Practical considerations for consolidating security environments

Data#3

cisco
Partner

In recent years, we've noticed an increase in customers asking us whether consolidating their security environments around a select few vendors is a good approach – and, if so, how to approach it.

The short answer is yes – it should be considered by every organisation. While no single vendor can provide all the security solutions you need today, a consolidation strategy can dramatically reduce complexity and risk. In this blog, we clarified what we mean when we talk about consolidation and shared some customer insights based on their experiences over the years.

In this eBook, we'll showcase some high-level examples of how consolidation can work in the real world, where years of investment have typically resulted in complex security environments with multiple overlapping solutions from different vendors.

To do this, we will look at four broad security areas and use Cisco's extensive security portfolio to illustrate the examples. The areas we will look at are:

- **User protection:** protecting remote and mobile workers using multiple devices in multiple locations, while still providing the same in-office experience
- **Network security:** revisiting the role of the firewall in a zero trust world
- **Breach detection and response:** an area of renewed investment lately, focusing on improving your ability to detect when a breach has happened and how to manage the response
- **Cloud security:** an area that still causes a lot of confusion with more acronyms per paragraph than normal – even for seasoned IT professionals

Contents

User protection

User protection may sound like it's about safeguarding users, but it's actually about shielding organisations from potential threats arising from compromised user credentials or devices. To achieve this, organisations deploy various software clients to manage different security capabilities, all while trying to give users the same working experience whether they're remote or in the office.

The primary requirement for these users is the ability to securely connect to applications and data, either on-premises or in the cloud, from anywhere.

VPNs have been the default option for users when accessing corporate applications and networks outside the office, but several issues have emerged with VPNs, such as:

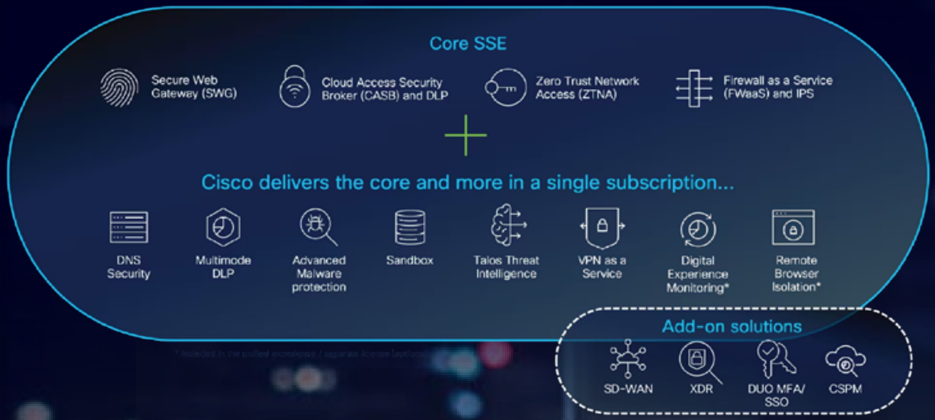
- Their inability to scale
- 'Hair pinning' traffic between on-premises and cloud applications with resulting performance issues
- Question marks over their security robustness in the event of user credential compromises
- A generally poor user experience with questionable reliability

A VPN needs its own client installed on the user's device, but this is also a source of frustration due to the growing number of software clients need for complete protection. As noted above, users might also need clients for MFA, SD-WAN, malware and antivirus protection, SSO, and more. If this sounds like your environment, then this is arguably the easiest area to start considering consolidation as it can greatly improve usability without compromising security.

Cisco solution example

Cisco's Secure Access solution is a template for consolidation, incorporating an extensive set of disparate capabilities in a single Secure Service Edge (SSE) client.

