and their solutions deserve a mention, so we provide short abstracts for them below.

Cato Networks is a networking and security company founded in 2015 and based in Tel-Aviv, Israel. Combining SD-WAN and network security capabilities in a cloud-native solution, the company strives to offer a full range of SASE functions in a single platform.

Why worth watching: Since its inception, the company focuses on converging software-defined networking and security into a unified cloud platform. Cato's solution combines a global network backbone, support for all types of devices and connections, and an integrated stack of managed security services to ensure consistent connectivity and protection for users on the Internet scale.

Check Point is an American-Israeli provider of hardware and software solutions for multiple areas of cybersecurity. Founded in 1993 in Israel, Check Point is currently headquartered in San Carlos, CA and Tel Aviv, Israel, offering a broad range of solutions for endpoint, network, and cloud security.

Why worth watching: The foundation of the company's cloud-delivered security portfolio is the Check Point CloudGuard platform – a suite of cloud-based solutions that provide advanced threat prevention, secure and flexible access to on-prem and cloud resources, and unified monitoring and protection for SaaS email and office applications.

Cloudflare is a company focusing on web infrastructure and application security solutions headquartered in San Francisco, California. Founded in 2009, the company has quickly grown from a simple “firewall in the cloud” to one of the leading providers of website performance and security services.

Why worth watching: Although Cloudflare is primarily known for its solutions that protect websites, the company also offers a platform for seamless secure access to corporate resources for users that work from home or on the road. Cloudflare for Teams combines a Zero Trust access solution to replace aging VPNs with a software-defined perimeter and a Secure Web Gateway to protect users from Internet threats. The platform is even free for small teams.

Cyren is a cloud security vendor established in 1991 and headquartered in McLean, Virginia. With its large security cloud, the company offers a range of solutions for email security, protection from attacks, and threat intelligence.

Why worth watching: Cyren offers several solutions for enterprise customers, including Inbox Security for Office 365 providing continuous and fully automated protection against sophisticated email attacks like phishing and BEC as well as Threat Intelligence services to help companies address these threats on a larger scale. The company also OEMs its email and web security technologies to MSSPs and other security vendors.

Fortinet is a cybersecurity company founded in 2000 with headquarters in Sunnyvale, California. It offers a wide range of network security and SD-WAN, network access control, authentication, public and private cloud security, endpoint security, and advanced threat protection solutions.

Why worth watching: as a veteran network and security vendor, Fortinet offers a massive selection of tools and services to design any enterprise’s security architecture, both on-premises or in the cloud. For this Market Compass, however, we’d like to highlight the cloud-delivered web and SaaS security products like Fortinet Secure Web Gateway for protecting against Internet threats and FortiCASB, a cloud access security broker for managing and securing SaaS applications.

iBoss is a network security vendor based in Boston, Massachusetts. Founded in 2003, the company provides a cloud-based platform for secure connectivity between on-prem and cloud destinations.

Why worth watching: iBoss provides an integrated, yet containerized and extensible cloud-native network security platform that supports any cloud, any network, and a broad range of devices to ensure secure and compliant access from any location. It combines the convenience of a fully managed SaaS offering with the flexibility of more traditional modular enterprise solutions.

McAfee is a security software company headquartered in Santa Clara, California. Founded in 1987 and acquired by Intel in 2011, it was known as Intel Security until 2017, when it was re-established as a separate company.

Why worth watching: the company’s MVISION security platform spans both endpoint devices and the cloud to provide open, insight-driven enterprise security architecture. MVISION Unified Cloud Edge is a cloud security platform that combines Data Loss Prevention, Secure Web Gateway, and Cloud Access Security Broker capabilities to ensure consistent data and threat protection delivered from the cloud.

Menlo Security is a network security company headquartered in Mountain View, California. Founded in 2013, the company focuses on eliminating web and email security threats through a cloud-based isolation platform.

Why worth watching: the company's Security Isolation Platform moves the web content execution from endpoints to a cloud-based platform, ensuring that users are never exposed to web and email threats and only receive safely rendered content locally. Based on this technology, Menlo Security offers a full stack of security tools including data loss prevention, cloud firewall, Zero Trust access, and CASB, among others.

Netskope, founded in 2012, is a cloud-native security vendor based in Santa Clara, California with offices across the US, UK, Australia, India, Singapore, and Japan.

Why worth watching: Netskope's Security Cloud combines comprehensive visibility, data protection, and threat prevention for websites, cloud services, and enterprise applications. The company's Cloud XD technology enables data-centric protection beyond traditional DLP and CASB, provides granular visibility into users, devices, and application activities, and protects users of cloud services from advanced threats. Integrating with leading identity-as-a-service (IDaaS) providers, Netskope can offer full SASE capabilities to enterprise customers.

Proofpoint is a security and compliance company founded in 2002 and based in Sunnyvale, California. The company offers a range of solutions for email security, advanced threat protection, cloud security, and compliance.

Why worth watching: Proofpoint has been a leading email security and compliance solution provider for years, offering comprehensive protection from advanced email, mobile, social, and desktop cyberthreats. More recently, the company has branched into cloud security, offering a Cloud Access Security Broker solution with a unique "people-centric" approach to identify and protect the Very Attacked Persons in your company.

VMware is a software company established in 1998 and based in Palo Alto, California. Known primarily for its virtualization and cloud computing solutions, the company has expanded into other network- and cybersecurity-related markets as well.

Why worth watching: In 2017, VMware acquired a leading SD-WAN vendor VeloCloud in 2017, entering the market for cloud-delivered secure access solutions. Currently, the company offers a full-fledged SASE platform that combines Zero Trust network access, Secure Web Gateway, Next-generation Firewall and CASB functions with additional capabilities like workspace and application delivery, cloud workload management and security and many others, all in a unified, holistic solution.

4 Ratings at a Glance

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in table 1 below.

Product	Security	Interoperability	Usability	Deployment	Data Protection	Web Security	Email Security	Zero Trust Access
Akamai	●	●	●	●	●	●		●
Cisco	●	●	●	●	●	●	●	●
Forcepoint	●	●	●	●	●	●	●	●
Mimecast	●	●	●	●	●	●	●	
Palo Alto Networks	●	●	●	●	●	●	●	●
Pulse Secure	●	●	●	●	●	●		●
Retarus	●	●	●	●	●	●	●	
Symantec	●	●	●	●	●	●	●	●
Zscaler	●	●	●	●	●	●	●	●
Legend					● critical	● weak	● neutral	● positive ● strong positive

5 Product / Service Details

5.1 Akamai

Akamai is a content delivery network and edge service provider headquartered in Cambridge, Massachusetts, USA. Founded in 1998, the company is one of the veteran players on the market, providing a broad range of performance-, security- and even productivity-related services through their content delivery network (CDN), one of the world's largest distributed computing platforms.

