eBook

Cadre
information security

ULTIMATE GUIDE TO SECURING HYBRID WORK

TABLE OF CONTENTS

A SOLVABLE CHALLENGE: SECURING HYBRID WORK

Time provides perspective. In this case, the hype surrounding the impact of global events on IT and security hasn't been oversold. After years of nearly every security vendor pitch beginning with a mention of the pandemic, we've now had time to collect real-world data to understand the truth. And that is, all signs point to tangible trouble. We can verifiably say forced hybrid and remote work expanded the attack surface.

According to a survey conducted by Check Point Software, 45% of IT and security respondents have noted an uptick in cyber attacks since the shift to remote work.[1]

Top breach and attack vectors since COVID-19:

- **55%** Data exfiltration and leakage
- **51%** Phishing emails
- **44%** Account takeover

In the same study, respondents weighed in on their top challenges in the new, distributed environment. These included:

- **46%** Scaling performance
- **42%** Ensuring privacy
- **40%** Supporting Bring Your Own Device (BYOD)

Distributed workforce protected. Confidence restored.

Routing all traffic to the on-premises datacenter for traffic inspection was once an effective strategy. Now it falls short for both security and performance requirements as work is done outside of the perimeter. Past the point of devising "band aid fixes" to support daily work, now is the time to solve the security-performance balancing act.

The good news is that security vendors have developed innovative ways to protect our new environment. To help connect the dots between security and performance, this eBook aims to guide the reader through architecting an ideal technology and services toolbelt for a secure hybrid workforce.

Remote workers struggle most with performance (latency), instability and crashes, and VPN issues – resulting in an influx of help desk tickets.

[1] Check Point Software. "Remote and Hybrid Work Security Report." 2021

THE HYBRID LANDSCAPE

Employees, contractors, third-parties, and others connecting and sharing sensitive data are using multiple devices to access the internet, corporate network, and applications. As a result, that sensitive data becomes unmanaged as it continually flows from both corporate and personal BYOD devices to the cloud and datacenters.

In years past, security teams may have been able to say "no" to applications or certain methods of access because of difficulties of securing and maintaining visibility. Now, however, denying what boils down to being 'business enablers' is not an option. If users aren't granted access, and are autonomous with personal devices at hand, they have the option of going around deployed security for a productive workday.

You cannot protect what you cannot see

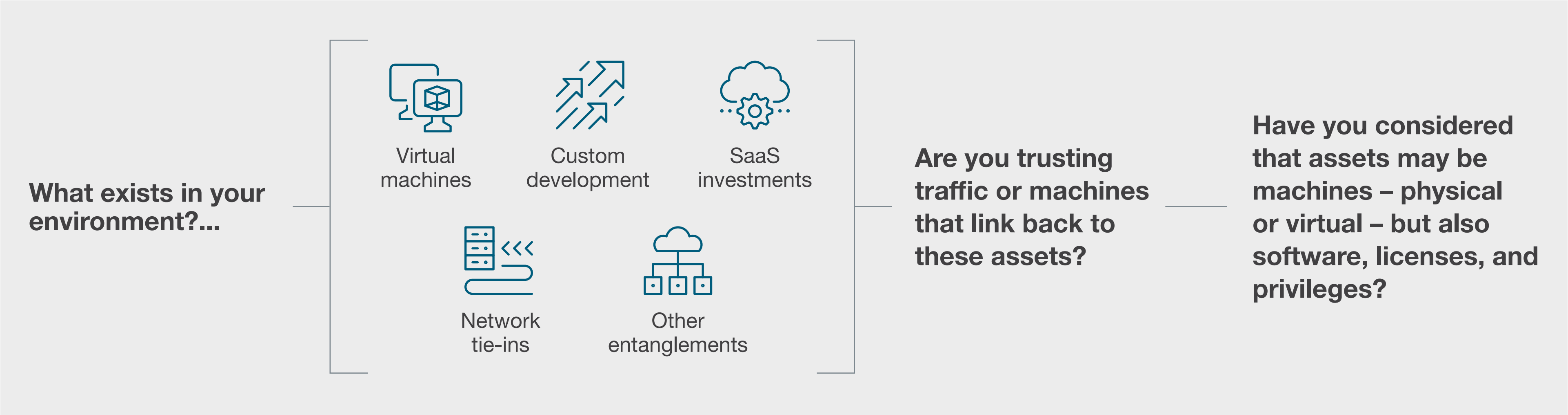
One of the most important starting points in cybersecurity is basic asset identification and visibility. This is especially true as companies expand their cloud footprint and users create Shadow IT and Shadow Cloud assets.