Cisco Secure Access


Core SSE
Secure Web Gateway (SWG)
Cloud Access Security Broker (CASB) and DLP
Zero Trust Network Access (ZTNA)
Firewall as a Service (FWaaS) and IPS
Cisco delivers the core and more in a single subscription...
DNS Security
Multimode DLP
Advanced Malware protection
Sandbox
Talos Threat Intelligence
VPN as a Service
Digital Experience Monitoring*
Remote Browser Isolation*
Add-on solutions
SD-WAN
XDR
DUO MFA/ SSO
CSPM
* Included in the unified experience / separate license (options)

What makes this approach particularly effective is that you don't need to include every capability all at once. It's a configurable option, where customers can select only the parts of the solution they need at the time. To add more capabilities down the line it's just a configuration change, not another client to install.

This approach has helped Cisco overcome a large barrier to adopting new technology. Orchestrating the rollout of yet another software client (along with its management tool) and integrating a new capability can be challenging for organisations. Using MFA as an example – if you want to implement MFA, it's an easier process to make a license change and include MFA capabilities in the Secure Access client you already know and understand rather than deploy a new one. Similarly, if you already have an MFA client from another vendor, you have a simple consolidation path to bring that capability under the existing Secure Access client.

For its 2023 Voice of the Enterprise Security Customer report, Frost & Sullivan cybersecurity researchers surveyed 2,448 enterprise CISOs in six regions around the world. Those security leaders were asked which were the primary cybersecurity vendors they chose for cloud security. More than half of those surveyed cited Cisco as a primary cloud security provider.[1]

Network security

Bringing our consolidation lens to Network Security, we'll focus on the firewall's role in managing security policies and how it's changing as our networks have evolved.

Most organisations have firewalls from various vendors across their environment. That might be because of company acquisitions over time, or perhaps different managers have had different preferred suppliers over the years.

Whatever the reason, this isn't normally a problem – they can all coexist happily. However, each firewall operates in slightly different ways, sometimes with subtle differences in how each applies specific security policies. Each firewall also has its own native management tools to account for those differences, which can introduce gaps in security when different firewalls are used in different areas. When you consider that 58% of organisations have over 1000 firewall rules[2] (some complex environments with rules in the millions) and Cisco estimates that one-third of those rules are broken[3], it's no wonder misconfigurations are the cause of 99% of all firewall breaches[4].

Consolidating around a single vendor for firewalls is the best (albeit difficult), way to solve these problems, but we can still take a simplified approach. In this case, we can look to SASE and AI advances to improve this environment.

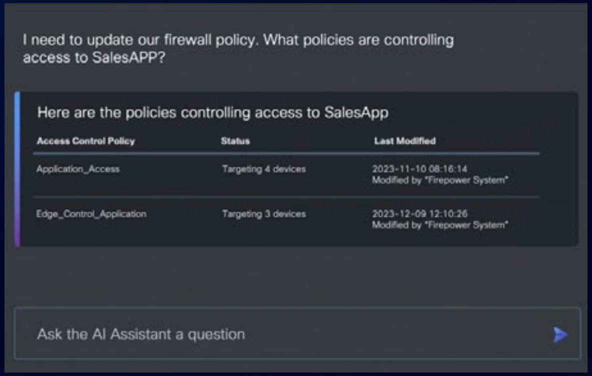
Cisco solution example

SASE allows us to remove the access control mechanism from firewalls and put those controls in the cloud. This ensures consistency over the security mechanisms and policies without the need for wholesale changes to your firewalls.

There is also a secondary benefit here. With the control mechanism in the cloud, you can start shifting away from full-featured firewalls towards lower-spec firewalls as renewals arise – or you can just sweat those assets for longer without the need to upgrade.

If you're not ready for SASE, there are numerous benefits in standardising on a single vendor for firewalls that make it worth the effort. As a starting point, all your firewalls can be managed through a single interface – in this case, Cisco Defense Orchestrator.

For rule management, Cisco's AI assistant for Security allows administrators to use natural language to accelerate troubleshooting and configuration tasks. It helps admins discover policies and get rule recommendations to eliminate duplicate rules and misconfigured policies. The AI Assistant can also check optimisation of current policies and rules on the FW, freeing up resources for other work.