Akamai's Intelligent Edge Platform aims to provide to a company of any size, without the need to invest in additional infrastructure or security expertise. The company's approach towards achieving Zero Trust security is to start the journey by enforcing the least-privilege access model consistently for all business applications using the Enterprise Application Access (EAA) service built on Akamai's cloud platform. This ensures that every such application is completely hidden from "trusted" public exposure regardless of where it is hosted – in a corporate LAN, on-premises datacenter, or public cloud – with access secured with means like multi-factor authentication (MFA), single sign-on (SSO) and enforcement of company-wide security and compliance policies.

Since the solution is completely offered as a service, there is no additional network hardware or security appliances to deploy and maintain. There is also no need for an inbound VPN for external users – Akamai does not require any direct connection to the customer's infrastructure at all. Once authenticated, users can "carry" their identities across multiple applications, even if those do not support this natively – the platform takes care of the needed transformations. For each request, the authorization platform will evaluate multiple contextual factors related to the identity of the user, geolocation, time of the day, device posture and so on to make a dynamic real-time access decision according to the active policy.

To extend protection from what used to be known as a "corporate network" to the rest of the Internet, Akamai complements EAA with another service, Enterprise Threat Protector (ETP). By forwarding user traffic to the Akamai platform using software agents or DNS-level redirection, customers can ensure that any such request will be validated against Akamai's constantly updated threat intelligence database, and access to any known malicious destinations are automatically blocked.

Additionally, real-time cloud-based malware scanning using multiple detection engines and offline sandboxing allows the solution to detect and immediately block a wide range of malware, from executables to macros in office documents and even malicious scripts. Integrated Data Loss Prevention allows organizations to identify the posting of sensitive information that might breach regulatory compliance. Application Visibility and Control allows the identification and control of Shadow IT based on application category or risk score.

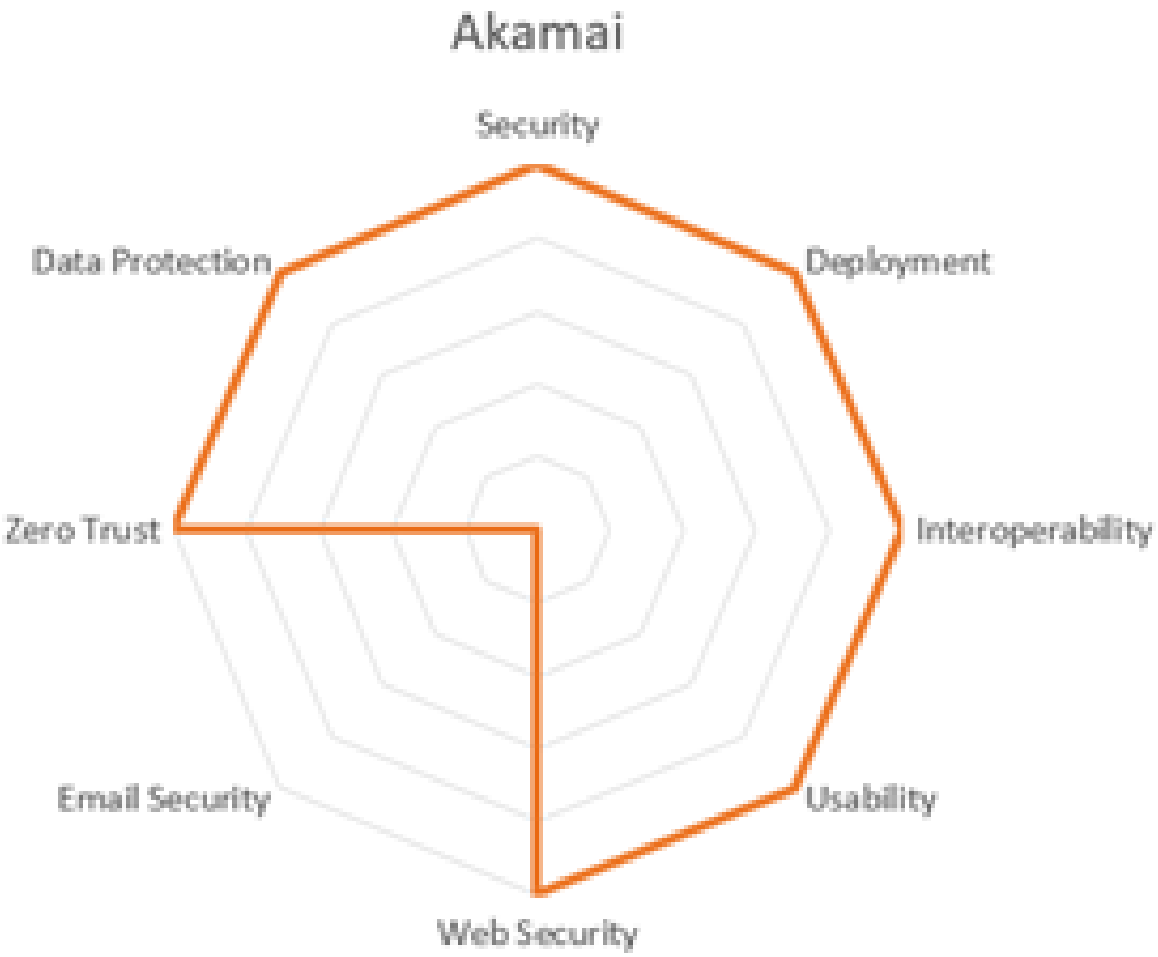
Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Data Protection	● ● ● ● ●
Web Security	● ● ● ● ●
Zero Trust Access	● ● ● ● ●

Strengths

- Massive scale and availability of Edge infrastructure in every region of the world
- No need to deploy and maintain any additional hardware infrastructure
- Consistent enforcement of secure access policies for hybrid environments, any network protocol
- Identity-agnostic, direct integrations with multiple on-prem or cloud IAM solutions
- Multiple layers of threat protection - DNS, URL and content

Challenges

- Targeted primarily at large enterprises, might be complicated for SMBs
- Multiple software agents are required for consistent access control and threat protection beyond web apps
- Does not cover e-mail security


Akamai
Security
Deployment
Interoperability
Usability
Web Security
Email Security
Zero Trust
Data Protection

5.2 Symantec (was acquired by Broadcom Inc.)

Broadcom is a large US-based manufacturer of semiconductor products and supplier of infrastructure software solutions founded in 1961 and currently headquartered in San Jose, California. Since the acquisition of Symantec in 2018, the company offers a broad portfolio of security solutions under the Symantec brand, covering such areas as endpoint security, web, and email security, data protection, and identity security.

With such a broad selection of tools, many of which were obtained through acquisitions, one of the goals of Symantec as a business unit of Broadcom is to integrate them into a unified security platform for consistent, scalable, and convenient customer deployment. The company refers to this as the Symantec Cyber Defense Platform, which is aiming to consolidate all available products and services.

One of the key components of this platform is Symantec Web Security Service that provides web security and threat protection, cloud application and data control, as well as security for Office 365. Delivered as a cloud-based service, it combines the functionality of the company's proven ProxySG secure web gateway with CASB capabilities of Symantec CloudSOC and a Cloud Firewall Service for non-web traffic. With further integrations with other Symantec solutions like DLP Cloud and Global Intelligence, it provides a comprehensive platform for protecting users against a multitude of cyber threats and to prevent data leaks and breaches.

