Evolution and Convergence of Vendor Product Portfolios Playbook

Evolution and Convergence of Vendor Product Portfolios

The one constant in technology is that change is ever-present. Nowhere is this more evident than in the changes we've seen in technologies just in the last 10 years. Going back 20 years is almost unrecognizable from where we are today.

Even the last couple of years has been a blur. Before the pandemic, digital transformation was just an 'interesting concept.' When the pandemic hit, transformation sped up: spurred on by a need for increased competitiveness and greater business resilience. Workforces went remote or hybrid, an increasing number of applications were migrated to the cloud, and security tools were upended as a result. To make matters worse, in the middle of all this massive global disruption, bad actors saw a window of opportunity and climbed through networks en masse. What they found was a proliferation of standalone security tools and gaps galore.

As a result, today's organizations are re-thinking their security posture. A recent survey found that 75% of organizations are pursuing security vendor consolidation in 2022, up from just 29% in 2020. And 57% of organizations are working with fewer than 10 vendors for their security needs—but they're seeking to downsize to fewer vendors in key areas like secure access service edge (SASE) and extended detection and response (XDR).[1]

> *Security and risk management leaders are increasingly dissatisfied with the operational inefficiencies and the lack of integration of a heterogenous security stack.*

Why? Organizations want to consolidate their security vendors to reduce complexity and improve risk posture (65%), not necessarily to save on budget or to improve procurement (29%). Organizations that have not pursued security vendor consolidation yet indicated that the two primary impediments were time constraints (34%) and having a rigid vendor partnership (34%). 1

As a result, vendors have begun to converge their security portfolios for improved interoperability and manageability, increased productivity, and continuous security. And just in time, too.

This playbook describes some of the history and portfolio consolidation taking place in four key areas: unified threat management (UTM), secure access service edge (SASE), extended detection and response (XDR), and identity and access management (IAM). Plus, we'll delve into how this convergence spells opportunity for you.

Unified Threat Management

Evolution of UTM Via Firewalls, Antivirus, VPNs, IDS/IPS and Web Filtering+

Firewalls: Blocking Unauthorized Users

Antivirus: Blocking malicious viruses

Number of Malware Samples in The AV-Test Database[4,5]

Intrusion Detection/Prevention Systems (IDS/IPS)

VPN: Securely Connecting Remote Users To Company Resources

Web Filtering: Controlling Access To Internet Content

The Rise of Unified Threat Management (UTM)

UTM today: Next-generation firewalls (NGFWs)

Unified Threat Management

Consider these solutions

Check Point

- **Check Point Harmony –** Protect devices and internet connections from the most sophisticated attacks, while ensuring zero-trust access to corporate applications, with the industry's first unified security solution for users, devices, and access.

Progress

- **Progress Flowmon –** Continuously monitor and safeguard network traffic, validate policy enforcement, detect breaches, and support enhanced collaboration between traditionally siloed teams.

SonicWall

- **SonicWall TZ Series Next-Generation Firewall (NGFW) –** Protect small business or branch locations from intrusion, malware, and ransomware with an easy-to-use, integrated security solution specifically for business needs, while delivering enterprise-grade protection—without the cost or complexity.
- **SonicWall NSa Series Next-Generation Firewall (NGFW) –** Enable businesses with 250+ users to work with the confidence of knowing they're protected against day-to-day incursions and advanced threats—like ransomware, attacks against non-standard ports, and breaches in firewalls—all at the speed of business.

Symantec

- **Web Protection Intelligence Service –** Get all the capabilities of WebFilter plus additional intelligence and data feeds, including 10 URL threat risk levels, to fine-tune risk management without over blocking and limit/eliminate access to known high-risk regions with geolocation intelligence.
- **Web Protection Web Filter –** Block web-based attacks as they occur and keep malicious threats out of the network—via a database that contains millions of website ratings, representing billions of web pages, in more than 60 languages, and organized into over 80 categories—with URL filtering, anti-malware technologies and web app control.

Trend Micro

- **Trend Micro Email Security –** Stop phishing, malware, ransomware, fraud, and targeted attacks from infiltrating your enterprise.

WatchGuard

- **WatchGuard Firebox Firewalls –** Put IT security professionals back in charge of networks with a comprehensive network security appliance that includes widely deployable, enterprise-grade security and threat visibility tools suitable for any organization—regardless of budget, size, or complexity.

Unified Threat Management

Evolution of UTM Via Firewalls, Antivirus, VPNs, IDS/IPS and Web Filtering+

ARPANET, the precursor to today's internet, "connected" government, the military, and academia. Hacking—which was not yet a criminal enterprise or nation-state power play—came into play, mostly by early ARPANET "hobbyists."

The Morris Worm, for example, was introduced in 1988 and could "connect to another computer, use vulnerabilities to copy itself, and send itself to a new location."[2] As a result, it used up so many resources that some 6,000 individual computers were infected, causing an estimated $100,000 in damages and exposing the vulnerabilities of networked computers.

Like today's government leaders trying to rein in the power of AI, leaders then expressed real concern about network security, prompting passage of The Computer Fraud and Abuse Act of 1986 and formation of the Computer Emergency Response Team (CERT) to actively spread awareness of security protocols and develop solutions to counter network threats.[2] Going into the 90s, threats continued to evolve and increase as ARPANET evolved from a strictly commercial venture to the publicly available internet.

The result was some of the first mass-produced security appliances and software programs, including:

- **Firewalls** to block unauthorized users
- **Antivirus software** to block malicious viruses
- **Intrusion detection/prevention systems (IDS/IPS)** to detect and prevent malicious traffic
- **A virtual private network (VPN)** to securely connect remote employees and locations to company resources
- **Web filtering** to control access to internet content

As the threat landscape grew, organizations deployed multiple appliances, each with distinct capabilities to defend against those evolving threats. The result was less a blanket-approach to security and more of a patchwork quilt that was growing in cost and complexity. Worse, its ability to effectively contain threats was diminishing as more appliances created more security gaps.

Firewalls: Blocking Unauthorized Users

Antivirus: Blocking malicious viruses

Number of Malware Samples in The AV-Test Database[4,5]

Intrusion Detection/Prevention Systems (IDS/IPS)

VPN: Securely Connecting Remote Users To Company Resources

Web Filtering: Controlling Access To Internet Content

The Rise of Unified Threat Management (UTM)

UTM today: Next-generation firewalls (NGFWs)

Consider these solutions

Unified Threat Management

Evolution of UTM Via Firewalls, Antivirus, VPNs, IDS/IPS and Web Filtering+

Firewalls: Blocking Unauthorized Users

In the simplest terms, firewalls monitor network connections. They were one of the earliest tools to combat malicious activity on the internet and are still a standard network feature.

At its most basic, a firewall either permits or blocks a requested network connection—e.g., an email, website, etc.—based on a set of policies. It also logs information about network traffic, which can help security teams better understand or prevent attacks.

The first "network layer" firewalls were developed in the 1980s. Although fast and transparent, these systems were fairly easy to attack.In the early 1990s, a new generation of "application layer" firewalls emerged: though more cumbersome to set up and operate, they performed a more thorough inspection then their predecessor.

By the early 2000s, most firewalls were hybrids of these two types. But these early firewalls had a huge disadvantage, as one paper pointed out: "Commonly deployed firewalls and routers with access control lists do not provide sufficient protection against increasingly sophisticated cyberattacks."[3]

Antivirus: Blocking malicious viruses

Number of Malware Samples in The AV-Test Database[4,5]

Intrusion Detection/Prevention Systems (IDS/IPS)

VPN: Securely Connecting Remote Users To Company Resources

Web Filtering: Controlling Access To Internet Content

The Rise of Unified Threat Management (UTM)

UTM today: Next-generation firewalls (NGFWs)

Unified Threat Management

Evolution of UTM Via Firewalls, Antivirus, VPNs, IDS/IPS and Web Filtering+

Firewalls: Blocking Unauthorized Users

Antivirus: Blocking malicious viruses

Another network security tool is antivirus software. The first antivirus program, Reaper, was developed in 1971 to combat the non-malicious Creeper virus, which was technically a demonstration of how a self-replicating program could spread to other computers. Upon locating Creeper, Reaper—a self-replicating antivirus—would delete it.

But the real heyday of antivirus software development came in the late 1980s when companies developed programs that would "clean" virus-infected computers. These were the first heuristic tools to find solutions faster than the more traditional self-replicating methods.