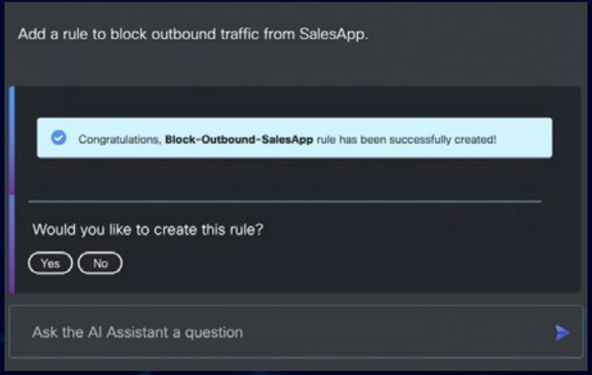


I need to update our firewall policy. What policies are controlling access to SalesAPP?

Here are the policies controlling access to SalesApp

Access Control Policy	Status	Last Modified
Application_Access	Targeting 4 devices	2023-11-10 08:16:14 Modified by "Firepower System"
Edge_Control_Application	Targeting 3 devices	2023-12-09 12:10:26 Modified by "Firepower System"

Ask the AI Assistant a question



Add a rule to block outbound traffic from SalesApp.

Congratulations, **Block-Outbound-SalesApp** rule has been successfully created!

Would you like to create this rule?

Yes
No
Ask the AI Assistant a question

The tight integration between firewalls from remote branches to campus delivers secure connectivity, identity, and policy management with end-to-end visibility, enforcement, and cloud security. It's a powerful outcome worth considering as your existing firewalls come up for refresh.

Breach detection and response

You can't fix what you can't see. Despite all the investment in cybersecurity, breaches can still happen. The critical question is: How long can the attacker remain hidden in your environment? This is known as 'dwell time.' On average, dwell times in 2023 ranged from 8 days to 9 weeks. The key takeaway is that detection happens after a breach has already occurred – and the longer they remain undetected, the longer the attackers have to steal data or plant ransomware. In worst case scenarios, organisations may never realise a breach has occurred.

There have been instances where customers began using a Data#3 managed security service, and during the onboarding and discovery, we found evidence of a breach that had gone undetected. Visibility is everything, but finding time to investigate all the alerts and notifications is challenging in environments with multiple monitoring tools covering infrastructure logs, endpoint telemetry, cloud and network data, and more.

Cisco solution example

There is a growing trend towards the use of XDR (Extended Detection and Response) tools, such as Cisco XDR, to consolidate all these individual capabilities and reduce dwell times. Cisco XDR brings a unified view to multiple sources of data regardless of vendor or attack vector. Unlike a more expensive and complicated SIEM (Security Information and Event Management), which primarily analyses log data, XDR integrates:

- Endpoint detection and response tools
- Cloud, network, and firewall tools
- Email and application data.

This combination of data sources allows XDR to contextualise events across multiple areas, leading to more accurate and timely detection. For example, while reviewing firewall event logs, you might see an external connection that should be checked if it wasn't buried in amongst other notifications. However, if that connection hits an endpoint and starts doing strange things, the combination of these two events viewed by an XDR could be enough to confirm there is an issue that requires urgent investigation.

Cisco XDR also enables tight integration with other tools and capabilities, such as email threat defence and network analytics, to further consolidate your security environment. These integrations provide a 1+1 = 3 capability by sharing information and providing more confidence in what actions to take through automation (where appropriate), and escalation.

The shift towards 'best-of-suite' over 'best-of-breed' reflects a prioritisation of integrated solutions over isolated product excellence. While the best-of-breed approach focused on individual product excellence, the power of tight integration and being able to consolidate and compare multiple capabilities can be more powerful.