In addition, Broadcom's portfolio includes Symantec Secure Access Cloud, a Zero Trust network access platform developed by Luminate Security, a company acquired by Symantec in 2019, that enables secure, policy-driven access to on-prem and cloud resources and applications. Delivered completely from the cloud, it supports quick, agentless deployments on a broad range of devices. It also integrates well with other Symantec products and 3rd party solutions, providing a foundation for designing SASE-like converged network and security architectures.

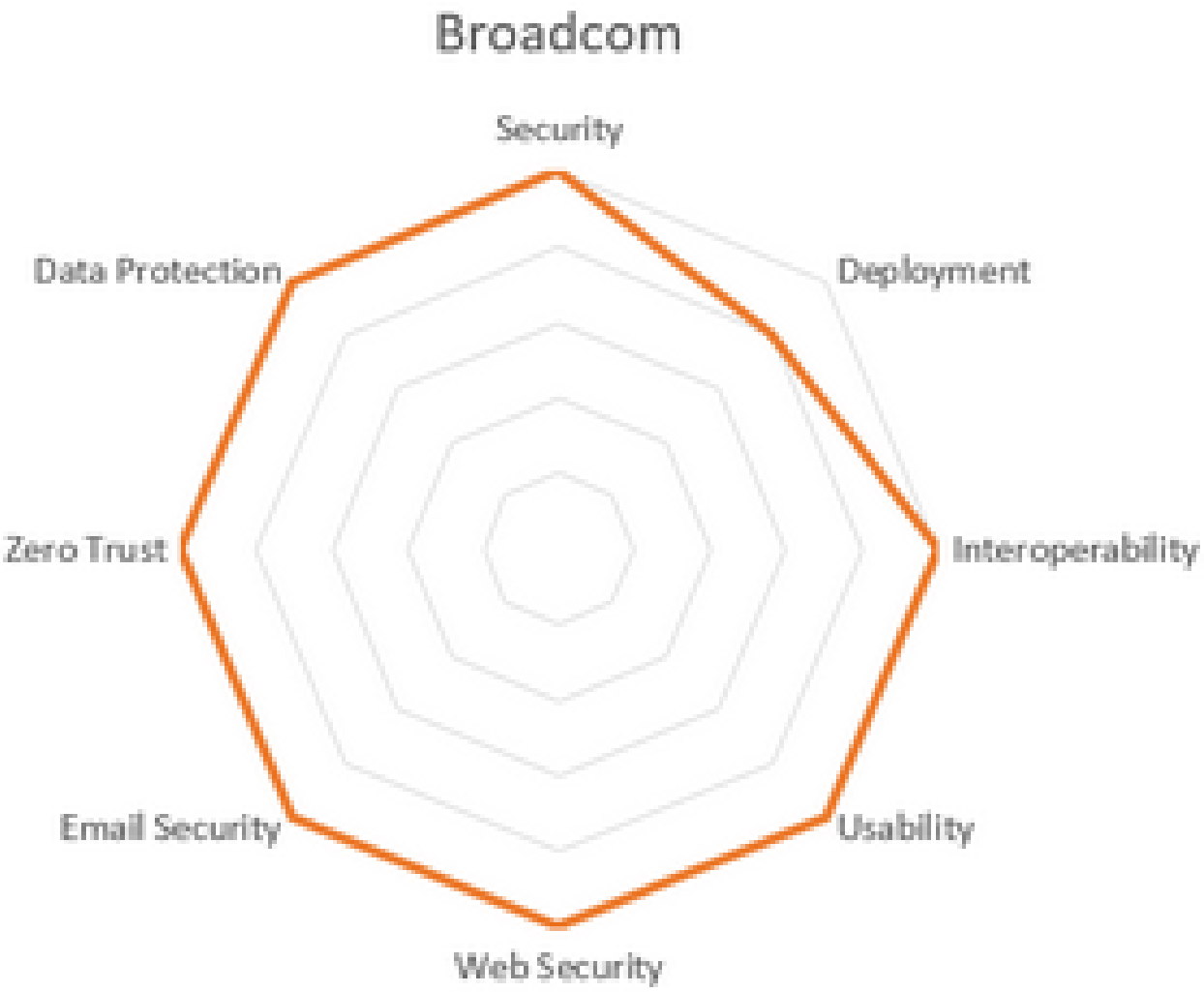
Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ○
Data Protection	● ● ● ● ●
Web Security	● ● ● ● ●
Email Security	● ● ● ● ●
Zero Trust Access	● ● ● ● ●

Strengths

- Comprehensive and capable web security and CASB solution with broad cloud app coverage
- A powerful ZTNA platform to enable secure access to all business apps
- Integrated Cyber Defense Platform to unify cloud and on-premises security
- One of the largest global threat intelligence networks

Challenges

- Full functionality is only reached after the deployment of multiple products
- Platform-level integration is yet to be achieved


Broadcom
Security
Deployment
Interoperability
Usability
Web Security
Email Security
Zero Trust
Data Protection

5.3 Cisco

Cisco is a multinational technology company headquartered in San Jose, California, USA. Founded in 1984, the company is the world's largest manufacturer of networking hardware and telecommunications equipment. Since 2015, when Cisco acquired OpenDNS, a company that operates one of the world's largest DNS infrastructures and extends it with a cloud security product suite, it is now offered under the Cisco Umbrella brand.

Since the Umbrella cloud processes billions of DNS requests from millions of users around the world every day, it collects an immense amount of security intelligence about malware, URLs, and domains across the internet. In addition, it can tap directly into the reputation database maintained by Talos Intelligence Group that powers all of Cisco's security products. Thus, even before a network connection is established, Umbrella can already determine whether it is associated with any kind of known risky activity as well as classify it according to over 60 predefined content categories.

For known malicious destinations like malware command and control domains or fraudulent websites, or simply to enforce acceptable use policies, a connection will be immediately blocked. For less risky domains, or to allow deep inspection of specific URLs, a DNS request will be transparently resolved to the Umbrella proxy service, which will perform real-time analysis using Cisco Advanced Malware Protection.

In addition to DNS security and a secure web gateway, the Umbrella platform integrates multiple additional security solutions, such as a Firewall-as-a-Service, the Cloudlock cloud-native CASB for protecting SaaS applications, Stealthwatch Cloud for cloud analytics and threat detection, Cloud Mailbox Defense for email security, and so on. Cisco SecureX platform provides a simplified integrated experience that connects the company's cloud-based solutions with customers' on-prem infrastructures, providing visibility and quick remediation workflows.