Starting in the 1990s, viruses became much more virulent and could infiltrate networks and steal data or disable networks. As a result, there was an explosion of antivirus companies and software, including some that still exist today. These tools used signatures to identify known viruses, a practice that continued for many years. One of the key disadvantages of signature-based virus detection was that there was no way to detect new or novel viruses. It also required significant human intervention.

By 2000, antivirus solutions became open sourced and by 2008, came the first cloud-based antivirus software. Beginning in 2014, solutions were starting to move away from signature-based approaches to detecting and mitigating zero-day attacks using behavioral detection, artificial intelligence, machine learning, and cloud-based file detonation.

As more traditional signature-based antivirus approaches have become ineffective and outdated, signature-less approaches have been increasingly defined as "next-generation" antivirus with traditional antivirus vendors incorporating these "next-gen" offerings into their portfolios.

Today, next-generation antivirus applications use predictive analytics, driven by AI and machine learning, to protect against malware. From this pairing of legacy AV technology with AI/machine learning, a new security category has emerged: endpoint detection and response (EDR). EDR has given rise to extended detection and response (XDR), which shifts the focus from endpoints to the whole network. XDR provides a holistic view of threats across the entire technology landscape for improved protection, detection, and response.

Number of Malware Samples in The AV-Test Database[4,5]

Intrusion Detection/Prevention Systems (IDS/IPS)

VPN: Securely Connecting Remote Users To Company Resources

Web Filtering: Controlling Access To Internet Content

The Rise of Unified Threat Management (UTM)

UTM today: Next-generation firewalls (NGFWs)

Consider these solutions

Unified Threat Management

Evolution of UTM Via Firewalls, Antivirus, VPNs, IDS/IPS and Web Filtering+

Firewalls: Blocking Unauthorized Users

Antivirus: Blocking malicious viruses

Number of Malware Samples in The AV-Test Database[4,5]

Year	Number of Malware Samples*
1994	28,613
1998	98,428
2005	333,425
2008	15,691,697
2013	120,310,364
2019	647,920, 244
2023	1,104,487,973

* All numbers represented are cumulative. 2023 numbers were pulled on Dec. 8, 2023 and may be subject to change.

Intrusion Detection/Prevention Systems (IDS/IPS)

VPN: Securely Connecting Remote Users To Company Resources

Web Filtering: Controlling Access To Internet Content

The Rise of Unified Threat Management (UTM)

UTM today: Next-generation firewalls (NGFWs)

Consider these solutions

Unified Threat Management

Intrusion Detection/Prevention Systems (IDS/IPS)

A 1986 academic paper launched the Intrusion Detection Expert System (IDES) model, the first real-time IDS system. IDES was "initially a rule-based expert system trained to detect known malicious activity."6 It later took a two-pronged approach, dubbed next-generation IDES (NIDES), which leveraged the rule-based expert system and added statistical anomaly detection, signatures, and user and host profiles to detect malicious network behaviors.[6]

This model posited that, by analyzing usage statistics, a bad actor's behavior can be distinguished from that of a legitimate user. It then creates a user's behavioral pattern based on the files, applications, and devices they access and adds rules based on known violations. IDES could then detect malicious behaviors, such as HTTP or FTP protocol misuse or denial of service (DoS) attacks. This paper—as well as others published in the early 1970s by the U.S. Air Force—were largely responsible for what ultimately became the early IDS systems of the 1980s and 1990s.

IDS uses a "mechanism capable of identifying or detecting the presence of intrusive activities. In a broader concept, this encompasses all the processes used in the discovery of unauthorized uses of network devices or computers. This is done through software designed specifically to detect unusual or abnormal activities."[3]

Network-based IDS identifies possible network intrusions by examining packets across the network. Its primary goal is to use pre-defined signatures to determine if those packets contain dangerous payloads and to check for malicious behavior patterns.[3]

On the other hand, host-based IDS resides on email, file, and database servers and examines changes made to a particular host. Its key goal is to inspect "the host computer system's configuration files, detecting unauthorized changes to key files and settings that indicate changes or policy violations."[3]

While IDS can effectively detect known threats, it's unable to detect new attacks. This required vendors to constantly provide updated signatures about new attacks—which would require an automated process that was non-disruptive to IDS operations—but which often failed due to the time lag between a new attack and getting updated information out about those attacks.

There was also the problem of false positives, which required human intervention and a tedious manual process to ferret out "real" threats. These issues required a new, more proactive approach.

IDS eventually evolved into IPS in the early 2000s. Where IDS automates intrusion detection, IPS prevents attacks. In addition to proactive protection, IPS offers a shorter time to remediation and reduced staffing time which drives increased return on investment.[3]

Like IDS, IPS provides either host-based or network-based intrusion prevention. Host-based IPS is installed on a host to monitor and deter malicious activity, while network-based IPS is an appliance that sits behind the perimeter firewall, working to detect and prevent harmful inbound TCP/IP activity.[3] As time went by, network security required additional capabilities to fend off new and evolving threats, notably VPNs and web filtering.

Consider these solutions

Unified Threat Management

Evolution of UTM Via Firewalls, Antivirus, VPNs, IDS/IPS and Web Filtering+

Firewalls: Blocking Unauthorized Users

Antivirus: Blocking malicious viruses

Number of Malware Samples in The AV-Test Database[4,5]

Intrusion Detection/Prevention Systems (IDS/IPS)

VPN: Securely Connecting Remote Users To Company Resources

Where antivirus and other software can effectively protect end-users, what they really need is a more secure network connection.

In the early 1990s, organizations realized the potential of the internet to connect their distributed locations. They also realized that the public internet could not secure their data or protect it from unauthorized access or interception. The answer? Create a secure, encrypted tunnel between two points on the internet, so that data could be securely and privately transmitted.

Virtual private networks (VPNs) were first developed by Microsoft in 1996 to create this more secure and private internet connection. A private "internet within the internet," remote workers, branch locations, and field personnel could access company files via a VPN while still safeguarding their data. While this protocol was vulnerable to certain types of attacks, it laid the groundwork for future VPN protocols and helped to popularize the concept of secure, private connections over the internet.

VPN technologies have continued to evolve, with new protocols and encryption methods to address ever-changing internet security threats. In the late 1990s, the Internet Protocol Security (IPsec) suite provided a more robust and flexible framework for creating secure VPN connections, making way for greater customization and improved security.[7]

The OpenVPN protocol developed in 2001 was another major milestone. This highly secure, open-source alternative to proprietary VPN protocols quickly gained popularity due to its strong encryption, high performance, and ability to bypass firewalls and network restrictions. OpenVPN remains one of the most widely used VPN protocols today, with many vendors offering it as a standard option for their customers.[7]

One key challenge with VPNs is that they expose entire networks to the threat. In other words, once a bad actor has breached the network through a compromised device, the entire network can be brought down.

As new threats emerge, VPNs will likely be shaped by new security developments—for example, integrating VPNs with other security tools and services, such as antivirus software and intrusion detection systems. And, as more devices and appliances are connected to the internet, the demand for VPNs that can protect a wide range of devices and platforms is likely to increase.[7]

In conclusion, VPNs have grown into a critical tool for millions of internet users worldwide and they will continue to evolve and adapt in response to changing internet security and privacy.[7]

Web Filtering: Controlling Access To Internet Content

The Rise of Unified Threat Management (UTM)

UTM today: Next-generation firewalls (NGFWs)

Unified Threat Management

Evolution of UTM Via Firewalls, Antivirus, VPNs, IDS/IPS and Web Filtering+

Firewalls: Blocking Unauthorized Users

Antivirus: Blocking malicious viruses

Number of Malware Samples in The AV-Test Database[4,5]

Intrusion Detection/Prevention Systems (IDS/IPS)

VPN: Securely Connecting Remote Users To Company Resources

Web Filtering: Controlling Access To Internet Content

Web filtering, or the ability to filter web content to specific users, largely came about in the educational setting where children were being exposed to the internet. Advocates of web filtering were especially concerned about public libraries, where—once upon a time—school-aged children could access the internet. It also raised constitutional issues about free speech.

Ultimately, the Children's Internet Protection Act (CIPA) was passed in 2000 to address these issues. The legislation required schools and libraries to certify that they have an Internet safety policy in place with technology protection measures that could block content that was obscene and harmful to children. They also had to monitor the online activities of minors and educate them about social networks and cyberbullying. Schools and libraries that did not attest to these requirements were unable to receive valuable E-Rate discounts to build and expand their school networks.