Multi-cloud security

The need to protect hybrid and multi-cloud environments with end-end security for applications, workloads, networks, and data is obviously crucial. However, any discussion on multi-cloud security needs to start with an introduction (or refresher) on acronyms such as CNAPP, CSNS, CWPP, and CSPM.

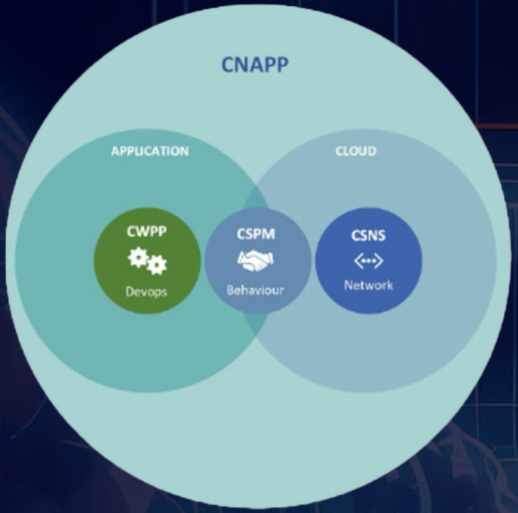
CNAPP: Cloud Native Application Protection Platforms. Coined by Gartner, this term refers to a “unified and tightly integrated set of security and compliance capabilities, designed to secure and protect cloud-native applications across development and production.” It’s an overarching term for the capabilities included in any discussion of hybrid and multi-cloud security. Understanding these capabilities is crucial for effective cloud security management.

CSPM: Cloud Security Posture Management. This looks at how secure your cloud environment is in terms of misconfigurations, which could expose cloud resources and cause security incidents.

CWPP: Cloud Workload Protection Platform. Similar to an antivirus for cloud workloads, CWPP protects your cloud infrastructure workloads across VMs, databases, APIs, containers, and Kubernetes.

CSNS: Cloud Service Network Security. Aims to protect cloud infrastructure in real-time using mechanisms such as Next-Gen Firewalls, Web Application Firewalls, DDOS protection, load balancing, and SSL inspection.

This diagram shows the relationship between all four terms.



Cisco solution example

Cisco Multicloud Defense is a highly scalable, on-demand ‘as-a-Service’ solution that provides agile, scalable, and flexible security to your multi-cloud infrastructure. It unifies security controls across cloud environments, protects workloads from every direction, and drives operational efficiency by leveraging secure cloud networking.

Consolidation of multiple cloud provider solutions is one thing, but when they each have differentiators to bring to the customer, it can be challenging to consolidate on just one platform.

That’s where Cisco Multicloud Defense excels. It allows organisations to set security policies across all these platforms using a common language. This means you’re not only consolidating multiple solutions into one but making your employees more efficient in managing them and creating security policies by removing the need for them to know what language each cloud provider ‘speaks’. It connects the language of IPs (traditional side of the fence) to services (cloud provider language). Another key benefit of Cisco Multicloud Defense is its ability to enforce these policies dynamically. With dynamic multi-cloud policy management, you can:

- Keep policies up to date in near-real time as your environment changes
- Connect continuous visibility and control to discover new cloud assets and changes, associate tag-based business context, and automatically apply the appropriate policy to ensure security compliance
- Power and protect your cloud infrastructure with security that runs in the background via automation, getting out of the way of your cloud teams
- Mitigate security gaps and ensure your organisation stays secure and resilient
- Add enforcement points (PaaS) in both distributed and centralised architectures

Considerations when consolidating

Any consolidation from a multi-vendor environment in one or more of the areas we've discussed in this eBook requires a well-thought-out strategy to ensure a smooth transition, minimal disruption, and security maintenance or enhancement throughout the process.

Here's a generalised list of steps to consider as a starting point. Data#3's dedicated cybersecurity practice can tailor an approach that focuses on the area with the most consolidation potential to help improve and simplify your environment.

