



WE GET COMPREHENSIVE CYBERSECURITY.

For a multilayered cybersecurity solution that protects your organization from current and future threats, you need IT Orchestration by CDW®.





Elevating Cybersecurity to Protect Your Legacy

Today's workforces are more remote than ever, yet they still require fast, easy digital connectivity to support unwavering productivity. But more employee locations mean more opportunities for hacks and breaches to occur – from cybercriminals leveraging software, hardware and end-user devices to wreak havoc on your network, to unintentional employee errors can that lead to compromised data.

At CDW, we offer solutions and support to shore up cybersecurity on all fronts. We can advise you on your security posture, assess your environment, design the best approach, deploy your solution and manage it throughout its lifecycle. The result is a comprehensive cybersecurity platform that supports the future of work and how organizations will operate, while also enabling growth and innovation.

Our Comprehensive Expertise

Whether you're looking to tweak your existing cybersecurity posture or perform an enterprisewide overhaul of your entire platform, we can help you achieve your cybersecurity goals. Our experts have in-depth expertise to enable companies of all sizes, across all industries. We can help any organization achieve a comprehensive cybersecurity solution by leveraging hardware, software and services to encompass:



Advisory Services



Information Security



Network Security



Cloud Security



Emerging Cybersecurity Technologies

A History of Cybersecurity

We've been addressing cybersecurity since 1998, so we understand the mindset of a cybercriminal. We work with every customer individually to take a holistic approach to enterprise security so you can get the most out of your IT investment. Our security services are predominantly performed by in-house security professionals, well versed in multiple technical disciplines, who hold numerous security and partner certifications.

Partnerships

As a top partner for the industry's leading security vendors, we're able to offer an array of products and solutions to meet your unique security needs. We leverage our industry expertise to help you evaluate your options and discern which vendor technologies are ideal for your cybersecurity environment.

Security Certifications

CDW has mastered key private and public coursework in the latest security advances, including:



GIAC/GCIH
Certified



GSEC
Certified



CISSP
Certified



CEH
Certified



Certified in Risk
and Information
Systems Control
(CRISC)



Cisco Certified
Internetwork
Expert – Security

Partner Certifications



Cisco Master
Security
Specialized



Palo Alto Networks
Diamond Certification
Level and Authorized
Services



Design with Cybersecurity in Mind: An End-to-End Security Approach

Achieving a multifaceted cybersecurity solution means fortifying security controls across gateways and networks, servers, clients and applications. It also means being prepared to battle lurking intruders and instantly react in the event of a breach or attack.

Our cybersecurity experts are ready to advise you on the best approach, assess your environment, help you successfully implement the right solution and help you extend that success post-adoption. It's this end-to-end approach to cybersecurity that best protects your IT infrastructure from both current and future threats.



Advisory

Our advisory services are easily packaged workshops to help a customer just starting their new initiative.



Assessment

Using tools, data and years of expertise, we can make specific recommendations.



Implementation

Our expert engineering teams implement the right technology and ensure it works the first time.



Adoption

We help you get the best results from your solution and fully realize the expected value.



