Evolving threats and lack of visibility make it difficult for organizations to stay ahead of threats while maintaining industry compliance. CDW’s Amplified Security™ consultants design, orchestrate and manage a comprehensive security strategy with a portfolio of services that identify and assess IT network security risks, increase your understanding of and visibility into risks, and prepare your organization for an evolving threat landscape.

**CDW Amplified™ Secure Platform**
- Next-Generation Firewall and IPS
- Content Security
- Identity and Access Management
- Policy and Access

**CDW Amplified™ Secure Edge**
- Network Visibility and Endpoint Protection

**CDW Amplified™ Detect and Respond**
- Log Aggregation and Correlation
- Security Incident Response Services

**CDW Amplified™ Information Security**
- Information Security
An increasingly mobile workforce is accessing your network with personal devices. Your organization's data is flowing to and from the cloud with increasing speed. The Internet of Things is connecting more devices to the web than ever before. Each of these advances has made network security more complex and even more critical to your organization. A robust network defense strategy lets you understand which people and devices are accessing your network — and what they're doing when they get there. We understand that the internal demands are lofty and that the stakes couldn’t be higher. We have the partner relationships and experience to consult, design and implement the right security infrastructure to meet your unique needs — before, during and after an attack.

Solution Benefits
Your organization can achieve the following by employing a CDW Next-Generation Firewall and IPS solution:

• Make sure only people you want to have access to your network are permitted to do so.
• Protect users and secure the traffic that is coming into and out of your network.
• Protect valuable assets inside your data center.
• Ensure users are not visiting dangerous websites that could result in your environment being exposed to malware.
• Prevent users from visiting workplace-inappropriate websites.
• Keep rogue devices off of your network.

Vendors Supported
• Cisco
• Palo Alto Networks

CDW can deliver additional Cybersecurity solutions by utilizing its vast network of trusted third-party partner service providers.

Services
CDW’s Next-Generation Firewall and IPS services fall into one of three lifecycle phases — Design, Orchestrate and Manage.

Design
Advisory/Assessment

• Cisco Firepower Threat Defense Planning and Design: CDW will evaluate whether your organization’s current Firepower Threat Defense deployment meets your requirements. We will provide a findings report, assist in Next-Generation application firewall rule creation, remediation and make upgrades as requested.

• Cisco ASA with Firepower Planning and Design: CDW can evaluate business and technical requirements and custom design a solution for your organization.

• Cisco ASA with Firepower Health Check: CDW will evaluate whether your organization’s current ASA with Firepower deployment meets your requirements. We will provide a findings report, assist in Next-Generation application firewall rule creation, remediation and make upgrades as requested.

• Palo Alto Networks Planning and Design: CDW can evaluate business and technical requirements and custom design a solution for your organization.

• Palo Alto Networks Health Check: CDW will evaluate whether your organization’s current Palo Alto deployment meets your requirements. We will provide a findings report, assist in Next-Generation application firewall rule creation, remediation and make upgrades as requested.

Orchestrate
Implementation/Adoption

• Cisco Firepower Threat Defense Implementation: After a solution for your organization has been designed, we will plan the deployment and then help you implement the Cisco Firepower Threat Defense solution.

• Cisco ASA with Firepower Implementation: After a solution for your organization has been designed, we will plan the deployment and then help you implement the Cisco ASA with Firepower solution.
• **Palo Alto Networks Implementation:** After a solution for your organization has been designed, we will plan the deployment and then help you implement the Palo Alto solution.

• **Palo Alto Networks Prisma Access Jumpstart:** Accelerate timelines and maximize results for your Palo Alto Networks Prisma Access solution with this cost-effective approach providing a pre-packaged experience.

• **Palo Alto Networks Prisma Access Custom Implementation:** After CDW helps you design your solution, we plan the deployment and then help you implement the Palo Alto Networks Prisma Access solution.

• **Configuration Services:** Technology products don’t come off the assembly line ready to work for you. They must be custom-configured to meet your organization’s unique needs and specifications. That’s not as easy as it sounds. It takes time and expertise that your IT team might not have. CDW has a wealth of experience in satisfying customers’ needs for Network and Security Device Configuration, Rack Configuration, Asset Management Services.

### Next Steps

An in-depth discussion with CDW can provide you with more insight into the importance of this work and help determine how much effort will be required. Contact your CDW account manager to speak with one of our security solution architects.