Around this time, web filtering software became available for use by both parents and organizations to track what their kids and employees were doing on the internet. These tools often came bundled with firewalls and, as they evolved, functionality such as categorization, reputation, dynamic DNS searching, geo-location, and other features were added to keep up.

The Rise of Unified Threat Management (UTM)

UTM today: Next-generation firewalls (NGFWs)

Unified Threat Management

Evolution of UTM Via Firewalls, Antivirus, VPNs, IDS/IPS and Web Filtering+

Firewalls: Blocking Unauthorized Users

Antivirus: Blocking malicious viruses

Number of Malware Samples in The AV-Test Database[4,5]

Intrusion Detection/Prevention Systems (IDS/IPS)

VPN: Securely Connecting Remote Users To Company Resources

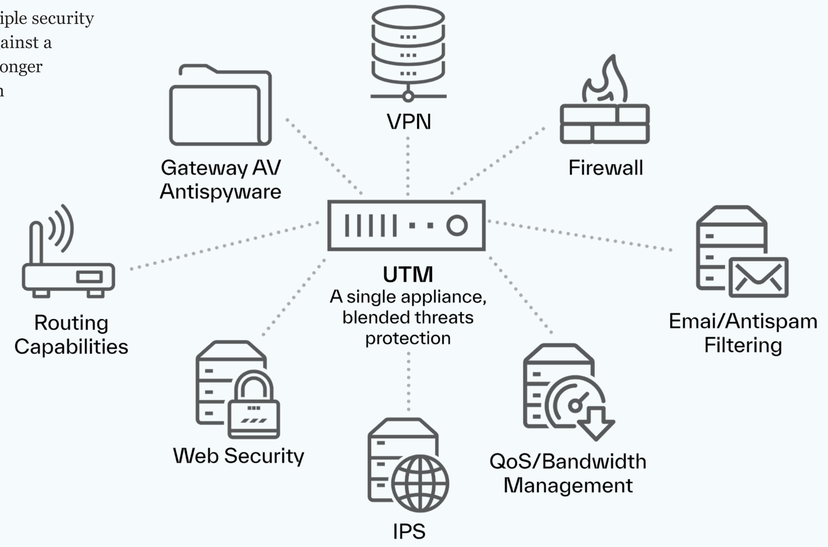
Web Filtering: Controlling Access To Internet Content

The Rise of Unified Threat Management (UTM)

These one-off solutions led to increased network complexity and security gaps. To resolve this issue, several vendors launched "all-in-one" security products. IDC first identified the concept of unified threat management (UTM) in 2004, calling it "a new category of security appliances and that it was necessary to have at least the functionality of a firewall, a network intrusion prevention system, and a gateway Antivirus to be part of this security appliance category."[8] Though UTM functionality has evolved over the years, the name continues to be used today.

With UTM, firewalls could consolidate multiple security services into a single appliance to protect against a range of blended attacks. Organizations no longer needed to deploy multiple devices, each with its own management dashboard and login credentials. To simplify management and reporting, vendors offered all-in-one management interfaces to centrally manage multiple services, features, policies, and rules.

Even though a UTM system offers consolidated management, it's antithetical to one of the basic tenets of the defense-in-depth approach: a single device introduces a single point of failure. Compromise at the UTM layer would break the entire defense-in-depth approach.



UTM today: Next-generation firewalls (NGFWs)

Consider these solutions

Unified Threat Management

Evolution of UTM Via Firewalls, Antivirus, VPNs, IDS/IPS and Web Filtering+

Firewalls: Blocking Unauthorized Users

Antivirus: Blocking malicious viruses

Number of Malware Samples in The AV-Test Database[4,5]

Intrusion Detection/Prevention Systems (IDS/IPS)

VPN: Securely Connecting Remote Users To Company Resources

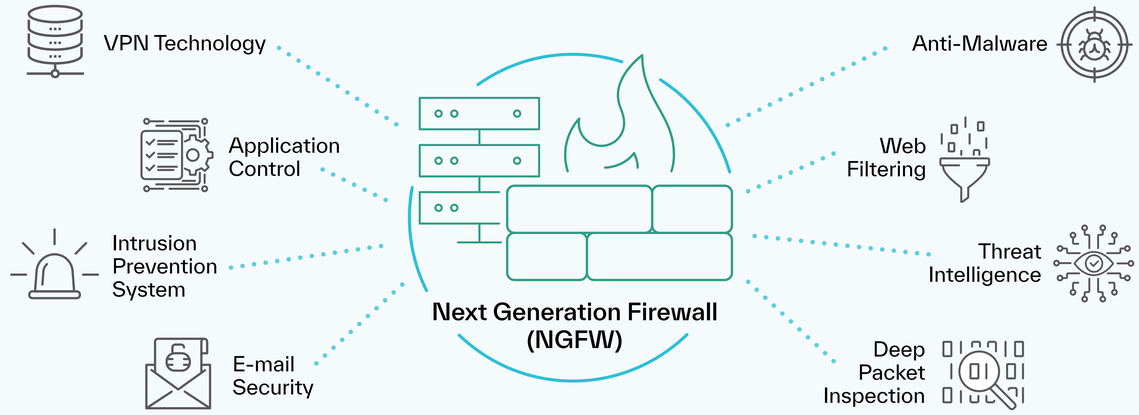
Web Filtering: Controlling Access To Internet Content

The Rise of Unified Threat Management (UTM)

UTM today: Next-generation firewalls (NGFWs)

Today, UTMs are now typically called next-generation firewalls (NGFWs). Both consolidate multiple security functions into a single solution. Beyond that, the differences are less clear. What is clear is that NGFWs solve performance deficiencies found in many UTMs, delivering application control features and deep packet inspection in a highly performing and cohesive architecture.

What is a Next Generation Firewall (NGFW)?



NGFWs have also improved the coordination and communication between multiple services that UTM firewalls consolidated. AI, machine learning, and automation have also begun to feature prominently, enabling improved threat intelligence and response times.

To effectively manage these more advanced systems, vendors have begun to offer single pane-of-glass management, eliminating the need to navigate between multiple tabs while managing a network.

NGFWs block more attacks than ever, while providing ample scalability and reliable performance. Where typical UTM systems may get overwhelmed by a large number of demands, NGFWs can handle those demands, making them an effective security solution for large enterprises.

Consider these solutions

Secure Access Service Edge

Evolution of SASE via SWG, CASB, ZTNA, FWaaS Convergence

CASB: Protecting Against Cloud-Based Threats

FwaaS: Leveraging a Cloud-Based Firewall

How You Can Help Your Customer Choose

SWG: Reducing Internet Risk Through Controlled Access

Secure Access Service Edge

Consider these solutions

Aruba (HPE Aruba Networking)

- **HPE Aruba Networking SSE + Axis Security Platform –** Connect users and servers to the business resources needed for work via one, cloud-delivered platform that integrates ZTNA, SWG, CASB and DEM and uses 500+ edge locations—it's simple, secure, and controlled by a single pane of glass.
- **HPE Aruba Networking Unified SASE Platform –** Enable hybrid working, tackle the networking and security challenges of cloud computing, and simplify SASE deployment with a unified SD-WAN + SSE secure access strategy.

Check Point

- **Check Point Quantum Network Security –** Get ultra-scalable protection against Gen V cyberattacks on your network, cloud, data center, IoT, and remote users.

Progress

- **Progress Flowmon –** Continuously monitor and safeguard network traffic, validate policy enforcement, detect breaches, and support enhanced collaboration between traditionally siloed teams.

Symantec

- **Cloud SWG –** Enforce consistent web security and compliance policies for all users, regardless of location or device, with a cloud-delivered network security service.
- **Secure Access Cloud –** Allow only authorized users to connect to specific applications, while making applications invisible to attackers, with a SaaS solution that provides zero-trust access to any corporate resource hosted in cloud environments or on-premises data centers—eliminating the inbound connections to customer networks and creating a software-defined perimeter (SDP) between users and corporate applications.
- **CloudSOC CASB –** Simplify and enhance the security infrastructure and provide unequaled cloud app security with the deepest visibility, tightest data security, and strongest threat protection—includes built-in integrations with Symantec's industry-leading solutions, such as DLP, Secure Web Gateway, and Endpoint Security.