According to the 2022 SANS Survey: Securing Infrastructure Operations, much of what the greater end user population accesses exists in the cloud.[2]

Types of cloud services/applications organizations utilize most:

- **56%** Web applications (external)
- **52%** Office automation
- **51%** Web applications (internal)
- **48%** File storage
- **46%** Databases

These results, while unsurprising, place emphasis on where security teams need to focus their efforts.



What exists in your environment?...

Are you trusting traffic or machines that link back to these assets?

Have you considered that assets may be machines – physical or virtual – but also software, licenses, and privileges?

[2] SANS Institute. "SANS Survey: Securing Infrastructure Operations." March 2022

FAST, PRIVATE, SECURE WEB ACCESS

Securing web usage typically boils down to an acceptable use policy. For example, organizations may choose to block policy-violating websites during work hours, like those used for gambling, while persistently severing access to malicious websites known for malware or phishing attempts.

Malicious actors understand the way users work and how legacy security solutions are ill-equipped to protect against an online world that changes daily. A website that may be deemed “safe” one day is not guaranteed to be uncompromised the next.

If the internet is the new office, then securing the web browser has to be at the top of the security to-do list. Whether employees are inside or outside of the office, ransomware, malware, and phishing attacks are threatening sensitive business data and worker productivity.

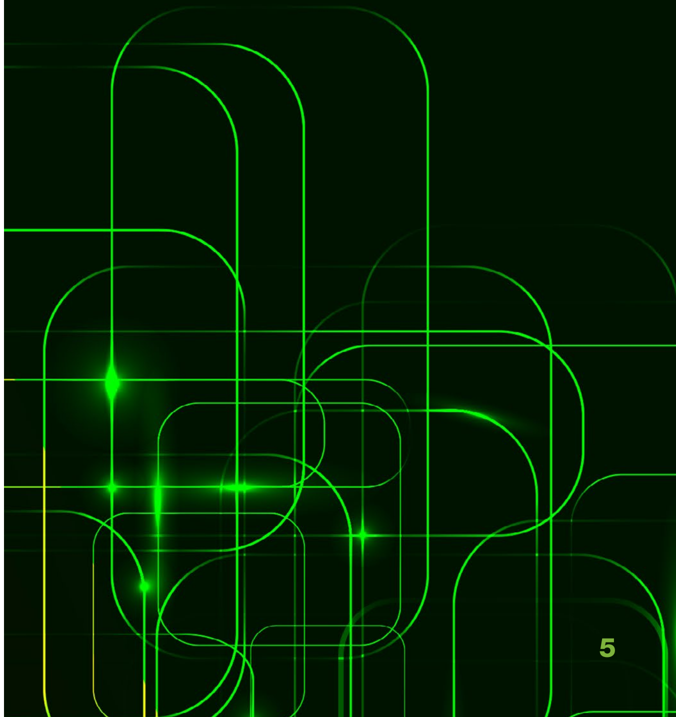
Remote Browser Isolation adoption soars

One of the most efficient and effective ways to protect web browsers is remote browser isolation (RBI).

Similar to zero trust, RBI technology trusts no websites. It ensures a secure web browsing experience by moving all internet activity to an isolated environment in a remote cloud-based container. This sandboxing of internet browsing protects data, devices, and network from a variety of threats originating from infected website code, such as:

- Zero-day exploits
- Malicious browser plugins and extensions
- Infected file downloads
- Malicious links and phishing emails
- And many more

To be productive, users need safe and reliable access to web-based information, applications, and productivity tools.



EMAIL: THE MAIN ENTRY POINT FOR ATTACKS

Email is a ball of twine when it comes to risks. Not only does it have multiple risk vectors – attachments, links, and social manipulation – but it is also the Matryoshka doll of communication. Alerts from chat messages or shared documents often get forwarded to email, expanding possibilities for attacks. The reality is, this danger has never been more prevalent as hybrid work distributes people and increases the reliance on email to keep communication flowing, no matter the location of the end user.