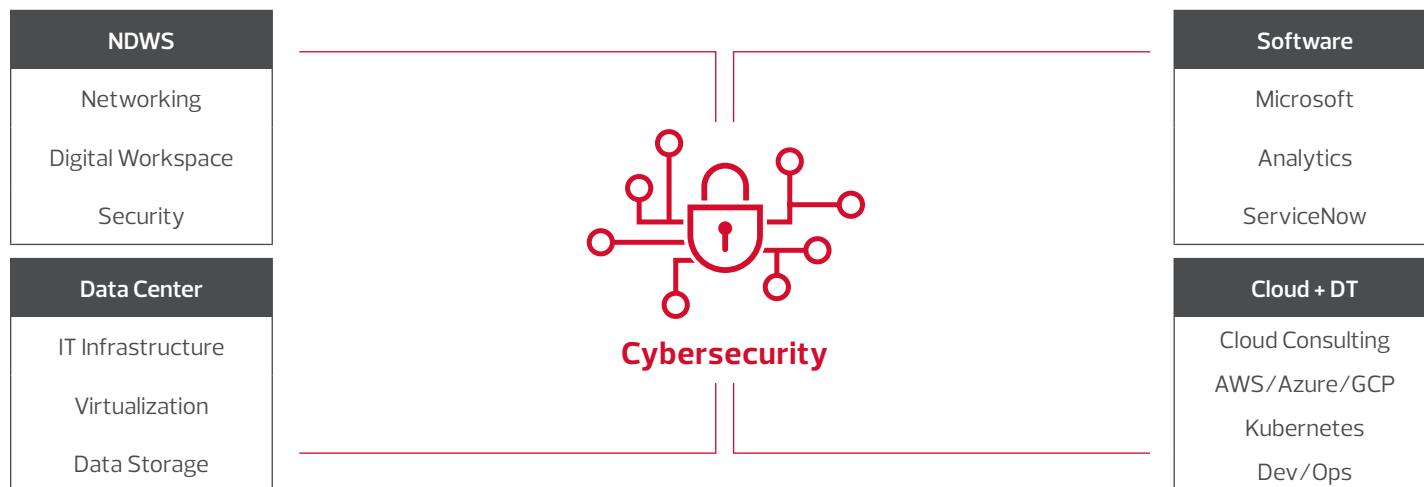


Design with Cybersecurity in Mind: Integrated Cybersecurity

Cybersecurity isn't a stand-alone proposition. It's integrated into every facet of your organization, from networking to collaboration, software to cloud, mobility to data center and more. It requires a holistic approach to solution design coupled with in-depth knowledge of how all these technologies work in concert to support business operations despite their unique vulnerabilities that require specific security tools and protections. CDW provides the integrated cybersecurity planning you need to ensure comprehensive security protocols are in place for every technology and solution within your organization.

Cybersecurity Integrated Anywhere

Digital transformation + cloud journey



We manage risk and protect the information of your enterprise and workforce no matter where IT resides



Advisory Services

CDW offers advisory services that help assess your cybersecurity environment, determine the best strategy for moving forward and bolster your organization's incident response capabilities.



Security Remediation Workshop

Receive help prioritizing the findings of an assessment, audit or penetration test performed by CDW experts. Learn the best tools and processes for improving your organization's cybersecurity posture.



Incident Response

Respond to a breach and identify the scope of an incident with triage, incident handling and investigation performed by CDW engineers, and system forensics completed by CDW's partners.



Security Architecture Workshop

Whether you are developing a network segmentation or IoT cybersecurity strategy, CDW can evaluate your business goals and your technology landscape to develop the strategy that is right for your organization.



Security Maturity Assessment

CDW will provide a technology-neutral Security Consultant to support your security strategy and planning, and facilitate efficient rollout and alignment of security products and services.



vCISO

CDW's vCISO service helps you improve the maturity and scope of your existing security practices by providing a technology-neutral Security Consultant. Using a three-step process, the Security Consultant advises you on your organization's security strategy and planning initiatives.



Compromise Assessment

CDW leverages consultants and tools to respond to an incident and look for signs of a breach, malware outbreak or other malicious activities that may indicate an undetected compromise.



Information Security

CDW offers cybersecurity-centric assessments and services based on decades of experience and a comprehensive set of risk management, policy and procedure, and advanced consulting capabilities:

Vulnerability Assessment

An automated, machine-generated exercise that delivers a set of reports specific to your organization's vulnerabilities, highlighting what needs to be done to eliminate identified vulnerabilities along with a list of action items to accomplish that task.

Penetration Testing

A paid professional consulting engagement with skilled security practitioners. Following testing, experts complete a report that places context and meaning around security findings to ensure risk mitigation is properly addressed – including a roadmap for architecture planning/remediation, a gap analysis of existing tools residing within your organization and, if need be, assistance in responding to a breach (identifying incident scope, triage plan and steps for handling the investigation process).

Application Security Assessment

Our experts review your organization's coding processes to evaluate the soundness of existing procedures and determine where best practices can be applied to your application development lifecycle in order to build a more agile infrastructure based on safer coding.

Policy and Procedure Framework

We offer framework-based models to help your organization adhere to an array of compliance standards – NIST, PIC, HIPAA, GDPR and more – and help you benchmark performance in terms of measuring security improvements over time.

Social Engineering

This includes the creation of scenarios used to test, measure and deliver reports, based on phishing exercises performed by CDW experts to identify phishing threats. We then help you understand if policies or procedures exist that enable users to help identify phishing threats and notify proper responders within the information security practice. If they don't exist, we help you develop those procedures.

Red/Purple Team Exercises

In the event of an incident – ransomware, cryptomining, an APT attack, an insider threat, etc. – our expert team walks through the exercise of training and educating your organization and helping to prepare a customized assessment that deliberately targets specific systems or specific core assets/data elements important to revenue generation. We help you understand the extent to which systems are vulnerable and how triage, chain of command and proper procedures are critical to a comprehensive response (this includes IT, C-suite, communications, HR, legal, PR and more).