Trend Micro

- **Trend Micro Network Security –** Expand the power of XDR with network detection and response.

Secure Access Service Edge

Evolution of SASE via SWG, CASB, ZTNA, FWaaS Convergence

Web filtering, or the ability to filter web content to specific users, largely came about in the educational setting where children were being exposed to the internet. Advocates of web filtering were especially concerned about public libraries, where—once upon a time—school-aged children could access the internet. It also raised constitutional issues about free speech.

Ultimately, the Children's Internet Protection Act (CIPA) was passed in 2000 to address these issues. The legislation required schools and libraries to certify that they have an Internet safety policy in place with technology protection measures that could block content that was obscene and harmful to children. They also had to monitor the online activities of minors and educate them about social networks and cyberbullying. Schools and libraries that did not attest to these requirements were unable to receive valuable E-Rate discounts to build and expand their school networks.

Around this time, web filtering software became available for use by both parents and organizations to track what their kids and employees were doing on the internet. These tools often came bundled with firewalls and, as they evolved, functionality such as categorization, reputation, dynamic DNS searching, geo-location, and other features were added to keep up.

CASB: Protecting Against Cloud-Based Threats

FwaaS: Leveraging a Cloud-Based Firewall

How You Can Help Your Customer Choose

SWG: Reducing Internet Risk Through Controlled Access

Consider these solutions

Secure Access Service Edge

Evolution of SASE via SWG, CASB, ZTNA, FWaaS Convergence

CASB: Protecting Against Cloud-Based Threats

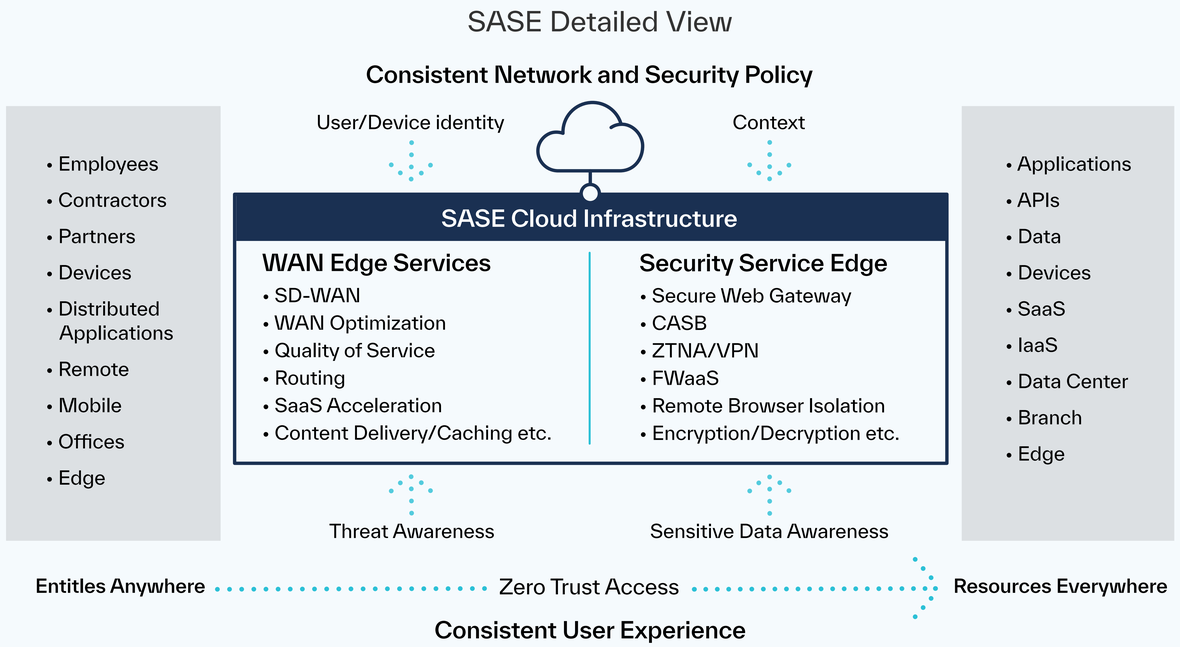
FwaaS: Leveraging a Cloud-Based Firewall

How You Can Help Your Customer Choose

While SASE offers clear benefits, it really depends on your customer's environment and where they're at in their security journey. If they don't already have an SD-WAN, start with SSE or SASE "light"—a standalone framework that easily integrates CASB, SWG, and ZTNA into an existing security architecture and puts your customer on the path to a full-stack SASE architecture.

On the other hand, SASE represents more of a strategic approach that enables enterprises to benefit from a fully integrated security stack. Or optimize your customer's SD-WAN with a highly secure FWaaS and add on CASB, SWG, and ZTNA capabilities, while simplifying security and maximizing the efficiency of your customer's IT and security architecture in a phased way.

Helping your customer choose the right CASB strategy and solution will save them time, effort, and money, in addition to protecting them against potential dangers.



SWG: Reducing Internet Risk Through Controlled Access

Consider these solutions

Secure Access Service Edge

Evolution of SASE via SWG, CASB, ZTNA, FWaaS Convergence

CASB: Protecting Against Cloud-Based Threats

Cloud-based infrastructures require a comprehensive cloud access security broker (CASB) to guarantee the security and integrity of your customers' data and applications. As edge and cloud security become the next pain point, CASBs are becoming an increasingly vital component of the secure access service edge (SASE).

CASBs sit between users and cloud services to enforce security policies and prevent internal and external threats, such as malware and phishing. They enable organizations to mitigate threats by restricting access to critical data, monitoring users' online activity in real time, managing privileged accounts, and controlling cloud-based file sharing. This helps enterprises prevent data leakage by enforcing rules around user activity, such as access, devices, location, and time restrictions.

CASBs also increase visibility into network activity to prevent shadow IT by limiting or removing unmanaged cloud applications and identifying risky cloud applications.

CASB is best at protecting enterprise cloud applications. It helps your customers to apply the same protections of traditional perimeter-focused security models to their cloud-based deployments. It can easily be deployed as a standalone framework that easily integrates into an existing security architecture—or with a SWG and ZTNA for SSE or SASE "light" that puts your customer on the path to a full-stack SASE architecture.

The CASB market is expected to reach

$25.6 billion

by 2030, for a CAGR of

17.6% from 2022 to 2030.[11]

> *"The CASB market is primarily driven by…growing demand for visibility into shadow IT operations, rising need for securing and compliant cloud use, and increasing use of cloud-based applications among small and medium-sized businesses. Moreover, cloud protection services are challenging to manage for enterprises. Thus, the need for security solutions to be outsourced has pushed the cloud access security broker market even further forward."*[11]

FwaaS: Leveraging a Cloud-Based Firewall

How You Can Help Your Customer Choose

SWG: Reducing Internet Risk Through Controlled Access

Consider these solutions

Secure Access Service Edge

Evolution of SASE via SWG, CASB, ZTNA, FWaaS Convergence

CASB: Protecting Against Cloud-Based Threats

FwaaS: Leveraging a Cloud-Based Firewall

How You Can Help Your Customer Choose

SWG: Reducing Internet Risk Through Controlled Access

Today's hybrid workforce combined with an onslaught of online threats have made it difficult for organizations to protect against threats as employees access the internet and an increasing number of cloud-based apps. To solve those challenges, organizations have traditionally used an array of point products—which then created new security gaps and led to increased operational complexity.

The earliest web gateways were built for on-premises use and looked at all egress traffic. As such, they required rigorous control. But these and other more traditional security methods are no longer the most reliable methods for detecting and responding to today's threats.

A more modern SWG helps organizations keep pace with evolving business demands and increasingly complex security environments.

A key component of a SASE architecture, an SWG "filters unwanted software/malware from user-initiated Web/Internet traffic and enforces corporate and regulatory policy compliance." Unlike web proxies, they typically include URL filtering, malicious-code detection and filtering, and application controls at a minimum, as well as data loss prevention for managed and unmanaged devices.[12] In other words, SWG reduces internet risks through authenticated and controlled access for all users and devices and can be delivered on-premises or in the cloud.

Finally, the power of SWGs comes from the quality of threat intelligence that's feeding it. Consider a vendor with a strong record of global threat intelligence and an established, automated process to curate and update a threat feed data for SWGs.