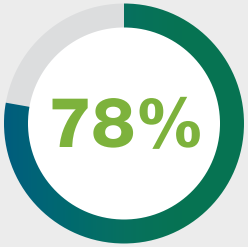
Protecting users from themselves

Human activated attacks are at the center of email attacks. A person has to click a phishing link for it to work, they have to download a malicious file for it to infect. The only real way to stop these behaviors is to educate, making security awareness and training a “must have” for all organizations. Even with security solutions that isolate potentially dangerous attachments or automatically tag suspicious email, all it takes is for one malicious email to get by and for a user to fall for the adversary’s tricks.

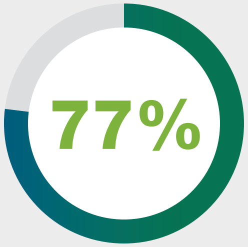
Email protection checklist

- ✓ Use an email security solution that includes anti-phishing technology to protect against BEC and uses artificial intelligence to identify anomalies in communication patterns and inspect for suspicious URLs.
- ✓ Use context-aware banners to reinforce security awareness training.
- ✓ Implement standard operation procedures for handling and sharing sensitive data commonly targeted by impersonation attacks.
- ✓ Use APIs to integrate email events into Extended Detection and Response (XDR) platforms and/or Security Information and Event Management (SIEM) tools to spot and remediate incidents faster and more efficiently.
- ✓ Examine what types of data are shared internally and externally via email and put appropriate controls in place.

Email attacks on the rise



of organizations experienced email-based ransomware attacks in 2021[3]



faced business email compromise (BEC) attacks – an 18% YoY increase[4]

[3] Proofpoint. “2022 State of the Phish.” February 2022

[4] Ibid.

SECURITY SERVICE EDGE

Achieving the security-performance balance for hybrid workforces relies on the Security Service Edge (SSE).

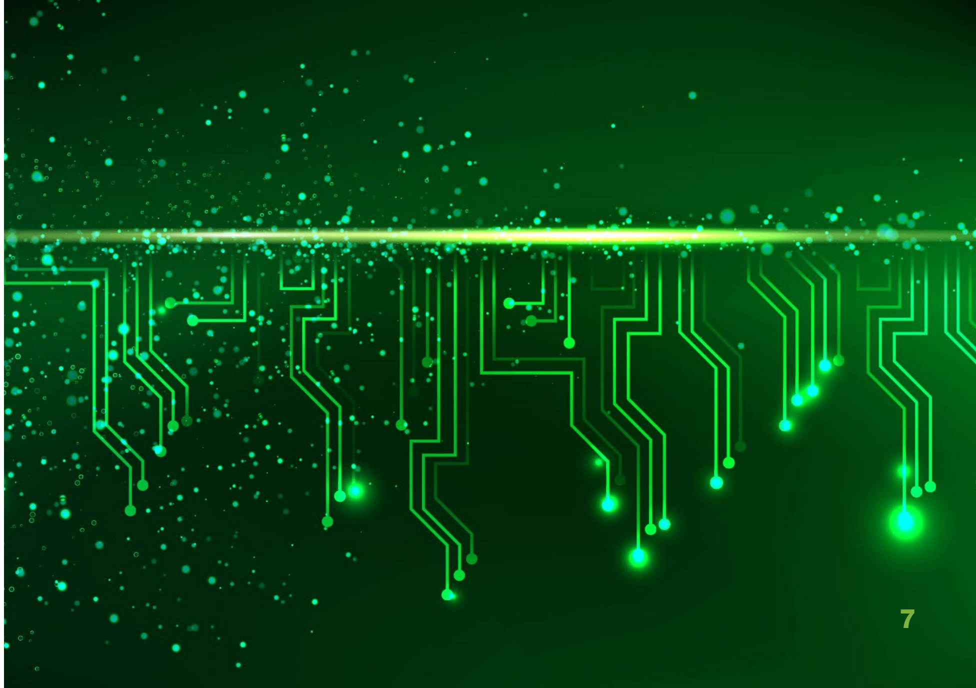
Defined by Gartner, SSE “secures access to the web, cloud services, and private applications. Capabilities include access control, threat protection, data security, security monitoring, and acceptable use control enforced by network-based and API-based integration. SSE is primarily delivered as a cloud-based service and may include on-premises or agent-based components.”[5]

The main idea of SSE is that security needs to be flexible and fit the “anywhere, anytime” approach to work. By offering a more dynamic and decentralized security architecture, it is able to scale to protect a large number of users, devices, applications, and data located outside the enterprise perimeter.