Success Spotlight

CDW can help any organizations overcome an array of cybersecurity issues.

An organization recently engaged CDW to test existing security controls and validate its security posture to ensure compliance regulations were being met. Their goal was to confirm whether all resources were fully protected by multifactor authentication (MFA), while also measuring the effectiveness of their third-party monitoring service.

Over a one-week period, CDW conducted a Vulnerability Assessment and was able to gain access to the organization's network due to an overlooked service exposure and MFA misconfiguration. CDW was then able to compromise the Active Directory environment that controlled all systems without raising a single alert or notification from the organization's third-party monitoring solution provider.

These findings were detailed in a Vulnerability Assessment Report, along with actionable recommendations for improvement. CDW was sure to take specific measures to protect any information discovered through the assessments, as engineers work within a protected network and engagement reports are not accessible beyond the engineering team.

The assessment opened the organization's eyes to significant vulnerabilities within their environment, while CDW's guidance around infrastructure security improvements helped the organization address these cybersecurity gaps and improve compliance efforts.

Network Security

Network security doesn't happen in a vacuum. It's directly linked to the security of storage area networks, Wi-Fi, email and the web – all of which are dependent on access control and firewalls to block unwanted devices and traffic, as well as unauthorized users.

Next-Generation Firewall

Detects and blocks sophisticated attacks by enforcing security policies at the application level and by port and protocol. This enables strong threat detection for users and your network by arming your team with early warning and notification systems to help assist with quick investigations and forensic triage.

Endpoint Protection

This software runs on end-user devices to provide anti-malware, firewall, host-based intrusion prevention and other security-related services. In addition, our firewall and host-based intrusion protection services help guard against malware, illicit traffic and other threats on client devices and network infrastructures.

Email Security

Helps to control spam and keep phishing and malware from infecting your entire system. In addition, it helps to prevent disruptive leaks while providing the ability to sandbox suspicious items in a quickly evolving threat landscape.

Web Security

Protects employees from phishing attacks, watering holes and malvertisements. In addition, it helps limit employee application use to control data flow and access to proprietary information, while leveraging URL filtering, advanced threat defense, legacy malware protection and application control technologies to defend users from internet-borne threats.



Cloud Security

Cloud popularity has skyrocketed. Organizations across all industries are embracing cloud for its convenience, flexibility and agility. But like other technologies and solutions, the cloud brings with it security concerns.

The security challenges you face will depend on where your organization is within its cloud journey. CDW is here to help you manage your cloud security infrastructure, whether you're a first-time adopter or longtime user, and keep your data secure with the right solutions.



SASE

Secure Access Service Edge combines network security functions (e.g., SWG, CASB and Zero Trust), with SD-WAN capabilities to support the dynamic secure access needs of organizations.

CSPM

Fundamental to cloud security, cloud security posture management tools focus on security assessment and compliance monitoring and typically leverage API integrations with one or more cloud providers.

CWPP

Cloud workload protection platforms address unique requirements of server workload protection in modern hybrid data centers that span on-premises, physical and virtual machines, and multiple public cloud Infrastructure as a Service environments.

CASB

A cloud access security broker serves as a broker between your organization's network and its various cloud services, intercepting data traffic as it passes from the cloud using application programming interfaces (APIs) and enabling administrators to create policies that provide insight into, and enhance the security of, all cloud-based resources.

Cloud Check

CDW provides an opportunity for you to demo cloud security posture management tools from select vendors within your own cloud environment. We'll onboard the tool, which will examine your organization's security configuration and compare against security frameworks such as NIST or AWS to determine if gaps exist. The tool's output highlights where your environment could benefit from updates or upgrades.

Emerging Cybersecurity Technologies

CDW provides specialized cybersecurity capabilities geared to specifically address emerging technologies and their unique solution design and strategy requirements.

Zero Trust

Works under the assumption that a network is innately hostile, and users and devices must prove their identities to gain trust. Transitioning to a zero-trust approach (ZTA) involves a paradigm shift requiring effective information security and resilience practices. With a broad portfolio of partner solutions around device, user, session, application and data trust, CDW can help you through your entire ZTA journey.

IAM

Identity and access management provides the right people with the right access, verifies identity and ensures compliance with security policies to better protect the network from threats originating both outside and within your organization.

GRC

ServiceNow Governance, Risk and Compliance (GRC) is a suite of applications within the ServiceNow platform that provides timely, comprehensive, continuous information for auditing, reporting and compliance purposes. It helps transform inefficient processes across your extended enterprise into an integrated risk program and delivers a real-time view of compliance and risk to help improve decision-making and increase performance across your organization and with vendors.