### Manage

Security Infrastructure and Information Security solutions require constant attention to reduce risks associated with vulnerabilities. CDW can help your IT team stay vigilant and focused by taking on the responsibilities for tasks associated with monitoring, upgrades, maintenance, and reporting and management for your Cisco and Palo Alto Networks security infrastructure.
As essential as email and internet access are for today’s businesses, hackers view them as a door into organizations’ networks and sensitive information. Spam filters have gotten better at stopping unsolicited and undesirable emails, but the variety and ingenuity of attacks is growing — and basic products have given many customers a false sense of safety. As for the web, employees can unwittingly put your organization at risk by clicking where they shouldn’t. CDW can help design a solution to minimize threats from damaging your organization.

Solution Benefits
Your organization can achieve the following by employing a CDW Content Security solution:

- Cloud architecture that boasts 99.999 percent uptime.
- Combine traditional URL filtering, reputation filtering, malware filtering and data security on a single platform.
- Global email threat intelligence, with spam blocking, malware protection, outbreak filters, data loss prevention, forged email detection and more.

Vendors Supported
- Cisco

Services
CDW’s Content Security services fall into one of three lifecycle phases — Design, Orchestrate and Manage.

Design
Advisory/Assessment
- Cisco Web Security Appliance (WSA) Planning and Design: CDW can evaluate business and technical requirements to help secure users’ connectivity to the internet and custom design a solution for your organization.
- Cisco Web Security Appliance (WSA) Health Check: We can evaluate whether your organization’s current Web Security Appliance deployment meets your requirements, provide a findings report and assist you with any design or configuration changes that are needed.
- Cisco Email Security Appliance (ESA) Planning and Design: CDW can evaluate your email security requirements and design a solution for your organization.
- Cisco Email Security Appliance (ESA) Health Check: We can evaluate whether your organization’s Email Security Appliance deployment meets your requirements, provide a findings report and assist you with any design or configuration changes that are needed.
- Cisco Umbrella Planning and Design: Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet. Umbrella is delivered from the cloud, making it simple to protect all of your users rapidly. CDW can evaluate your current business requirements and help design a solution that ensures you are protecting users both inside the network and on the go.
- Cisco Umbrella Health Check: We can evaluate whether your organization’s current Umbrella deployment is optimally configured to meet your security needs, provide a findings report and assist you with any design or configuration changes that are needed.

Orchestrate
Implementation/Adoption
- Cisco Web Security Appliance (WSA) Implementation: After designing a solution to help secure users’ connectivity to the internet, we will plan the deployment and then help you implement the solution.
- Cisco Email Security Appliance (ESA) Implementation: After designing a solution for your organization, we will plan the deployment and then help you implement the solution.
- Cisco Umbrella Implementation: Cisco Umbrella is a cloud security platform that provides the first line
of defense against threats on the internet. Umbrella is delivered from the cloud, making it simple to protect all of your users rapidly. CDW can implement a solution that ensures you are protecting users both inside the network and on the go.

**Manage**

- **Managed Services for Cisco Umbrella:** CDW Managed Services’ Enterprise Command Center and security engineers work together to help you block requests to malicious and unwanted destinations and provide visibility into the threats your organization is experiencing by taking responsibility for monitoring Umbrella functionality, implementing policy configuration changes, providing reporting and many, many more day-to-day tasks.

**Next Steps**

An in-depth discussion with CDW can provide you with more insight into the importance of this work and help determine how much effort will be required. Contact your CDW account manager to speak with one of our security solution architects.

800.800.4239 | CDW.com/cdwservices
Employees in your enterprise are working with dozens of applications and juggling multiple mobile devices. Switching from one app to another, and from one device to another, doesn’t change the user’s identity. Without the right tools to authenticate the identity of the user, though, things can get pretty messy and result in reduced productivity.

Life is complicated. Your workplace — with new technology, hardware and software coming online at a fever pitch — can be equally as complicated.

But it doesn’t have to be.

With the right Identity and Access Management solution, controlling information about users in your environment and determining who has access to what can be simplified. CDW has the experience and resources to deliver the right solution for your business.