As the security portion of Secure Access Service Edge (SASE), SSE aligns secure web gateway (SWG), cloud access security broker (CASB), and zero trust network access (ZTNA). While each of these security solutions can be purchased and maintained separately, many vendors are now offering all three along with other technologies like RBI, data loss prevention (DLP), and cloud firewall.

When managing a hybrid workforce, there are already an overwhelming number of moving parts. To simplify this, choosing a vendor that can supply everything necessary to achieve SSE is the optimal decision.

Reactive legacy solutions rely on allow-or-block controls. This can frustrate users when they are stopped from accessing legitimate work and lead to more help desk tickets. SSE offers adaptive controls that improve security and reduce risk without additional hassles.



[5] https://www.gartner.com/reviews/market/security-service-edge

SSE COMPONENTS

It is important to set the expectation that translating SSE into your hybrid environment will take time and informed decisioning. For example, while SWG is a longstanding solution, not all are built for highly-distributed, work-from-anywhere environments.

Adoption milestones & outcomes

- Full cloud-based SSE stack → secures all users, everywhere
- Update DLP policy → provides clear guidance on where data can be stored, used, and accessed depending on user location
- Add CASB data authentication and encryption points → protects applications in the cloud with control and improved visibility
- Adopt ZTNA → overcomes shortcomings of overburdened VPNs in the hybrid work environment

Balancing technologies for positive outcomes

SSE is a general guidance, rather than a prescription on how to achieve positive security outcomes. By bringing the three core technologies in balance with operating needs, organizations can expect:

- **Strengthened security** by offering consistency both inside and outside of the physical office.
- **End user experience optimization** through seamless security that doesn't produce roadblocks, which users tend to go around.
- **Cost reduction** when consolidating SSE capabilities. And, through the security benefits that prevent or reduce data loss and event recovery.

SWG
Controls, monitors, and protects web traffic with the ability to enforce granular access and security policies.

CASB
Gives users safe access to SaaS platforms while offering security teams deep visibility and control.

ZTNA
Provides brokered access for users to applications.

PROTECT PRODUCTIVITY AND RISKS ON THE ENDPOINT

Protect against ransomware, phishing, bots, file-less attacks, and malware.

As employees split time between working in-office and remote, there must be a way to protect the variety of endpoints in use. While IT-issued desktop computers inside the corporate office have a verified history of security and connecting only to the corporate network, other devices aren't as clean cut.

Portable devices like laptops and smartphones used by remote workers often have a muddied past of network promiscuity. IT and security teams can't tell where they have been, if they were secured, or what other devices were plugged into them.

Companies not only need to reassess their technologies to ensure they are nimble enough to cover every use case, but also adopt strategies that will keep IT and security teams from burning out.

Strategies and technologies to protect endpoints for hybrid workforces

- ✓ Implement a Unified Endpoint Management strategy that doesn't rely on domain connectivity.
- ✓ Regularly patch both operating systems and applications.
- ✓ Implement a Principle of Least Privilege (PoLP) strategy that allows users to successfully accomplish their jobs without creating an attack vector, while also preventing lateral movement in case of an insider attack.
- ✓ Enforce Zero Trust principles to ensure no user, device, or application is automatically trusted.
- ✓ Use multi-factor authentication, single sign-on, continuous monitoring and auditing.
- ✓ Automate attack detection, investigation and remediation.
- ✓ Utilize RBI to protect devices by moving web browsing off endpoints to remote containers.
- ✓ Employ threat hunting software to cover both defensive and offensive measures.

MOBILE SECURITY FOR WORK ON THE GO

Mobile devices have tremendous benefits for users and organizations from a productivity standpoint. The problem though is that with Bring Your Own Device (BYOD) policies, many of those mobile devices used are unmanaged.

Protecting devices even when managed has never been easy. Application stores are chock full of malicious downloads, identifying suspicious email contents and attachments is harder on a mobile screen, and mobile specific vulnerabilities are a favorite attack vector of phishers.

Including mobile in Zero Trust Network Architecture

Mobile users are not always using VPNs to connect to your organization's data in the cloud. But you need to make sure they don't put sensitive data at risk. Using ZTNA, organizations can continuously authenticate users and revoke access at any time.