GSOC/MDR/SOC as a Service

The Global Security Operations Center (GSOC) provides around-the-clock management of both internal and external threats to CDW's assets and operations to include vendors, partners and supply chain. Should a disruption occur that impacts you, in accordance with the Business Continuity Plan, the GSOC will be responsible for facilitating communication throughout the course of the event.





CDW Breadth of Partnerships

CDW is dedicated to all facets of cybersecurity for every organization – and that extends to having deep partnerships with industry-leading security software and hardware providers to ensure that customers have access to a wide array of solution components to meet their unique needs.

Next-Generation Firewall

Check Point®
Cisco®
Fortinet®
Palo Alto Networks®
SonicWall®

Endpoint Security

Cisco
CrowdStrike®
FireEye®
McAfee®
Microsoft
Palo Alto Networks
Sophos®
Trend Micro™
VMware® Carbon Black®

Email Security

Cisco
Microsoft
Mimecast®
Proofpoint®

Phishing Awareness

KnowBe4®
Cofense
Proofpoint

SASE

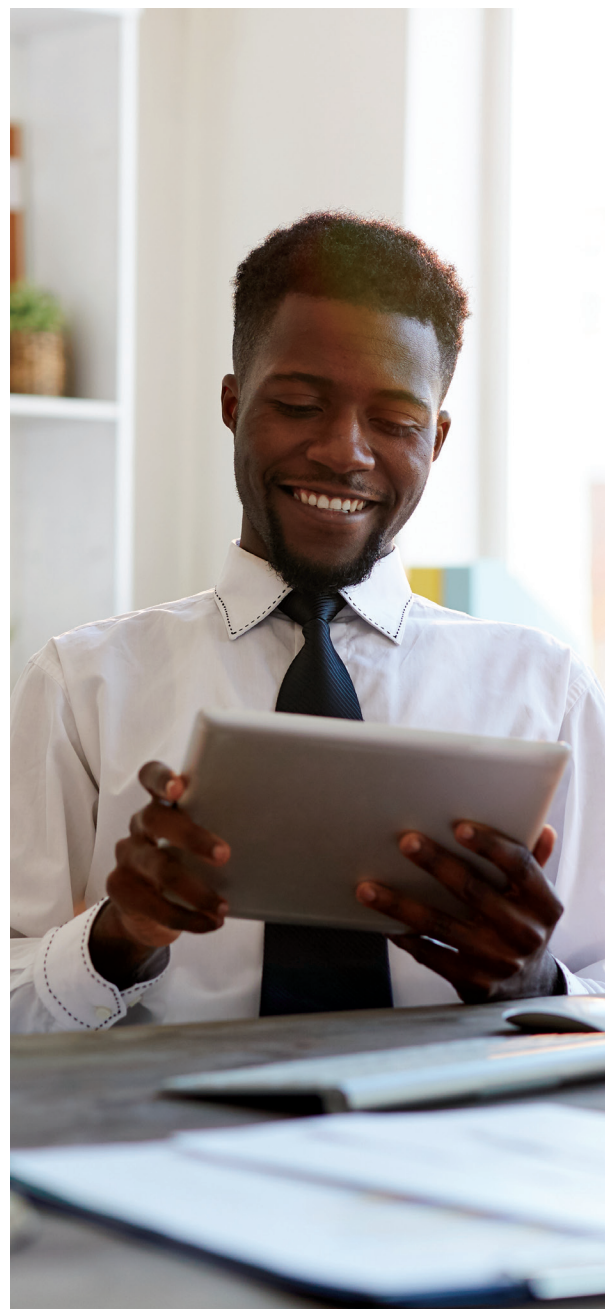
Barracuda®
Cisco
F5®
Fortinet®
McAfee
Microsoft
NetSkope®
Palo Alto Networks
Zscaler™

Analytics/SIEM

Cisco
ExtraHop®
IBM®
Splunk®

Identity

CyberArk
Okta
Thycotic





Whatever your cybersecurity goals, CDW is here to help you achieve them.

With more than 20 years of experience performing risk analysis, gap analysis and security assessments and testing for the country's largest Fortune 100 organizations, our team of 250+ solution architects and dedicated engineers is ready to provide a customized set of cybersecurity assessments for any customer in any industry.

If you have any questions or are ready to begin transforming cybersecurity across your organization, contact your CDW account manager or visit [CDW.com/cybersecurity](https://www.cdw.com/cybersecurity) today.



[CDW.com/cybersecurity](https://www.cdw.com/cybersecurity) | 800.800.4239