ZTNA: Modernizing the traditional VPN

As workers decamped to the safety of their homes—and beyond corporate firewalls—seemingly overnight, cybersecurity teams raced to deploy virtual private networks (VPNs).

But routing traffic through narrow, dedicated, point-to-point tunnels via indirect security gateways negatively impacts the user experience. Taking outbound traffic to an on-premises security stack for inspection first only exacerbates the problem. Plus, VPNs don't protect against threats carried in through a home network. This calls for a new approach to security: zero trust network access (ZTNA).

Today's modern organization must make their digital assets available to a distributed workforce and third-party cohorts—anywhere, anytime, and from any device. ZTNA applies zero-trust principles to application access, where users and devices are authenticated and monitored every time they seek access to an application.

ZTNA "includes verification of user and device identity and checks for other factors such as time-of-day, location, and the state of the device prior to granting access. ZTNA also continues monitoring those factors and identities."[13] Benefits of ZTNA include:

- Reduced attack surface via network micro-segmentation
- Limited damage due to insider threats using least privilege
- Reduced threat to internet-based threats by keeping applications from being exposed to the internet
- Minimal risk and spread due to compromised user accounts
- Restricted access to cloud environments and applications
- Improved compliance with greater control over application and data access

Consider these solutions

Secure Access Service Edge

FwaaS: Leveraging a Cloud-Based Firewall

Cloud, distributed environments, remote and hybrid workforces, and IoT have largely rendered network perimeters extinct, reducing the effectiveness of traditional perimeter security.

Unlike traditional firewalls, which rely on physical or virtual devices located at the network perimeter, NGFWs typically add advanced features—such as application awareness, intrusion prevention, deep packet inspection, user and identity awareness, and SSL/TLS decryption—to provide packet filtering and stateful inspection.

FWaaS, on the other hand, offers the same protection as traditional on-premises firewalls delivered as a cloud-based service, enabling your customer to efficiently protect digital assets outside the network perimeter, consistently enforce security policies, and better respond to new threats.

FWaaS can also leverage NGFW capabilities—including some advanced functionality—as well as real-time data analysis and machine learning to combat constantly evolving threats and an expanding attack surface. It also makes it easier to scale security and keep up with firewall advancements, updates and maintenance.

To be sure, it's a small step up from traditional security models—but one that provides a giant leap in protection.

By 2025.....

One-third of new SASE deployments will be based on a single-vendor SASE offering, **up from 10%** in 2022.[11]

80% of enterprises will have adopted a strategy to unify web, cloud services and private application access using a SASE/SSE architecture, **up from 20%** in 2021.[11]

65% of enterprises will have will have consolidated individual SASE components into one or two explicitly partnered SASE vendors, **up from 15%** in 2021.[11]

50% of new SD-WAN purchases will be part of a single-vendor SASE offering, **up from 10%** in 2022.[11]

Consider these solutions

Extended Detection and Response

Evolution of XDR via Endpoint Security, Cloud App Security, and Identity Convergence

Endpoint Security: Providing Endpoint Visibility And Control

Cloud Security: Joining With XDR for Rapid Response

Identity: Stopping Identity-Based Attacks in Their Tracks

Extended Detection and Response

Evolution of XDR via Endpoint Security, Cloud App Security, and Identity Convergence

Endpoint Security: Providing Endpoint Visibility And Control

Cloud Security: Joining With XDR for Rapid Response

Identity: Stopping Identity-Based Attacks in Their Tracks

Consider these solutions

Check Point

- **Check Point Horizon –** Provide complete coverage of networks, endpoints, cloud, email, and IoT—all from one pane of glass—with XDR, MDR and events management solutions.

Symantec

- **Symantec Endpoint Security Complete –** Automate protection configuration to deliver custom protection specifically to your organization, while saving time, money, and effort.
- **VIP Authentication Service –** Protect mobile and web applications for employees, customers, and partners with a cloud-based authentication solution that silently and transparently collects data and assesses risk—based on device identification, geolocation, and user behavior, among other factors—in a secure and user-friendly way.
- **CloudSOC CASB –** Simplify and enhance the security infrastructure and provide unequaled cloud app security with the deepest visibility, tightest data security, and strongest threat protection—includes built-in integrations with Symantec's industry-leading solutions, such as DLP, Secure Web Gateway, and Endpoint Security.

Trend Micro

- **Trend Vision One™ Endpoint Security –** Defend the endpoint through every stage of an attack.
- **Trend Micro Email Security –** Stop phishing, malware, ransomware, fraud, and targeted attacks from infiltrating your enterprise.
- **Trend Micro Network Security –** Expand the power of XDR with network detection and response.

WatchGuard

- **WatchGuard ThreatSync –** Automatically neutralize cyberattacks before it is too late with the advanced XDR capabilities needed to correlate threat intelligence across environments, users, and devices.

Extended Detection and Response

Evolution of XDR via Endpoint Security, Cloud App Security, and Identity Convergence

Today's IT teams face challenges navigating a complex threat detection and response landscape. Acronyms meant to simplify understanding—such as EDR, XDR, and MDR—just make it more confusing. Add an increasing number of vendors—and solutions with varying degrees of capabilities—and you can see why it's tempting to put off threat detection and response decisions.

In truth, most IT teams want greater visibility across all across all corporate endpoints, no matter what those endpoints are or where they're located. And they want to remediate any issues remotely—before they wreak havoc on their infrastructure.

Extended detection and response (XDR) takes an enterprise-level approach, giving security teams a holistic view of their organization's security posture and enabling them to make fast, informed detection and response decisions. XDR natively integrates data from multiple security products—including endpoint detection and response (EDR), network security, cloud security, and email security—to provide a unified view of security threats across the organization.

XDR solutions use advanced analytics and machine learning algorithms to identify and prioritize threats, automate incident response workflows, and provide actionable insights to improve security operations. XDR also applies continuously updated threat intelligence to add context and drive better detections.

MSPs and MSSPs should familiarize themselves with XDR so that they understand—and can speak knowledgeably about—XDR solutions and how they might add value to both their and their customers' businesses.

Up to 40%

of end-user organizations

will use an extended detection and response (XDR)

solution by 2027,

primarily to consolidate the number of security vendors they work with.[15]

Endpoint Security: Providing Endpoint Visibility And Control

Cloud Security: Joining With XDR for Rapid Response

Identity: Stopping Identity-Based Attacks in Their Tracks

Consider these solutions

Extended Detection and Response

Evolution of XDR via Endpoint Security, Cloud App Security, and Identity Convergence

Endpoint Security: Providing Endpoint Visibility And Control

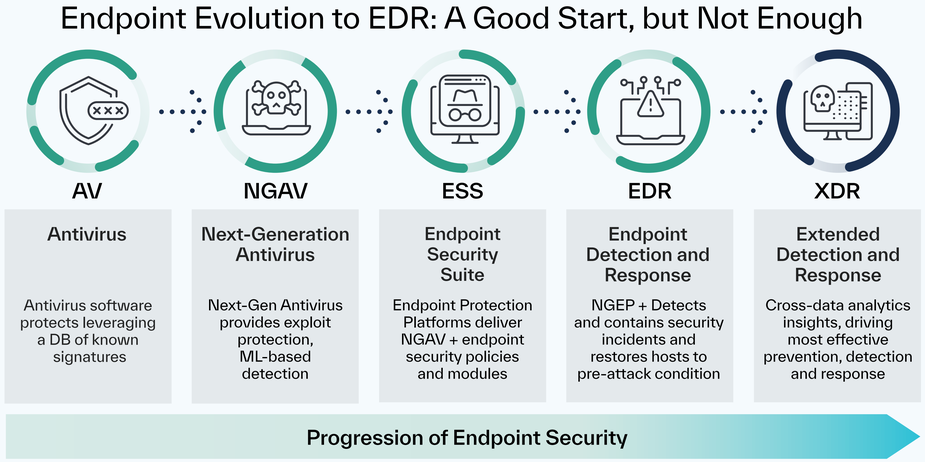
The number of endpoints in organizations continues to increase. They're no longer limited to traditional end-user devices, such as laptops, desktops, and printers, etc. Instead, the increased number of traveling or remote employees means that endpoints are now located outside the network (e.g., end-users' laptops and mobile devices) or as endpoint-to-endpoint connections across the entire environment. That makes monitoring and securing endpoints a challenge.