Beyond technology

Every tool that has the potential to make operations run smoother or faster also acts as a vehicle for bad actors to do the same. Where before, many organizations leaned on Mobile Device Management (MDM), it can now be used as an attack vector. For example, the Cerberus malware variant infected over 75% of one company's devices via corporate-owned MDM.[6] The malware, once installed, collected large amounts of sensitive data, including user credentials, and sent it to a remote command and control server.

Even with security technologies in place, users play the greatest part in protection. They can choose whether to click on a link, download a malicious attachment, or send confidential data unencrypted. It cannot be overstated that training employees on acceptable use, password hygiene, and mobile-specific threats are essential to mobile security.

3 Key Considerations for Mobile Security

1. **Complete protection**
   Mobile security should work across all attack vectors: applications, network, and OS.

2. **Operational ease**
   Mobile security should be part of the larger security ecosystem for easier management and scalability.

3. **User friendly**
   Mobile security must be easy to adopt and have zero or near zero impact on user experience or privacy.

[6] Check Point. "Mobile Security Report 2021." 2021

THE PERFECT HYBRID PLAN

With the vast number of options to secure a hybrid environment there hardly seems like a perfect plan. And while that's true given the ever-evolving nature of threats and cybersecurity technologies, there are steps everyone can take to get close to perfection. Instead of implementing stand-alone tools, organizations should consider a multi-faceted plan that goes beyond technology.

Starting with assessment

Assessments can happen at any time. There may be actual needs to conduct penetration tests or architecture reviews on a scheduled basis for compliance such as PCI, HIPAA, NIST and HI-TRUST. Even if compliance does not set an assessment schedule, it is sensible to engage a third-party annually for an assessment to avoid confirmation bias.

Knowledge is power

The best hybrid workforce security plans also take into consideration the people that interact with your data. This is threefold:

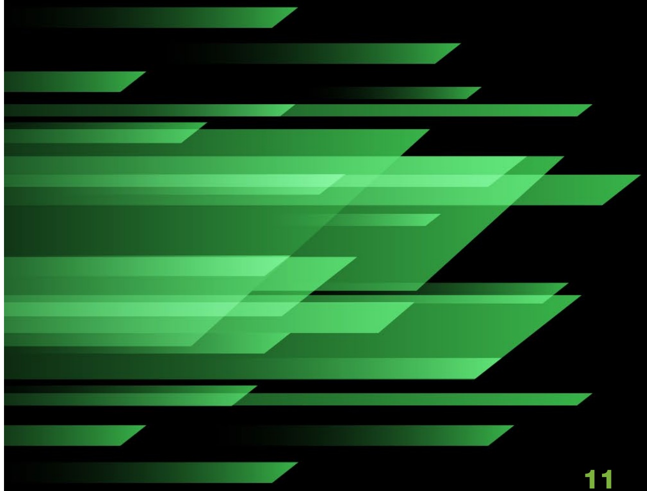
1. Educating users on security best practices.
2. Educating security teams on how to best use deployed technologies to get the most return on investment.
3. Educating everyone on the benefits of a security culture and how to always operate with security in mind.

Sort through the solution noise

It's not uncommon these days to read through security solution datasheets and come away thinking that every vendor offers the same thing. As vendors continue to add to their portfolios, it can be hard to discern who offers what and which solutions reign supreme (or at least for your specific environment).

Partnering with experts who have done the legwork of vetting vendors and their technologies is one way to circumvent the hours of research it takes to find the technologies you need. By engaging with a company that offers cybersecurity consulting, you can get a fresh perspective which has been enriched through work with similar organizations. In addition, you gain access to lessons learned and former successes which would have otherwise taken time, resources, and potentially irreparable damage to learn.

Rule of thumb: If you have a plan of what to do with the results of an assessment, it is always worthwhile. Discovering security gaps and unknown vulnerabilities provides a first step towards moving to a more secure environment both inside the office and anywhere work can be done.