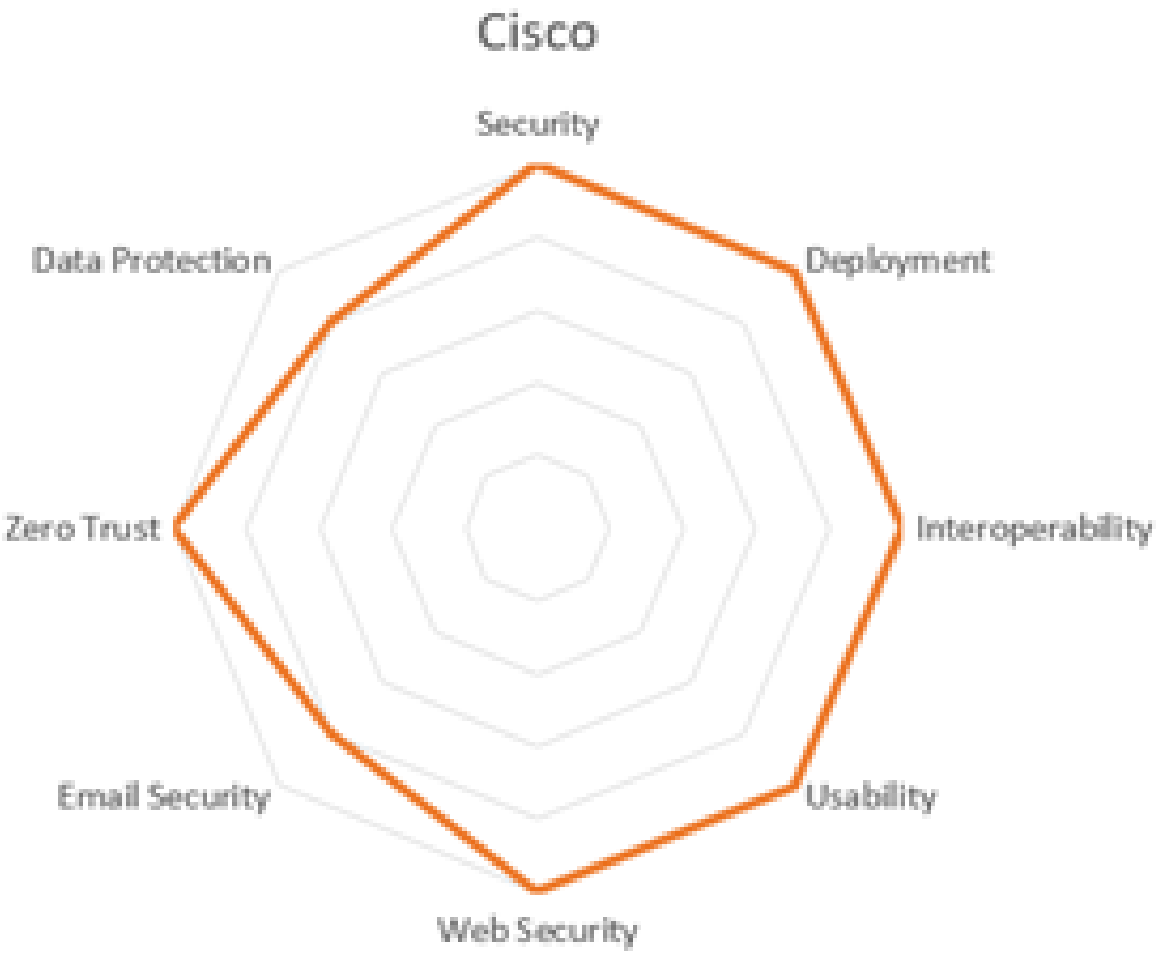
Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Data Protection	● ● ● ● ○
Web Security	● ● ● ● ●
Email Security	● ● ● ● ○
Zero Trust Access	● ● ● ● ●

Strengths

- Implements Zero Trust for users, devices, networks, and applications
- A broad range of solutions to implement security consistently across on-prem and cloud
- Comprehensive risk-based and adaptive access capabilities with endpoint visibility
- Simplified integrated security experience platform
- Open ecosystem with many third-party integrations and partnerships

Challenges

- Some components are primarily targeted towards enterprises with large own IT infrastructures, less suitable for smaller companies
- Cloud deployments limited to AWS public cloud


Cisco
Security
Deployment
Interoperability
Usability
Web Security
Email Security
Zero Trust
Data Protection

5.4 Forcepoint

Forcepoint is a cybersecurity corporation headquartered in Austin, Texas. Although established in 2016, the company traces its roots back to Websense, a major provider of network security solutions since the late 1990s. Since 2015, the company is a subsidiary of Raytheon, a major US defense contractor. Forcepoint's behavior-based solutions adapt to risk in real-time and are delivered through a converged security platform that protects network users and cloud access, prevents confidential data from leaving the corporate network, and eliminates breaches caused by insiders.

The foundation for the company's portfolio is the Forcepoint Dynamic Security Platform – a highly modular yet integrated, cloud-first but hybrid-ready technology platform that can deliver a broad selection of behavior monitoring, data protection, and threat intelligence functions. Individual capabilities are implemented as microservices that, connected via APIs with agents deployed on endpoints focus on performing continuous behavioral analysis of users, devices, and applications. As opposed to more traditional UEBA products, Forcepoint does not focus on forensics and manual mitigation; instead, it performs continuous risk evaluation and intervenes automatically with measures like forced re-authentication using MFA.

On top of this platform, the company offers three distinct security products. Dynamic User Protection is a cloud-based user activity monitoring solution that provides real-time visibility and risk assessment of users based on high-level Indicators of Behavior instead of individual activities. The goal is to identify and isolate risky users before their actions lead to a data breach.

Dynamic Data Protection is a data discovery, classification, and governance solution that combines data loss prevention with dynamic behavior analysis to enforce the Zero Trust paradigm to any enterprise data, on-prem or in the cloud.

Dynamic Edge Protection, the latest addition to Forcepoint's portfolio, is a cloud-based SASE solution that combines cloud data protection, advanced threat protection, and secure access to private apps and integrates it with the company's user behavior and risk monitoring capabilities.

Security	●●●●●
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○
Data Protection	●●●●●
Web Security	●●●●●
Email Security	●●●●○
Zero Trust Access	●●●●○

Strengths

- Modern, cloud-native, modular architecture aligns well with SASE, Zero Trust paradigms
- Strong focus on human behavior analytics and real-time risk assessment
- Major productivity boost for security analysts compared to traditional SIEM/UEBA
- Convenient one-price, unlimited consumption licensing model

Challenges

- Full range of email security capabilities relies on hybrid deployments
- Relatively small partner ecosystem


Forcepoint
Security
Deployment
Interoperability
Usability
Web Security
Email Security
Zero Trust
Data Protection

5.5 Pulse Secure (was acquired by Ivanti)

Ivanti is a software company specializing in IT asset and service management, supply chain management, and IT security headquartered in South Jordan, Utah with a history going back to the 1980s, when it was known under the name LANDESK. In 2020, Ivanti has acquired Pulse Secure, a provider of secure access solutions, which traces its history to the remote access business of Juniper Networks and has nearly two decades of R&D in various related technologies.

Pulse Secure's existing portfolio contains solutions for VPN, application delivery, IoT security and network management and analytics. In 2020, the company has introduced Pulse Zero Trust Access – a new, cloud-based SaaS secure access platform that implements the concepts of Zero Trust network architectures but allows customers to adopt Zero Trust at their own pace by enabling hybrid configurations under a single control pane.