Solution Benefits
Your organization can achieve the following by employing a CDW Identity and Access Management solution:

- Centralize network access policy management to provide consistent and secure access to your users, no matter how they connect to your network.
- Reduce management and support burdens by centralizing and unifying device administration, authentication and user access policy.
- Simplify guest experience for easier onboarding and administration.
- Control who and what is on your network.
- Design a solution so that resources are only granted to those users who are entitled to them.
- Provide adaptive single sign-on to identity-federated devices.

Vendors Supported
- Microsoft

CDW can deliver additional Cybersecurity solutions by utilizing its vast network of trusted third-party partner service providers.

Services
CDW’s Identity and Access Management services fall into one of three lifecycle phases — Design, Orchestrate and Manage.

Design
Advisory/Assessment

- Microsoft Azure Sentinel Workshop: CDW helps you experience Microsoft Azure Sentinel within your own environment, get a bird’s-eye view across all data ingested, and detect threats using Microsoft’s analytics and threat intelligence. In addition, product and solution best practices configuration provides evidence-based insight to ensure security governance and compliance is applied to your multicloud solution.

- Microsoft 365 Security Assessment: The Microsoft 365 suite contains numerous products and features designed to keep applications, data and users secure, while providing advanced notification of security threats from many sources. Security is at the forefront of every organization’s concerns and poses a real threat to their business. Maximize the benefits of Microsoft 365 by performing a Security Assessment of your current environment to determine where there are gaps and how Microsoft 365 can help address the risks. We can help you understand some of the features you may have overlooked and educate you on the benefits of Microsoft 365 E3 or E5 Enterprise.

- Microsoft Active Directory Domain Services Planning and Design: CDW will provide you with an Active Directory architecture design and an administrative model design. We can also handle consolidation and migration.

- Microsoft Active Directory Domain Services Health Check: CDW will investigate your domain controllers, check logs, check networking, look for gaps in security and best practices deployment, and provide detailed remediation recommendations.

- Microsoft Public Key Infrastructure (PKI) Health Check: This engagement is a systemic and rigorous evaluation of an existing PKI implementation. Auxiliary environments that have a dependency on the health of the PKI are also examined for functionality and configuration. The Health Check
CDW Amplified™ Secure Platform
Identity and Access Management (continued)

will include an architecture review and system and gap analysis. A Findings and Recommendation Report will be presented to you upon completion of the project.

- **Azure Advanced Identity and Authentication Workshop:** This workshop service offering formulates a complex identity and authentication architecture for your organization after you’ve decided to move to the cloud. The cloud decision has an impact on how your environment is set up and early decisions are necessary, as the cloud identity will become the foundation for cloud transition efforts. This three-day engagement will help you understand complex environments and requirements and sort through all the available services, products and configuration options, resulting in the development of a high-level cloud identity and access architecture that meets your requirements. Among the items typically discussed during the workshop are: Azure AD Connect, Active Directory Federation Services, Microsoft Identity Manager, Azure Active Directory, Active Directory Federation Services, Microsoft Exchange/O365, Active Directory, Active Directory Lightweight Directory Services, migration tools and user experience and client behaviors.

- **Microsoft 365 Security Information Protection:** Information is one of your most valuable assets and can easily be shared, even outside the organization. Protecting and managing access to this information is vital to your organization to retain the trust and confidence of your customers. Microsoft 365 has a variety of tools to help protect and manage this information. The Information Protection engagement will provide the best practices on how to configure the products to achieve your goals. This will provide a functional roadmap to ensure security and compliance is built into the Office 365, Windows 10 and EMS solution. Some of the products and tools covered in Information Protection include: Current Security Controls, Azure Sentinel, Cloud App Security, Azure Information Protection, Data Loss Prevention, Information Security and Email Security.

- **Microsoft 365 CISO Security Workshop:** This engagement focuses on learning your organization’s unique needs and develops a strategic plan based on approaches recommended by Microsoft experts. The workshop will cover both product and solution best practices configuration recommendations around the security features of Microsoft 365. This will provide a functional roadmap to ensure security and compliance is built into the Office 365, Windows 10 and EMS solution. This will benefit both highly regulated organizations and those who have concerns about increasing their information security posture.