EDR—and, ultimately, XDR—began in the 1980s as what we know today as basic antivirus software. While these simple tools effectively leveraged known signatures to detect threats, there was little to no protection against novel threats.

As the threat landscape evolved, antivirus products evolved as well, adding features like host firewall, device control, and web traffic filtering. These "next-generation" antivirus solutions became known collectively as an endpoint protection platform (EPP), a solution that is "…deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts." These solutions are typically cloud-managed, enabling endpoints—whether on the corporate network or outside the office—to be continuously monitored and remotely remediated. Advanced EPP solutions often use multiple detection methods, from static IOCs to behavioral analysis.[16]

EDR solutions help organizations detect, investigate, and respond to security incidents by monitoring endpoint activities and behaviors and providing visibility and control. They provide detailed information—for example, process activity, file changes, network connections, and system events—that help security teams to quickly identify and respond to threats.

Today, cloud-based, vendor-agnostic XDR has consolidated tools and data for extended visibility, analysis and response across all endpoints, workloads, users, and networks. Like SIEM, it takes in data from everywhere and generates security alerts. But its roots in EPP and EDR enable robust endpoint protection with superior detection and prevention.



Cloud Security: Joining With XDR for Rapid Response

Identity: Stopping Identity-Based Attacks in Their Tracks

Consider these solutions

Extended Detection and Response

Evolution of XDR via Endpoint Security, Cloud App Security, and Identity Convergence

Endpoint Security: Providing Endpoint Visibility And Control

Cloud Security: Joining With XDR for Rapid Response

As good as EDR solutions are, they're limited to securing just endpoints. They're no match for protecting IoT devices, applications, user identities, applications, or cloud environments. Thus, as organizations increasingly adopt cloud-based applications and infrastructure, they'll have to integrate EDR and XDR with cloud security tools—such as CASBs, cloud security posture management (CSPM), and cloud workload protection platforms (CWPPs)—for a more holistic view of their security posture.[17]

To fully integrate security across on-premises and cloud-based assets, organizations will need XDR to automatically correlate and aggregate security and event data across the security stack, empowering security and IT teams to quickly detect and respond to a wider range of threats. Machine learning, automation and threat intelligence provide in-depth insights and context into security incidents, eliminating false positives and providing high-fidelity detections across the entire network infrastructure from a single console.[17]

Identity: Stopping Identity-Based Attacks in Their Tracks

Extended Detection and Response

Evolution of XDR via Endpoint Security, Cloud App Security, and Identity Convergence

Endpoint Security: Providing Endpoint Visibility And Control

Cloud Security: Joining With XDR for Rapid Response

Identity: Stopping Identity-Based Attacks in Their Tracks

As organizations work to strengthen network and endpoint protection, stealing and compromising credentials has become a new weapon to infiltrate organizations. Unfortunately, identity and access management (IAM) solutions typically lack the telemetry needed to identify modern identity-based attacks in real-time—across hybrid environments, remote workers, and multiple identity stores—without disrupting users.

That's why marrying IAM with an XDR tool that includes endpoint, data lake, orchestration, source of identity data for correlation, and threat intelligence—at a minimum—should be a top priority. A holistic XDR solution that connects endpoint, identity, and threat intelligence together ensures coverage everywhere—cloud, on-prem, mobile, unmanaged devices, etc.[v]

This holistic XDR solution should have "unified cross-domain detections and investigations to effectively connect the dots, understand the context, and automate the risk response to stop or contain adversary attacks. XDR with identity protection stops threats, and also improves the bottom line."[18]

Nearly 80% of attacks leverage identities identities to compromise legitimate credentials and use techniques like lateral movement to **quickly evade detection.**[19]

There was a **112% jump** in access broker activity from 2021.[19]

Consider these solutions

Identity and Access Management

Evolution of IAM via New Access Management, Governance, Admin Access, Privileged Access

New Access Management: Making Identity the New Security Perimeter

Privileged Access Management: Validating Access to Resources

Identity and Access Management

Evolution of IAM via New Access Management, Governance, Admin Access, Privileged Access

New Access Management: Making Identity the New Security Perimeter

Privileged Access Management: Validating Access to Resources

Consider these solutions

Check Point

- **Check Point Harmony –** Protect devices and internet connections from the most sophisticated attacks, while ensuring zero-trust access to corporate applications, with the industry's first unified security solution for users, devices, and access.

Progress

- **Progress Flowmon–** Continuously monitor and safeguard network traffic, validate policy enforcement, detect breaches, and support enhanced collaboration between traditionally siloed teams.

Symantec

- **Symantec Privileged Access Management (PAM) –** Minimize the risk of data breaches by continually protecting sensitive administrative credentials, controlling privileged user access, and monitoring and recording privileged user activity across virtual, cloud, and physical environments.
- **VIP Authentication Service –** Protect mobile and web applications for employees, customers, and partners with a cloud-based authentication solution that silently and transparently collects data and assesses risk—based on device identification, geolocation, and user behavior, among other factors — in a secure and user-friendly way.
- **Symantec Management Center –** SimpliEnsure the consistent application of web security and governance by scaling deployments and applying powerful proxy policies that address specific needs throughout the environment with a unified management platform—which features centralized visibility and control of ProxySG, Advanced Secure Gateway (ASG), Web Application Firewall (WAF), Web Security Service (WSS), SSL Visibility Appliance (SSLV), Security Analytics (SA), Content Analysis (CAS), and Reporter deployments.

WatchGuard

- **AuthPoint Total Identity Security –** Have everything needed for a full MFA solution, including SSO and risk-based authentication, corporate password management, plus the ability to activate monitoring for domain(s) in case a new database with credentials is found on the dark web.

Identity and Access Management

Evolution of IAM via New Access Management, Governance, Admin Access, Privileged Access

Today's organizations require robust IAM solutions to protect and ensure secure access to critical resources. Before it was IAM, it was authentication and it only required usernames and passwords. But the rise of interconnected systems and the internet called for a more comprehensive and centralized solution, leading to the development of directory services such as lightweight directory access protocol (LDAP) and IAM. Today's IAM has become integral to managing user identities, controlling access privileges, and enforcing security policies across multiple systems and applications. It offers enhanced security, ample scalability and flexibility, better compliance and auditing, and a more streamlined user experience. Even better, the future of IAM full of promise. Here are some potential advancements that may be ahead:[20]

- **Context-aware authentication –** Analyze user behavior, location, and device information using AI and machine learning for more context-aware authentication, enabling real-time risk assessments and dynamic access controls.
- **Biometric authentication –** Increasingly integrate biometric authentication methods—such as fingerprints, facial recognition and voice patterns—to reduce reliance on traditional passwords and improve the user experience.
- **Zero-trust security model –** Continuously verify and authenticate users, regardless of their location or network, using IAM as part of the zero-trust security model.
- **Blockchain-based identity management –** Give users complete control over their identities and enhance data privacy with secure and tamper-proof blockchain-based IAM.

IAM has evolved into a fundamental element of modern technology frameworks and its ability to enhance security, streamline user experiences, and ensure compliance makes it indispensable for your customers. Going forward, IAM is poised to leverage emerging technologies—such as AI, biometrics and blockchain—to address future challenges, adapt to new threats, and drive even greater security and convenience.

New Access Management: Making Identity the New Security Perimeter

Privileged Access Management: Validating Access to Resources

Consider these solutions

Identity and Access Management

Evolution of IAM via New Access Management, Governance, Admin Access, Privileged Access

New Access Management: Making Identity the New Security Perimeter

Today, cloud-first, access-data-from-anywhere network models challenge how your customer securely accesses corporate data and applications. SaaS, IaaS, and PaaS technologies typically exist in a hybrid or multi-cloud environment where requests for access can originate from anywhere in the world. In this context, "identity is the new perimeter." This means that your customer's cloud security strategy must govern digital identities and access.

Where access management refers to all the tools, policies, and procedures used to control and manage user access within an enterprise IT ecosystem, modern access management solutions let you "assess identities every time a user tries to access a resource. This allows for adaptive authentication, a dynamic way of assessing identities and managing risk in real time, making each access request unique."[21] Modern access management enables:[21]

- **Adaptive authentication –** Assess identities and manage risk in real time, making each access request unique.
- **Flexibility –** With identity as the new perimeter, there's no need to re-define security models each time a resource is moved (e.g., migrating on-prem applications to the cloud or dismantling on-prem applications and adopting cloud applications).