The PZTA platform enables direct and convenient, yet secure and continuously authenticated access for any users and locations to any kind of application or data source. Delivered as a multi-tenant SaaS platform, where the central controller is managed by the company, it supports quick deployments of Zero Trust gateways on-prem or in any cloud but also seamlessly connects to existing networks where other Pulse Secure products are operated.

Endpoints that have existing client software can also connect to the new platform without any changes. This way, customers can mix and match traditional VPN and remote access solutions with modern ZTNA architectures to enable faster adoption and easier migrations over time.

Advanced capabilities of the platform include full visibility and analytics for network activities as well as the built-in user and entity behavior analytics (UEBA) to identify suspicious and malicious activity in real time and perform quick threat mitigation.

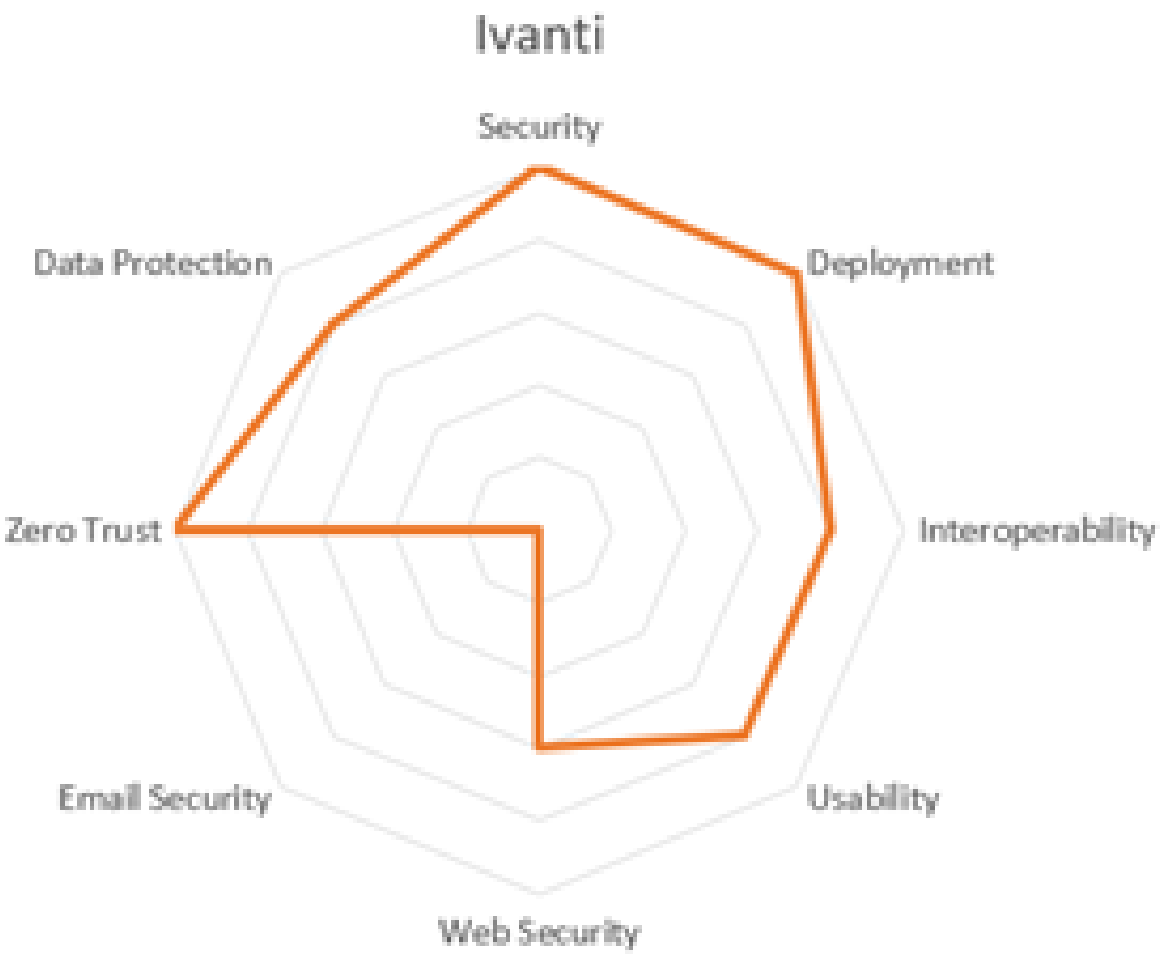
Security	●●●●●
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●●
Data Protection	●●●●○
Web Security	●●●○○
Zero Trust Access	●●●●●

Strengths

- Comprehensive Zero Trust Network Access platform that integrates seamlessly with existing remote access tools
- SaaS delivery model enables quick deployments and integrations
- Full encryption of all user and application data for privacy and data sovereignty
- Advanced monitoring, analytics, and threat mitigation capabilities

Challenges

- Web and email security in the traditional sense is not the focus of the solution
- Unclear long-term strategy after the acquisition


Ivanti
Security
Deployment
Interoperability
Usability
Web Security
Email Security
Zero Trust
Data Protection

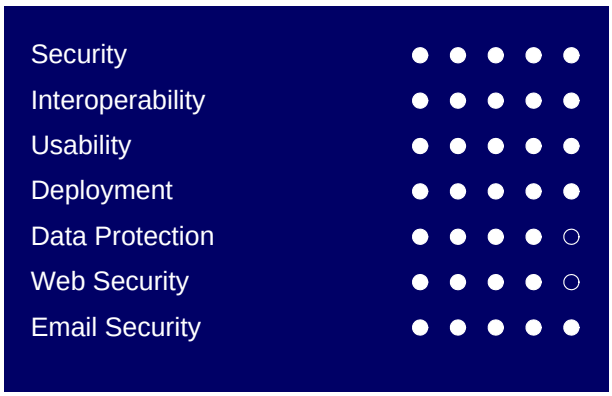
5.6 Mimecast

Mimecast is a company specializing in cloud-based email management and security. Founded in 2003 in London, UK, the company currently has a worldwide presence with a massive cloud infrastructure for storing and processing emails. Mimecast offers a range of services for mailbox continuity, archiving, email security, and threat protection, as well as web security, online brand protection, and security awareness training.

Mimecast has been consistently recognized by the expert community as one of the leading email security solutions and not without reason. Built on a common cloud-based multi-tenant Mime|OS architecture developed by Mimecast, the company can offer a massive selection of products and services that cover all aspects of email security, from email continuity and threat protection to such specialized tools like DMARC Analyzer and Brand Exploit Protect that help to maintain brand reputation by preventing email domain and website spoofing.

Mimecast's secure email gateway service provides a full set of threat protection capabilities including anti-spam, malware and zero-day attack detection, spear-phishing protection, as well as protecting users from malicious websites, social engineering/impersonation, and ransomware-based attacks. This includes inspecting outgoing emails as well and even internal emails that never leave your corporate mail server or cloud-based email system such as Microsoft 365 or Google Workspace, to ensure that no sensitive data can leak uncontrollably or that attacks are not spreading outbound or laterally.