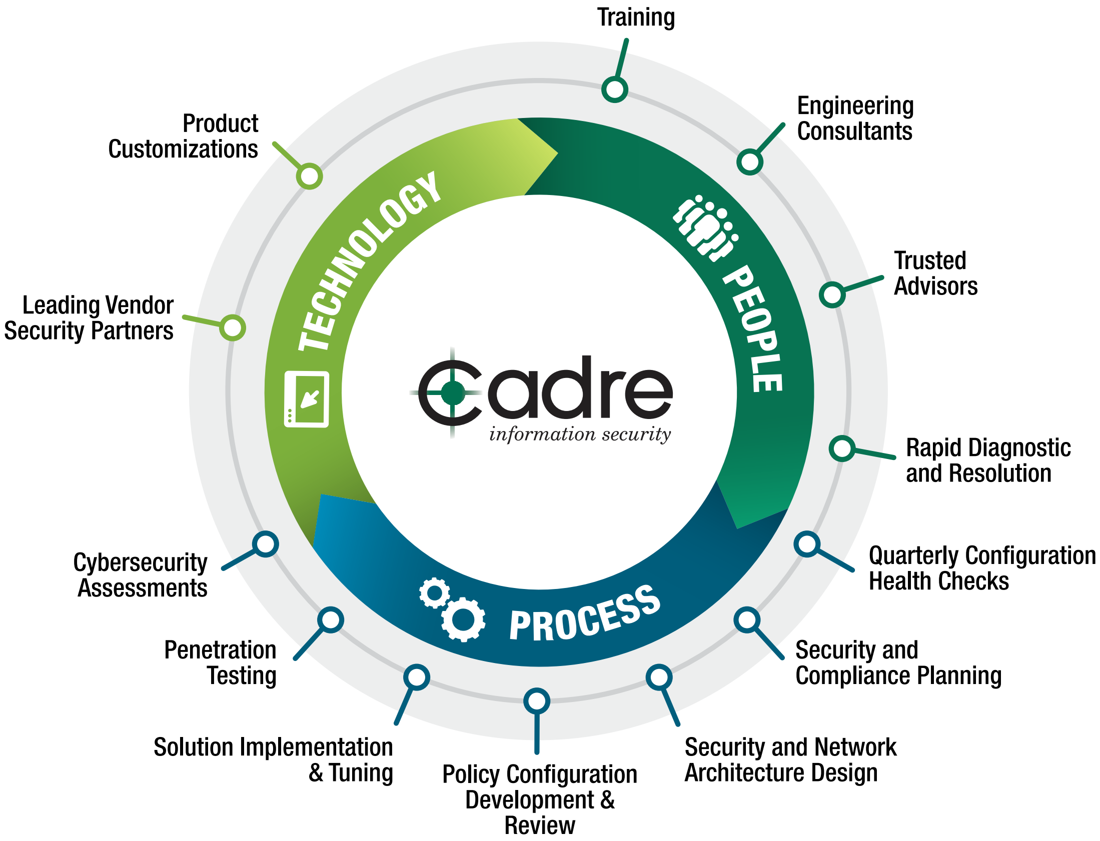
CADRE: YOUR TRUSTED ADVISOR

As a collective, we didn’t expect remote work to take such a sharp turn. Going from the exception to the primary form of work has shaken up the cybersecurity industry – highlighting the importance of remaining flexible and innovative.

While some companies are returning to the office, hybrid work is going to be the norm for the long haul and you will need to adapt and map the new security journey. As a group of unrelenting cybersecurity experts, Cadre has over 20 years of experience working with businesses of all shapes and sizes to ensure they are the most secure and efficient workplaces possible.

We’ve also formed a hand-picked vendor ecosystem to bring the best cybersecurity technologies straight to our customers. Paired with our assessments, training, deployment and tuning, Trusted Engineer services, and consulting/vCISO services, Cadre enriches every technology selected. Through our partnership, we enable you to increase the return on every security investment to propel your business forward.

For more information, visit Cadre.net


Training
Engineering Consultants
Trusted Advisors
Rapid Diagnostic and Resolution
Quarterly Configuration Health Checks
Security and Compliance Planning
Security and Network Architecture Design
Policy Configuration Development & Review
Solution Implementation & Tuning
Penetration Testing
Cybersecurity Assessments
Leading Vendor Security Partners
Product Customizations
TECHNOLOGY
PEOPLE
PROCESS
Cadre
information security

PNC Center, 201 E. Fifth Street
Suite 1800
Cincinnati, OH 45202

888.TO.CADRE
WWW.CADRE.NET