Creating a modern access management solution for your customer starts with embracing smart, cloud-based single sign-on (SSO) to manage how users interact with cloud services as well as on-premises applications. Modern SSO centralizes access across a large number of users and services, enabling your customer to track the entire user journey, assess requests in real-time, and make decisions based on updated information. Finally, consider implementing policy-based access restrictions along with modern SSO. Policy-based access restrictions consider what users can access (entitlement) and when users are allowed to access applications (real-time access control), giving your customer control over the applications their employees can use.

Governance: Defining and enforcing policies

What's the difference between identity management and identity governance? According to the Identity Management Institute, identity governance refers to "a set of policies, systems, and processes that organizations employ to manage and control user access to critical systems and data within their infrastructure. It involves defining and enforcing policies related to user identities, roles, and privileges to ensure that only authorized subjects have appropriate access to objects."[22] The primary objective of identity governance is to establish a framework for managing an organization's user identities, entitlements, and access rights. Components include:[22]

- **Identity lifecycle management –** Manage the entire lifecycle—creating, modifying, and deleting user identities—including provisioning, deprovisioning, and access request management.
- **Role-based access control (RBAC) –** Define and enforce roles and grant users appropriate access based on their job responsibilities.
- **Access certification and recertification –** Provide mechanisms for managers and data owners to periodically review and approve user entitlements to validate that user access rights are still necessary and appropriate.
- **Segregation of duties (SoD) –** Identify and manage conflicting access rights to by enforcing separation between incompatible duties to ensure that users do not have privileges that could lead to abuse or unauthorized actions.
- **Audit and compliance –** Provide mechanisms to track and record user access activities to detect any unauthorized access or policy violations, ensuring that organizations demonstrate compliance with regulatory requirements.

Though identity management and governance seem to overlap at times, they do have distinct differences. Governance essentially sets identity management strategy through policies, processes, and technologies and identity management carries out that strategy by executing on those policies, processes, and technologies. At the end of the day, instilling governance serves to streamline user access management processes, improve operational efficiency, and centralize visibility into user access across the organization.

Privileged Access Management: Validating Access to Resources

Consider these solutions

Identity and Access Management

Evolution of IAM via New Access Management, Governance, Admin Access, Privileged Access

New Access Management: Making Identity the New Security Perimeter

Privileged Access Management: Validating Access to Resources

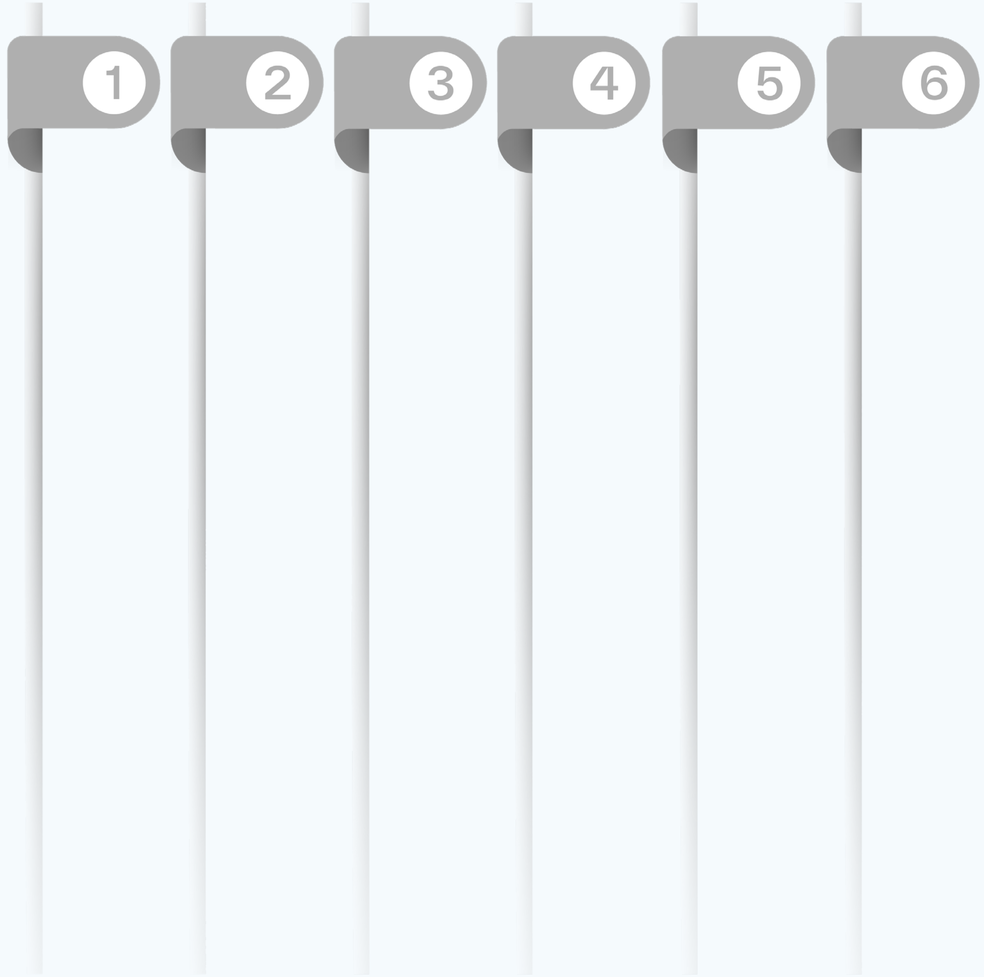
Where IAM is based on validating identities, privileged access management (PAM) is based on validating access to resources, particularly critical or sensitive resources. PAM essentially operates as a gatekeeper, providing certain employees with access to certain pieces of privileged information. That said, IAM and PAM do share some similarities. For example, who has access to what in both IAM and PAM solutions is role-based. Both require strong authentication and multi-factor authentication, continuous monitoring, and strict policy enforcement.

But they are distinct. PAM provides more granular control over assets and, more importantly, it can also protect against attacks on those assets by non-authorized users. PAM also brings strict access control standards to critical assets, making it much less flexible but much more secure. Finally, PAM ensures that accounts established by IAM and bolstered by MFA can only access the assets for which they have privileges, ensuring that only verified users can access sensitive or critical assets.

Rather than leverage one or the other, centralized tools marry IAM and PAM to reduce hassles for end-users—which is key to ensuring that organizations can successfully control access. With IAM and PAM enjoined for centralized access, end-users can enjoy faster logins while IT staff receive detailed reports that enable them to identify risky use patterns or compromised credentials before the damage is done. And your customer can better manage access across their entire business.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps?



Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps?

1 Build a Zero-Trust Roadmap

Success starts with a comprehensive zero-trust roadmap that outlines the activities needed to implement your customer's zero-trust strategy. This strategy document will provide a clear view of the deliverables, budget, and business outcomes expected.

- Determine a framework, whether it's the NIST or CISA framework or a framework from Gartner, Forrester, or others. TD SYNNEX can help you select the right vendors to help you craft a zero-trust vision.
- Recruit business and IT stakeholders—from IT operators to enterprise architects to business unit leaders to C-suite executives—who can help build your customer's zero trust roadmap and evangelize the need for new or shifting investments or significant cultural and organizational change.
- Identify interdependencies between the zero-trust implementation and other IT and business projects.

2 3 4 5 6

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps?

1 2 3 4 5 6

2 Refine the Business Continuity Plan

Every organization today should have a business continuity plan that outlines what happens when (not if) they're attacked. The next step is to help them adopt or periodically stress-test and refine their business continuity plan.

Then, put together an up-to-date inventory of systems (and prioritize them by the criticality of their stored data) to make it easy to structure actions in the case of a threat or attack. Create playbooks, conduct tabletop exercises and test backups for critical assets.

The more you can help them prepare, the better off they'll be in the event of a cyberattack or other disaster.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps?

1 2 **3 Assess Their Environment** 4 5 6

Next, help your customer understand their unique risks by identifying vulnerabilities in their environment and providing recommendations. Take advantage of these assessments:

- **Security Maturity Assessment –** Get a complimentary 45-minute assessment of your customer's security practices and controls and provide a graded report with a customized action plan to improve their security posture.
- **Penetration Testing –** Show them how bad actors exploit their systems to access and disclose sensitive data and how to best prioritize vulnerabilities for remediation.
- **Vulnerability Assessments –** Point out the pathways that attackers use to exploit their systems and provide a complete financial risk analysis with ways to re-allocate limited resources to ensure they're protected.
- **Additional Assessments –** Access additional assessment capabilities, including Security Risk Assessments, Physical Security Assessments, Physical Penetration Testing, GDPR Assessments, and many others.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps?