Most recently, Mimecast has strengthened its artificial intelligence detection capabilities with two new technologies: the first is the use of computer vision to detect logos belonging to highly phished brands on web sites; the second is an identity graph which uses machine learning to understand sender/recipient behaviors so that anomalous behaviors can be treated with suspicion. Mimecast Web Security service helps extend threat protection beyond emails. A cloud-based web security gateway, it uses DNS-level traffic redirection to prevent users from visiting malicious or inappropriate websites or downloading infected files, and to prevent compromised devices from connecting to C&C servers.



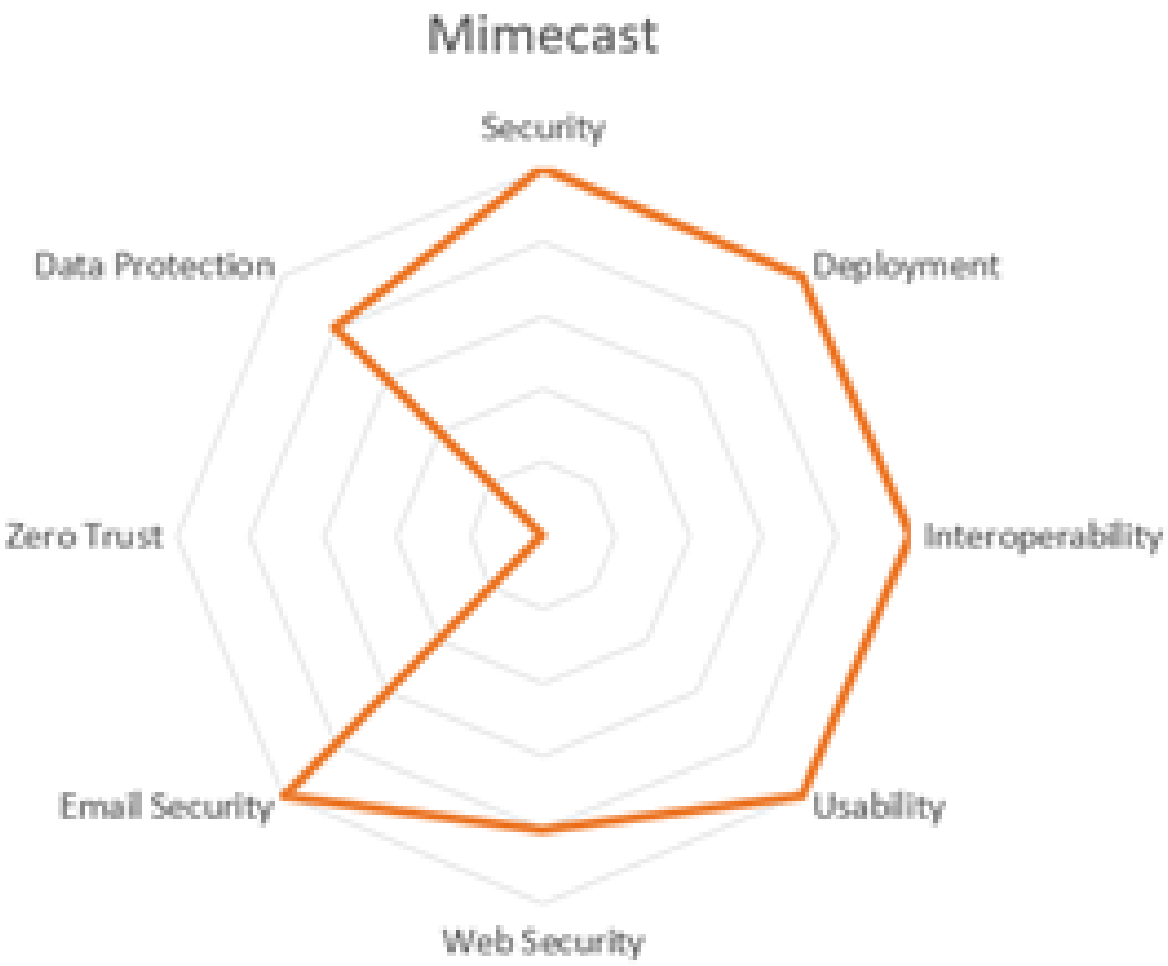
mimecast™

Strengths

- Powered by a common multi-tenant, cloud-native architecture developed internally
- A broad range of products, covering all aspects of email security and beyond
- Information protection capabilities like DLP, secure messaging, and large attachment handling
- A massive number of supported integrations for security and automation
- Security awareness training services

Challenges

- Does not cover Zero Trust network access
- Not all products are integrated into the single UI
- Initial setup can be challenging for some users


Mimecast
Security
Deployment
Interoperability
Usability
Web Security
Email Security
Zero Trust
Data Protection

5.7 Palo Alto Networks

Palo Alto Networks is a multi-national cybersecurity company with headquarters in Santa Clara, California. Founded in 2005, the company was the pioneer of the “next-generation firewall” market and continues to be one of the leading providers of both traditional network security tools and modern cloud-native security solutions and services.

The company’s cloud-based and cloud-focused security solutions are currently offered under the Prisma brand. Prisma is a comprehensive suite of services to predict, prevent, detect, and mitigate security and compliance risks in cloud environments, SaaS applications, and corporate networks. Built upon the company’s proven next-gen firewall technology in virtualized or containerized form factors and the SD-WAN platform acquired from CloudGenix, the company currently offers three cloud-native security solutions.

Prisma Access is a cloud-native platform that combines network-as-a-service and security-as-a-service layers in a unified architecture that aligns well with the SASE concept. Prisma Access enables secure, controlled and consistent access of remote users and branch locations to corporate and cloud-based applications and resources consolidating multiple point-products into a single converged platform that includes firewall-as-a-service capabilities, built-in secure web gateway, and threat intelligence from Palo Alto and its partners.

Prisma SaaS is a cloud service that allows organizations to govern sanctioned SaaS application usage across all their users. With comprehensive Cloud Access Security Broker (CASB) capabilities, the solution helps in discovering cloud risks, preventing data loss, improving the compliance posture, and controlling the use of shadow IT. Prisma SaaS is integrated with Prisma Access to enable full SASE capabilities.

Prisma Cloud is a cloud-native security platform that offers deep visibility and threat detection for various types of cloud workloads: from virtual machines to containers, serverless, and data stores. Its modular, hybrid architecture allows for complex deployments across on-prem and multi-cloud environments to provide a unified view into security posture across the whole enterprise.

Security	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○
Data Protection	●●●●○
Web Security	●●●●●
Email Security	●●●○○
Zero Trust Access	●●●●●

Strengths

- Complete implementation of the SASE paradigm
- On-prem and multi-cloud support make complex hybrid deployments possible
- Comprehensive management and analytics capabilities
- Seamlessly extends into DevSecOps and cloud-native security

Challenges

- Full functionality is achieved only by the deployment of several solutions; not available as a suite or platform offering
- No single management console available yet


Palo Alto Networks
Security
Deployment
Interoperability
Usability
Web Security
Email Security
Zero Trust
Data Protection

5.8 Retarus

Retarus is a company developing enterprise-level cloud solutions that support mission-critical messaging and business communications. Founded in 1992 and based in Munich, Germany, the company's been focusing primarily on enabling businesses to expand and automate their communications with partners and customers. The company's portfolio is built around a cloud-based unified communications platform for enterprises, focusing on business integration, process automation, security, and compliance for email and other channels.