- **Microsoft 365 SaaS Security Workshop:** This engagement will help customers evaluate their current business security threat landscape...
as well as their existing Office 365 security controls to create an evidence-based roadmap to meet organizational needs. Additionally, this workshop will pilot advanced features and controls which allows customers the ability to mitigate numerous attack vectors that are prevalent today. Office 365 is fantastic technology that enables productivity, but too often it has set security to a one-size-fits-all format which, in today’s fast-moving environment, can leave areas exposed. The workshop also will cover both product as well as the solution’s configuration best practices and associated recommendations. This will provide an evidence-based roadmap to ensure security, governance and compliance is uplifted into your Office 365 solution. This will benefit both highly regulated organizations and those who have concerns about increasing their cybersecurity posture beyond the default.

- **Microsoft 365 Security Device Protection:** As more and more users become mobile and are using a wider variety of devices, applications and documents need to keep up. How do you manage these devices while providing secure and reliable access to applications and data? Microsoft 365 helps provide easy, secure access to any device, no matter where someone might be. Device Protection will include the steps necessary to understand your requirements and develop the deployment plan just for you. There are many possible options which can include a variety of tools and techniques. Some of the products and tools covered in Identity Protection include: Current Security Controls, Azure Sentinel, Cloud App Security, Azure Active Directory Premium, Azure Advanced Threat Protection, Azure Active Directory Identity Protection, and Identity Governance.

### Orchestrate Implementation/Adoption

- **Microsoft Active Directory Federation Services:** CDW offers a variety of AD Federation Services, including Mini Design (an abbreviated design session for deployments in the simplest scenarios), Planning and Design (a complete discussion and design session covering all AD FS topics), Build (deploy two internal AD FS servers and two AD FS proxy servers, either on–premises or in Azure), and Configuration of trusts and claims transformation rules.

- **Microsoft Public Key Infrastructure (PKI) Services:** The Microsoft PKI Services include modules to assist in the design and deployment of Certificate Services to resolve a number of issues, representing work ranking from design to deployment, enabling a number of key technologies.

- **Windows Server DirectAccess:** This engagement will provide you with a clear vision and high-level DirectAccess architecture. CDW can assist with either a pilot or production deployment of the architecture determined during the design portion of the project.

- **Microsoft Identity Manager (MIM) Pilot:** This engagement provides you with a pilot production deployment of MIM based on the recommended design. CDW can assist with configuring additional identity workloads as needed and will work with you to determine the full scope of the engagement.

### Manage

- **Azure Identity Management:** Integrating your on–premises directories with Azure Active Directory will provide a common identity for access to both cloud and on–premises resources, simplifying things for your end users. CDW Managed Services can help by providing an integration and synchronization service between your on–premise Active Directory and Azure Active Directory using the AD Connect tool. This will allow your IT team to focus on more strategic initiatives because we are taking on the responsibility of monitoring, troubleshooting and dealing with the hassles associated with managing integration and synchronization of your Active Directory environments in Azure. On–premise Active Directory and/or Active Directory Federation Services management are separate service offerings and not included.
In today’s threat-heavy environment, the enterprises that have strong risk management policies in place are the most likely to emerge from a security breach incident in the best shape.

Is there a better way to mitigate risk than by knowing who is on your network, and what each end user is doing while connected?

Every organization is now faced with employees utilizing multiple devices. Companies also need to share their network with third-party partners and contractors, not to mention guests visiting your offices. A policy and access solution designed by CDW can help secure your network against malicious activity and insider threats.

**Solution Benefits**
Your organization can achieve the following by employing a CDW Policy and Access solution:

- Bolster the security of your network by ensuring all end users comply with your defined security policy.
- Identify users and devices on your network.
- Restrict the data that each end user may access.
- Regulate what end users may do while connected to your network.
- Take network action on compromised or non-compliant end users.
- Verify log-on information.

**Vendors Supported**
- Cisco
CDW can deliver additional Cybersecurity solutions by utilizing its vast network of trusted third-party partner service providers.

**Services**
CDW’s Policy and Access services fall into one of three lifecycle phases — Design, Orchestrate and Manage.

**Design**

- **Advisory/Assessment**
  - Cisco Identity Services Engine (ISE) Planning and Design: CDW can evaluate business and technical requirements and design a solution for your organization.
  - Cisco Identity Services Engine (ISE) Health Check: CDW will evaluate whether your organization’s current ISE deployment meets your requirements. We will provide a gap analysis report, assist in remediation and make upgrades as requested.
  - Cisco Duo MFA Planning and Design: CDW can evaluate business and technical requirements and design a solution for your organization.
  - Virtual Private Network (VPN) Planning and Design: CDW can evaluate business and technical requirements and custom design a solution for your organization’s remote access and branch needs.