1. Conduct a detailed assessment

Inventory: Start with a comprehensive inventory of all current security solutions, their configurations, and how they are used within your environment. This includes hardware, software, cloud services, and any custom integrations.

Identify dependencies: Understand the dependencies between your current security solutions and other IT systems. Some security tools might be tightly integrated with non-security systems, necessitating careful consideration during migration.

Assess overlap and gaps: Identify areas where consolidated options such as Cisco Secure Access will replace existing functionality or fill gaps in your current security posture. Conversely, note any capabilities your current solutions have that Cisco Secure Access does not directly replace.

2. Develop a strategic migration plan

Prioritise: Based on the assessment, prioritise migration phases. It might be practical to start with services that have the least dependencies or are easiest to transition.

Phasing: Determine if the migration will occur in phases or all at once. Phased approaches reduce risk but might prolong the total migration time.

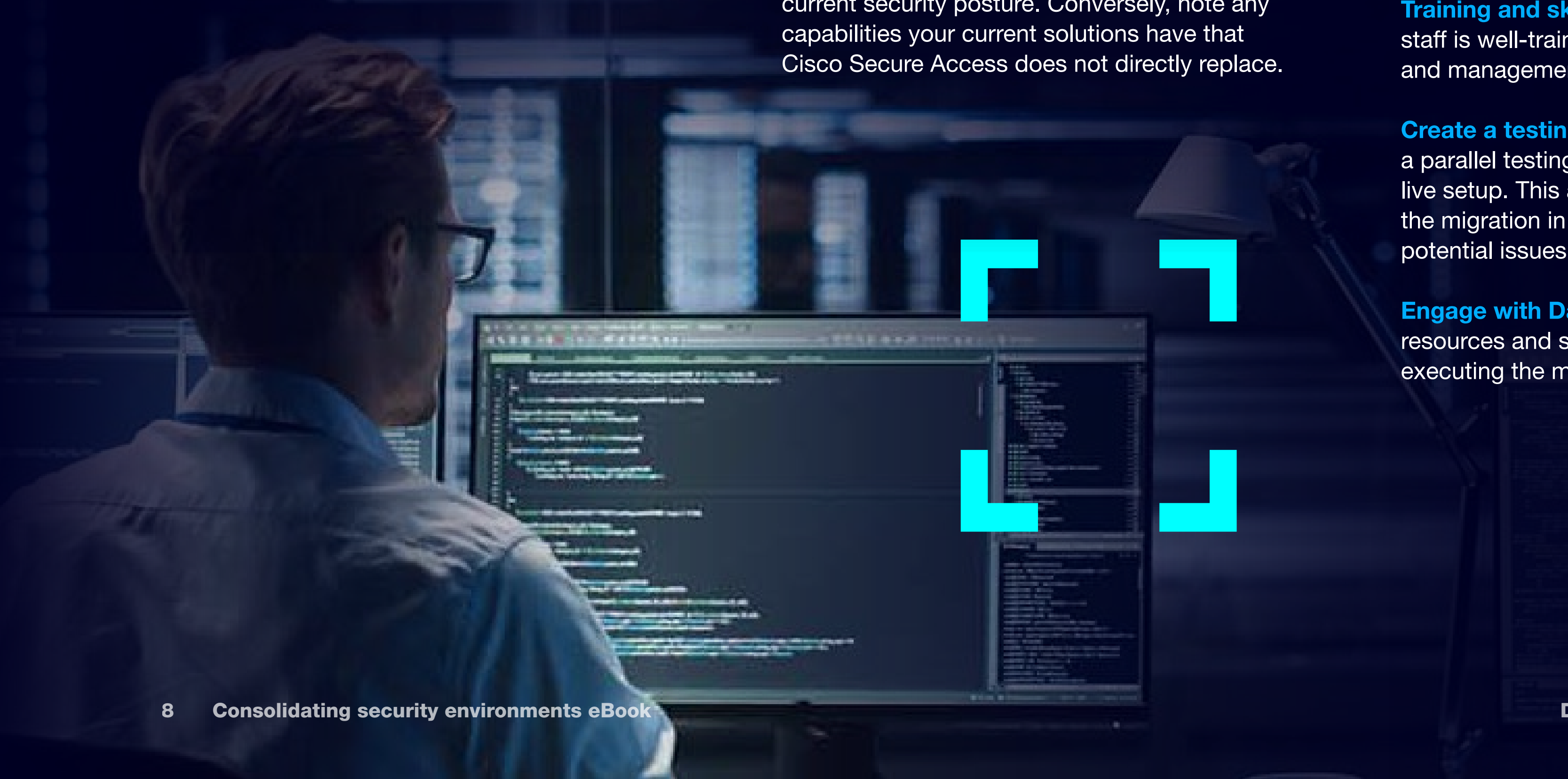
Blueprint for transition: Create a detailed plan for each phase, including what will be migrated, when, and by whom. Ensure contingency plans are in place in case of unexpected issues.