The platform is capable of handling multiple communication types, including emails, faxes, and text messages, providing full lifecycle management for this "digital logistics" - including delivery, sorting, classifying incoming communications, converting to structured formats, etc.

Retarus Secure Email Platform is a specialized solution providing a complete solution for email including email security and continuity, transactional and marketing email, real-time monitoring and analytics, as well as workflow and smart routing services. However, mail security is offered as a standalone service.

The platform provides a full stack of email security capabilities, starting with basic functions like traffic management, anti-malware detection, or antispam and spoofing protection to more advanced capabilities like AI-based anti-phishing, CEO fraud prevention, and cloud sandboxing for detecting unknown threats.

Although Retarus doesn't directly provide web security tools, a substantial part of the platform is devoted to post-delivery protection that does not just prevent opening malicious links but helps prevent social engineering attacks and even remove older emails after new threats are recognized later.

The platform can also massively improve data protection and compliance by introducing managed pervasive digital signatures and encryption with S/MIME, PGP, or OpenPGP. Compared to traditional decentralized deployments, this managed approach simplifies user enrollment, improves productivity, and allows for advanced multi-channel use cases powered by the Retarus Cloud.

Security	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●●
Data Protection	●●●●●
Web Security	●●●○○
Email Security	●●●●●

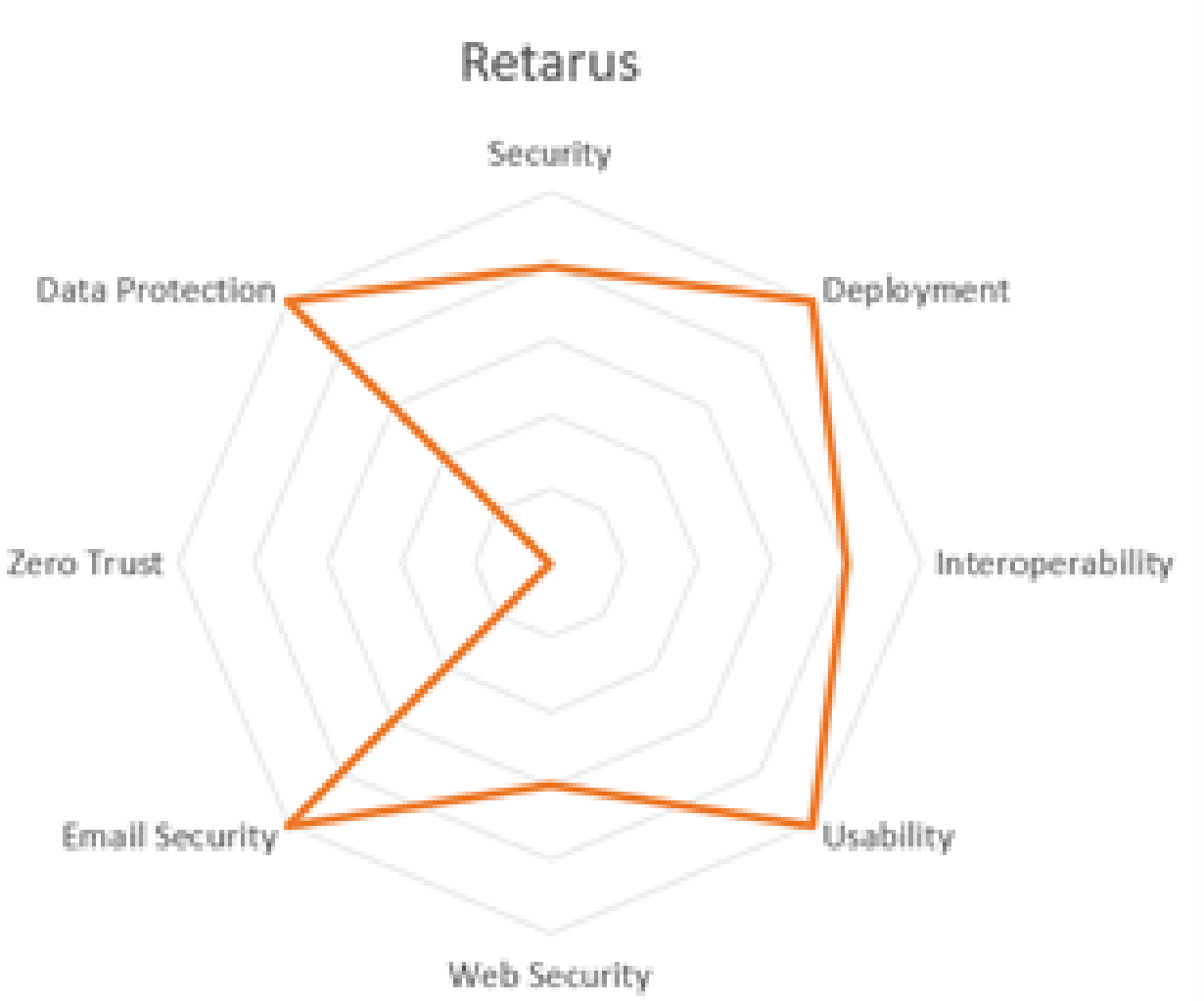
retarus

Strengths

- A holistic approach towards communications beyond just email
- Strong focus on compliance for large enterprises, including full GDPR compliance
- Protection from all types of email-based threats and risks
- Full-lifecycle encryption supporting multiple protocols and methods
- Global communications cloud with strong automation capabilities, own infrastructure in all major regions

Challenges

- Still relatively small visibility in the security market
- Security capabilities rely in part on 3rd party technologies
- Does not cover Zero Trust network access


Retarus
Security
Deployment
Interoperability
Usability
Web Security
Email Security
Zero Trust
Data Protection

5.9 Zscaler

Zscaler is a global information security company founded in 2008 and headquartered in San Jose, California. Zscaler was one of the first vendors to introduce a notion of “security cloud”, currently operating one of the largest specialized cloud security platforms for Internet access security, securing mobile workers, compliance assurance, advanced threat protection, and other security services. The Zscaler Zero Trust Exchange platform comprises thousands of Enforcement Nodes – specialized internet gateways performing traffic analysis and applying security policies in over 150 data centers around the world.

Consistent with its initial “no hardware” promise, Zscaler supports multiple methods of forwarding traffic from individual devices or whole networks such as tunneling, proxy configurations, and client connectors. Able to intercept both outbound traffic and inbound responses for all devices (including SSL-encrypted connections), it can apply multiple types of traffic analysis in real time, as well as combine them with historical data from their security cloud and external sources of threat intelligence.