**Orchestrate**

- **Implementation/Adoption**
  - Cisco Identity Services Engine (ISE) Implementation: After a solution has been designed for your organization, we will plan the deployment and then help you implement it.
  - Cisco Duo MFA Implementation: After a solution for your organization has been designed, we will plan the deployment and then help you implement the Cisco Duo’s MFA for your Cisco or Palo Alto VPN solution.
  - Virtual Private Network (VPN) Implementation: After the solution for your organization’s remote access and branch needs has been designed, we will plan the deployment and then help you implement it.

**Manage**

- **Managed Services for Cisco Identity Services Engine (ISE)**: CDW Managed Services’ Enterprise Command Center and security engineers work together to address critical authentication issues, certificate renewals, policy set configuration changes and security patch availability, in addition to performing many, many other ISE-related responsibilities.

**Next Steps**
An in-depth discussion with CDW can provide you with more insight into the importance of this work and help determine how much effort will be required. Contact your CDW account manager to speak with one of our security solution architects.
Go beyond traditional chokepoint and perimeter threat detection by utilizing the intelligence of the network and information that is available on the endpoints. Take advantage of the power of NetFlow and get advanced visibility, analytics and protection. You can see everything happening across your network and data center. Cisco Stealthwatch alone can uncover attacks that bypass the perimeter and infiltrate your internal environment, but when you combine it with an advanced next-generation endpoint security client you get increased visibility and protection for your systems — both inside your network and for those users who are on the go.

Solution Benefits
Your organization can achieve the following by employing a CDW Network Visibility and Endpoint Protection solution:

- Insight into attacks and malicious activity going on inside your network that many other solutions would never make visible.
- Embed security anomaly detection into the network element, using machine learning for incident response and device-level mitigation.
- Rapidly detect, contain and remediate advanced threats if they evade frontline defenses and get inside.
- Deep visibility into executable and file activity across all of your endpoints so you can spot threats fast, scope a compromise and remediate instantly to help with all those zero-day attacks.
- Continuous monitoring and recording of network and host activity for all hosts inside and out of your network.

Vendors Supported
- Cisco
- Carbon Black

Services
CDW’s Network Visibility and Endpoint Protection services fall into one of three lifecycle phases — Design, Orchestrate and Manage.

Design
Advisory/Assessment

- Cisco Advanced Malware Protection:
  - FireAMP Endpoint Planning and Design: CDW can evaluate business and technical requirements and help you plan and design a FireAMP endpoint security solution.
  - FireAMP Endpoint Health Check: CDW will evaluate whether your organization’s current FireAMP deployment meets your requirements and is providing the best protection available. We will provide a findings and recommendation report and can assist with any remediation and recommendations found.
- Cisco Stealthwatch Health Check: CDW will evaluate whether your organization’s current Stealthwatch deployment meets your requirements and make sure you are getting the visibility you expect. We will provide a findings and recommendation report and can assist with any remediation and recommendations found.
- Carbon Black Defense: CDW’s Carbon Black Defense (CbD) services will help organizations get the most out of their investment while creating a protected environment using this best-of-breed NGAV and Endpoint Detection and Response (EDR) solution.
  - Carbon Black Defense Services: CDW’s Carbon Black Defense (CbD) services will help organizations get the most out of their investment while creating a protected environment using this best-of-breed NGAV and Endpoint Detection and Response (EDR) solution.
  - Discovery and Design Session: CDW will demonstrate CbD’s use and functionality in real-work attack scenarios and walk throughs. This will help drive a thorough understanding of the solution’s features and capabilities.
- CDW Cloud Check: Adopting new cloud services can accelerate digital transformation across industries, but rapid cloud adoption can also expose organizations to unnecessary risk. Thankfully, cloud security posture management (CSPM) tools give IT professionals the deep visibility they need to recognize and correct security vulnerabilities and potential regulatory issues as they
CDW Amplified™ Secure Edge
Network Visibility and Endpoint Protection (continued)

arise. After setting you up with a complimentary trial license of your chosen CSPM solution, our CDW Cloud Check engineers will draw upon experience from thousands of security engagements to help you determine whether the tool fits your organization’s unique needs. Their detailed guidance can speed up the decision-making process to jump-start your risk-mitigation efforts.