3. Preparation and testing

Training and skills development: Ensure your IT staff is well-trained in capabilities, configuration, and management of the new solution.

Create a testing environment: If possible, create a parallel testing environment mirroring your live setup. This allows you to test every step of the migration in a controlled manner, identifying potential issues before they affect production.

Engage with Data#3 experts: Utilise Data#3's resources and support services for planning and executing the migration.



4. Implementation

Start with non-critical systems: If adopting a phased approach, begin migration with less critical systems to minimise the impact of any teething problems.

Monitor closely: Throughout the migration process, monitor systems closely for any issues. Quick identification of problems allows for speedy resolution, minimising impact.

Communication: Maintain clear and open communication with all stakeholders throughout the migration process. This includes IT staff, end-users, and management.

5. Optimisation and Continuous Improvement

Feedback loop: After each phase of the migration, gather feedback from users and IT staff. Use this feedback to improve the process for subsequent phases.

Optimise configurations: Continuously monitor performance and adjust as necessary to optimise security and efficiency.

Security posture review: Once the migration is complete, conduct a comprehensive review of your new security posture to ensure it meets all organisational requirements and addresses previously identified gaps.

6. Documentation and compliance

Update policies and procedures: Ensure all security policies and procedures are updated to reflect the new environment.

Compliance verification: If your organisation is subject to regulatory compliance, verify that the new setup complies with all relevant regulations and standards.

Cisco Master Security Specialised

Data#3 has one of the most mature and highly accredited security teams in Australia. Working in partnership with Cisco, we have been helping our customers achieve a more connected and secure organisation for more than 25 years.

To explore how you can simplify and strengthen your security environment, request a security audit with a Data#3 specialist today.

Talk to an expert

- data3.com
- facebook.com/data3limited
- twitter.com/data3limited
- linkedin.com/company/data3
- youtube.com/user/data3limited

Data#3 | cisco Partner

Sources

[1] Frost & Sullivan (2024). Best Practices Award. [ONLINE] Available at: https://learn-cloudsecurity.cisco.com/csa-library/frost-and-sullivan-award-2024

[2] Cisco (2023). Give your firewall admins superpowers with the Cisco AI assistant for security. [ONLINE] Available at: https://blogs.cisco.com/security/give-your-firewall-admins-superpowers-with-cisco-ai-assistant-for-security

[3] Cisco. [ONLINE] Available at: https://www.cisco.com/site/au/en/products/security/firewalls/index.html

[4] Security Week (2019). State of firewall report. [ONLINE] Available at: https://www.securityweek.com/state-firewall-report-automation-key-preventing-costly-misconfigurations/

[5] Sophos (2023). The 2023 active adversary report for tech leaders. [ONLINE] Available at https://news.sophos.com/en-us/2023/08/23/active-adversary-for-tech-leaders/

[6] Splunk (2024). State of security 2024: The race to harness AI https://www.splunk.com/en_us/form/state-of-security.html