This infrastructure provides a foundation for Zscaler’s Zero Trust Exchange, a cloud platform that secures all enterprise traffic based on the principles of zero trust access and ensures a good user experience by connecting through the node closest to the user location. Built to support the SASE framework, it combines secure Internet Access, a secure gateway with multiple threat protection, data loss prevention, and monitoring features, Private Access to public cloud and Data center applications, and Cloud Protection, a solution for remediating cloud workload risks. Zscaler’s platform provides a fully managed, scalable and lightweight solution to multiple security and compliance challenges for an organization of any size.

As opposed to many competitors, Zscaler’s portfolio is completely based on a single, fully integrated, and fully zero trust managed architecture, ensuring quick and smooth initial adoption and seamless expansion when needed. Single management console and consolidated monitoring ensure full visibility into performance and security metrics for any user, device, or application.

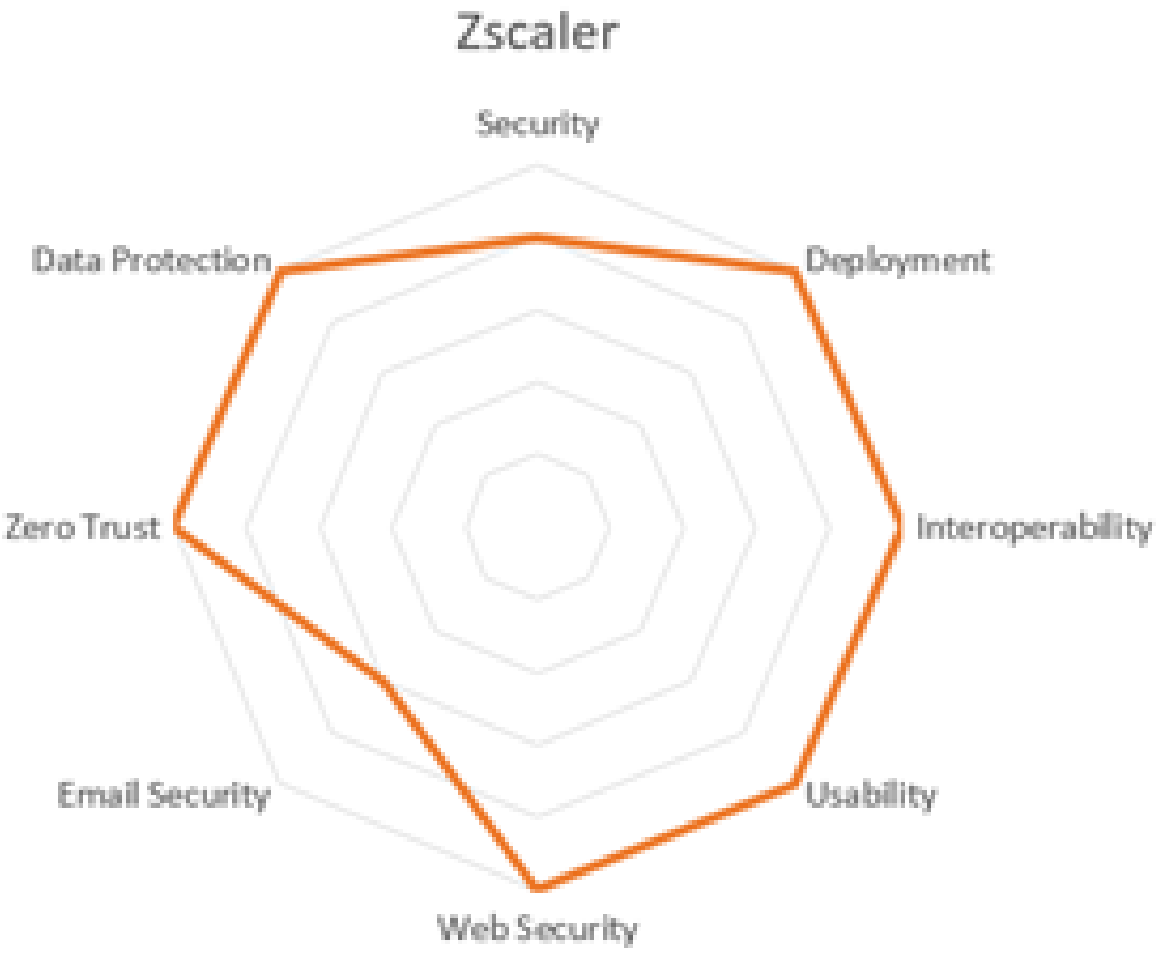
Security	●●●●○
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●●
Data Protection	●●●●●
Web Security	●●●●●
Email Security	●●●○○
Zero Trust Access	●●●●●

Strengths

- Unified Security-as-a-Service cloud platform without any hardware or software needed
- Massively distributed architecture optimized for scale ensures high performance and reliability
- Real-time inspection of all traffic, including encrypted connections, ensures comprehensive threat protection and data loss prevention capabilities
- Fine-grained secure access to on-premises and cloud applications based on the Zero Trust principle
- A unified client app with broad platform support simplifies the user experience

Challenges

- Zscaler Private Access lacks the flexibility and scope of more specialized SDN solutions
- Exclusively multitenant architecture offers no “private cloud” option for large enterprises


Zscaler
Security
Deployment
Interoperability
Usability
Web Security
Email Security
Zero Trust
Data Protection

6 Related Research

Advisory Note: Security Organization Governance and the Cloud - 72564
Advisory Note: Cloud Services and Security – 72561
Advisory Note: Firewalls Are Dead - How to Build a Resilient, Defendable Network – 72163
Market Compass: Web Application Firewalls - 70324
Executive View: Akamai Zero Trust Security – 80054
Whitepaper: Addressing Modern Cyber Threats with Cisco Umbrella – 80017
Blog: Palo Alto Networks Continues to Bet on Security-as-a-Service
Executive View: Zscaler Security-as-a-Service Platform – 72505
Executive View: Cisco Zero Trust Security – 80055

Methodology

About KuppingerCole's Market Compass

KuppingerCole Market Compass is a tool which provides an overview of a particular IT market segment and identifies the strengths of products within that market segment. It assists you in identifying the vendors and products/services in that market which you should consider when making product decisions.

While the information provided by this report can help to make decisions it is important to note that it is not sufficient to make choices based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Ease of Delivery
- Interoperability
- Usability

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and

the way the vendor deals with them.

Ease of Delivery is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Rating scale for products

For vendors and product feature areas, we use a separate rating with five different levels. These levels are

- **Strong positive**
  Outstanding support for the subject area, e.g. product functionality, or security etc.)
- **Positive**
  Strong support for a feature area but with some minor gaps or shortcomings. Using Security as an

example, this could indicate some gaps in fine-grained access controls of administrative entitlements.

- **Neutral**
  Acceptable support for feature areas but with several of our requirements for these areas not being met. Using functionality as an example, this could indicate that some of the major feature areas we are looking for aren't met, while others are well served.

- **Weak**
  Below-average capabilities in the area considered.

- **Critical**
  Major weaknesses in various areas.

Content of Figures

Copyright

KuppingerCole supports 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.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

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