Orchestrate
Implementation/Adoption

- **Cisco Advanced Malware Protection:**
  - **FireAMP Endpoint Implementation:** After your solution has been designed, CDW can help you quickly deploy and enable FireAMP endpoint’s security features.

- **Cisco Stealthwatch Services:** CDW can provide options when deploying Stealthwatch. We can assist with either getting it up and running quickly and help alleviate problems, or offer design and deployment services for a complete enterprise rollout.

- **Carbon Black Defense:**
  - **Implementation:** CDW will blend technological expertise and personalization to create an optimized security solution that can be deployed everywhere without impacting business-critical applications.

  **Extended Deployment Support:** CDW will help drive the complete adoption and optimization of the solution throughout your environment.

  **Threat Hunting:** CDW will leverage industry-recognized frameworks to conduct Threat Hunting to detect instances of unauthorized access, adversarial movement, advanced persistent threats (APTs), and Command and Control (CnC) activity.

Next Steps

An in-depth discussion with CDW can provide you with more insight into the importance of this work and help determine how much effort will be required. Contact your CDW account manager to speak with one of our security solution architects.
In today’s IT landscape, organizations large and small are overwhelmed by the amount of logs, alerts and notifications from security technology. How do you begin to sort through it all? By employing a Splunk and CDW Managed Security Information and Event Management (SIEM) solution. Splunk is a powerful tool that can assist in correlating and sorting data from a variety of systems and security devices and has full SIEM capabilities. This powerful tool can be quite complicated and overwhelming to manage. CDW can assist in harnessing the full security features of Splunk by implementing a new environment or optimizing a current deployment.

CDW’s Splunk Security Services team provides assurance that your organization is ready to fully adopt Splunk to gain deep security visibility in your environment. Additionally, CDW can manage your network security policies and troubleshoot issues with your security infrastructure around the clock. Our experts triage security alerts, notify you immediately of an attack, and take action to block further attacks.

Solution Benefits
Your organization receives many benefits by utilizing CDW Log Aggregation and Correlation Services:

- The knowledge and capabilities of an elite-level Splunk partner with Accredited Core Implementation certified engineers.
- Expertise with security and Splunk in large environments.
- Optimization of your Splunk environment to maximize value received from licensing.
- Hands-on knowledge transfer of your Splunk implementation to optimize your operational efficiency.
- Real-time incident response, log collection and correlation, and reporting.

Vendors Supported
- Splunk
- CDW

When You Need More Than Logs
While a syslog server is tried and true technology, gaining executable intelligence from it in near real time is almost impossible. Splunk can bridge the gap to help your organization respond to security threats and indications of compromise.

Services
CDW’s Log Aggregation and Correlation services fall into one of three lifecycle phases — Design, Orchestrate and Manage.

Orchestrate Implementation/Adoption

- **Splunk Installation Services**: Are you implementing a new Splunk environment or expanding your existing Splunk Security infrastructure? CDW Splunk experts can help you bring your Splunk security strategy to reality.

- **Splunk Security Product Add-On**: Are you engaging CDW for a security product installation? Check out our Splunk Security add-on service where CDW implements a Splunk instance with the tools to help you gain full visibility into your firewall and security logs with the power of Splunk.

- **CDW Incident Response Services**: With next-generation firewalls, endpoint protection, IDS/IPS, DNS security, machine learning and other technologies, it would be nice if we could say our networks will never be breached. The reality is security incidents are inevitable, for all organizations of all sizes. The ability to respond effectively to limit the impact of such events is critical for every business, school, government agency and institution. CDW Incident Response Services are available to enable you to respond and adapt to incidents before they become disasters.

Manage

- **CDW Managed SIEM**: As an extension of your IT department, CDW provides trained experts and a cloud-based Security Information and Event Management (SIEM) solution to deliver real-time incident response, log collection and correlation, and reporting. In addition to helping you keep up with your logging compliance requirements, our experts notify you immediately of an attack, and quickly take action to block further attacks.
With next-generation firewalls, endpoint protection, IDS/IPS, DNS security, machine learning and other technologies, it would be nice if we could say our networks will never be breached. The reality is security incidents are inevitable, for all organizations of all sizes. The ability to respond effectively to limit the impact of such events is critical for every business, school, government agency and institution.

CDW Incident Response Services are available to enable you to respond and adapt to incidents before they become disasters.