1 2 3

4 Offer Comprehensive Services

5 6

Help customers focus on their core business by leveraging our advanced managed and other security services:

- **Incident Response Services –** Comprehensive Incident Response (IR) services—including Plan Development, Readiness Review, and Emergency Response—ensure they have the right capabilities to respond to and recover from threats.
- **Compliance Services –** Governance and compliance readiness services for HIPAA,cHITRUST, PCI-DSS, NIST 800-171, ISO 27001, NERC-CIP, SOC 1&2, GDPR and others—ideal for businesses that face a high regulatory burden.
- **Implementation Services –** Services for new installations, integrations, patch services, configurations, and staff augmentations to help you design the best solution for them.
- **Managed Security Services –** These managed services help you maximize limited resources:
  - **SOC as a Service:** Have a bench of cyber experts who can monitor, analyze, manage and act on threats across your customer's business.
  - **Firewall Services:** Help your customer focus on their core business while you administer, monitor and maintain their firewall infrastructure.
  - **ISAO Threat Feed:** Join a very large community of companies, local governments and security professionals to collaborate, share intelligence, and participate in training and conferences and leverage competent collaborative analysis.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps?

1 2 3 4

5 Engage Through Training and Engagement Experiences

6

Finally, engage your customer's team with numerous training and engagement experiences for both new and advanced users.

Training

- **Foundational –** Develop the foundational cybersecurity skills needed to advance to the next level through the Cyber Essentials Series.
- **Accelerated –** Access over 50 cloud-based, instructor-led classroom learning courses to prepare for cybersecurity careers and train on a hyper-realistic network within a cloud-hosted cyber range using the tools your team uses every day.
- **Virtual –** Choose from an extensive set of courses for new cybersecurity team members or, for more advanced users, an upgraded training program that includes the entire course library, 200+ Virtual Lab Environments, a guided mentor, and industry certification practice tests.
- **Advanced threat training –** Learn how to contain threats, fix weaknesses, and use the latest threat hunting tools via online, gamified training using real-world simulations within a protected environment.

Engagement

- **Demos –** Test and engage with leading cybersecurity offerings to see how they work in real time.
- **Engagement –** Engage in an "up close and personal" live cyber experience to test the responses of your team and/or environment in a cyber range.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps?

1 2 3 4 5

6 Sell and Build SASE and XDR into the Security Stack

According to Gartner, "by 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch and edge access, up from 10% in 2020."[1] Security leaders will also want to consolidate their products/vendors, be more proactive in their response to threats, and drive greater efficiency—and they're increasingly turning to MSPs and MSSPs who truly understand their security challenges.

- Perform a gap analysis and establish a high-level SASE strategy and roadmap that's closely aligned with business goals and wider organizational strategic initiatives (such as cloud migration, cybersecurity policies, and IT strategy plans). Ensure the plan leverages the customer's existing assets and enables them to transition to an SASE model over time.
- Assess your client's current network and security environment, and the resources they have available, to determine which services they need, the processes to be used, what technologies will be deployed, and the training required.
- If your customer already has an SD-WAN, they may only need SSE capabilities. If they don't, determine whether they can benefit from SASE now or whether SSE can be an on-ramp for SASE.
- Evaluate the point solutions your customer has and any underutilized functionality, as well as the level of automation and integration between them, and consider a consolidation strategy anchored with XDR.
- Help your customer understand the synergistic value offered by XDR—for example, underlying data lake foundation with lower-cost and flexible data storage, functional orchestration and automation, and advanced security analytics—and not just in how you can pare down the number of solutions and/or vendors.
- Deliver XDR as a service to minimize maintenance for you and your customer.
- Cut time to sale by packaging up or bundling solutions you've already vetted—or provide a menu of pre-vetted vendor solutions from which to choose.

We're Here to Help...

If your team is short on time, budget, or expertise, we can help. We're backed by a team of dedicated security consultants with the expertise and resources to ensure that your customer's environment is secure. Our solutions and services, extensive portfolio, and industry expertise help to address most critical cybersecurity needs.

Our sponsors are listed on the next page, along with contact information to reach a TD SYNNEX security professional. Contact us...Our experts are your experts!

Contact the Team

Thank You to Our Sponsors!

For more information on any one of these or other TD SYNNEX security solutions or services, please contact our security professionals below:

HPE aruba networking

Learn more about HPE Aruba Networking SSE, SASE and SD-WAN solutions and download related offers or contact the dedicated HPE Aruba Networking team at TD SYNNEX.

CHECK POINT™

Ready to kickstart your security business with Check Point? Contact us today at CheckPointBD@tdsynnex.com !

Progress®

To learn more, visit the Progress website.

SONICWALL™

Please contact SonicWallSales@tdsynnex.com with any questions or to explore a solution that's right for your customer's environment.

Symantec™ by Broadcom

To learn more, please visit our CyberSolv page at Symantec – CyberSolv (tdsynnex.com) or reach out to the Symantec TD SYNNEX team at BroadcomBD@tdsynnex.com.

TREND MICRO™

Learn more today by reaching out to our business development team at TrendMicroSales@tdsynnex.com.

WatchGuard™

To learn more, visit our WatchGuard website or contact WatchGuard@tdsynnex.com.

References and Further Reading

1. Gartner. Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022. Sept. 9, 2022.
2. ECPI University. The Evolution of Network Security. Accessed Dec. 8, 2023.
3. Kung, Dar-Ning. An Evolution in Security: Intrusion Prevention. SANS Institute. Oct. 2, 2003.
4. Williams, Greg. The digital detective: Mikko Hypponen's war on malware is escalating. March, 19, 2012.
5. AV Atlas. Total Amount of Malware and PUA. Accessed Dec. 8, 2023.
6. Bruneau, G. The History and Evolution of Intrusion Detection. SANS Institute, GSEC Version 1.2f. 2021.
7. Frąckiewicz, M. The History of VPNs: From Early Beginnings to Modern Usage. TS2.space. July 7, 2023.
8. Tam K., Salvador M.H., McAlpine K., Basile R., Matsugu B., & More J. UTM Security with FortiNet: Mastering FortiOS. Syngress. 2013. https://doi.org/10.1016/C2011-0-05893-3
9. Forrester. Forrester Zero Trust Edge (ZTE) Unifies SASE Architecture with Zero Trust Principles. Feb. 17, 2021.
10. TechTarget. Why SASE should be viewed as an evolution, not revolution. Oct. 23, 2020.
11. Grand View Research. Cloud Access Security Broker Market Size Worth $25.6 Billion by 2030: Grand View Research, Inc. GrandViewResearch.com. Oct. 3, 2022.
12. Gartner.com Glossary. Secure Web Gateway. https://www.gartner.com/en/information-technology/glossary/secure-web-gateway. Accessed Nov. 5, 2023.
13. NetworkWorld.com. The Evolution of Zero Trust Network Access. Feb. 24, 2023.
14. Gartner. Market Guide for Single-Vendor SASE. Gartner.com, ID G00768660. Sept. 28, 2022.
15. Gartner. Market Guide for Extended Detection and Response. Gartner.com. Nov. 8, 2021.
16. Gartner.com Glossary, Endpoint Protection Platform (EPP). https://www.gartner.com/en/information-technology/glossary/endpoint-protection-platform-epp. Accessed Nov. 5, 2023.
17. Cloud Security Alliance. Modernizing Security Operations with XDR. CloudSecurityAlliance.org. Nov. 22, 2021.
18. SC Magazine. Want to stop modern cyberattacks? Use XDR with identity. SCMagazine.com, Feb. 22, 2023.
19. CrowdStrike. CrowdStrike 2023 Global Threat Report. Crowdstrike.com. 2023.
20. CyberArk. The Evolution of Identity Access Management: A Look into the Past and the Future. CyberArk.com via LinkedIn. May 31, 2023.
21. SHI. Modern identity and access management. SHI.com. March 9, 2021.
22. Identity Management Institute. Identity Governance and Identity Management IdentityManagementInstitute.org.