### Solution Benefits
Your Security Incident Response (IR) Services enable an organization to be ready to respond to credential theft, malware outbreaks, security breach and other potential security incidents.

### Services

<table>
<thead>
<tr>
<th>Design Advisory/Assessment</th>
</tr>
</thead>
</table>

#### Incident Response Services
When you decide to add CDW’s Retainer-Based Security IR Services to your cybersecurity plan, that paperwork is handled up front, meaning there’s no downtime between discovery and action.

- **Premium and Essential IR:** Depending on your service level, our prepaid one-year agreements are good for up to 120 hours of service, and up to 40 hours of event preparedness services. Event Preparedness Services included may consist of: IR Readiness Assessment, IR Program Development (Policy, Plan & Playbook Development, IR Tablettop Exercise or IR First Responder Training). This service also allows you to reallocate a portion of unused services fees to additional security advisory and assessment services at the end of your contract.

- **Basic IR:** We understand that a prepaid option is not right for everyone. Our Basic IR Service provides you with access to CDW’s IR team, should you need it. This service gives you up to 80 hours of IR services on a time and materials basis.

### Proactive and Preparedness Services
CDW also provides four complete proactive event preparedness security services to help your team be better prepared for the inevitable. We utilize the same skilled consultants and tools for these services that we leverage to respond to security incidents.

- **IR Readiness Assessment:** CDW will review your IR policy, plan & playbook, evaluate roles, responsibilities, processes and security tools along with performing a refresher training for IR Handlers and First Responders.

- **IR Program Development (Policy, Plan & Playbook):** CDW will coordinate and lead a one-day workshop assessing your existing IR policy, plan, playbook and incident notification requirements and then provide you with a complete IR policy, plan and playbook.

- **IR Planning and Tabletop Exercise Workshop:** CDW will perform an assessment including a review of policy, plan and playbooks, review of tools, roles and responsibilities. We will also provide First Responder refresher training, IR tabletop exercise, after action review, playbook updates and complete knowledge transfer.

- **Compromise Assessment:** CDW will help you understand if/when you have been compromised by providing focused threat hunting in your environment.

### Next Steps
An in-depth discussion with CDW can provide you with more insight into the importance of this work and help determine how much effort will be required. Contact your CDW account manager to speak with one of our security solution architects.
As technology and IT environments continue to evolve at a rapid pace, security risks evolve right alongside them. In today’s climate, you can’t afford to be caught off guard when a security breach occurs.

A third-party security risk assessment process is the best way to root out vulnerabilities in your infrastructure before any damage occurs. CDW’s security threat assessment experts are here to put your network to the test and develop a smart risk management plan tailored to your organization.

Our team of white-hat hackers has been performing security threat assessments since 1998. From small business security protocols to enterprise risk management, we customize each service using security tools developed by our expert engineers as well as industry-standard tools.

**Solution Benefits**

Your organization can achieve the following by employing a CDW Information Security solution:

- Critical insight into undetected issues that pose significant risks to enterprise security.
- Factual information on security threats will leave you better prepared to defend your enterprise.
- Armed with practical, action-oriented information, your IT department can take immediate action to remedy major security issues and reduce the risk of future compromises.
- Minimal demands on your IT department’s time.

**Services**

CDW’s Information Security services fall into one of three lifecycle phases — Design, Orchestrate and Manage.

**Design Advisory/Assessment**

**Technical Assessments**

CDW can assist your organization conduct third-party agnostic security assessments; whether technical or procedural in nature. The assessments always combine vulnerability scanning with manual penetration testing and a human-generated final report to give you the clearest picture of your security posture.

- **Comprehensive Security Assessment (CSA):** CDW provides a tailored approach to assessing your security posture, including external, internal and wireless networks, application security, and social engineering campaigns. In addition, the CSA provides technical security assessments for mature or advanced operations such as: Red Team and Purple Team Assessments; IoT Assessments; SCADA Assessments; Advanced Social Engineering, and Asset-Centric Assessments (PHI, PII, proprietary data, etc.).

- **Rapid Security Assessment (RSA):**
  This service provides a quick view into your security posture, including External, Internal, and Wireless networks and Phishing Campaigns.

- **Purple Teaming Services:** CDW Purple Teamers simulate real-world cybersecurity attacks in collaboration with your defensive team with the primary goal of testing and assessing your organization’s detection and response capabilities overall. This helps assess not only your Blue Team’s capabilities, but also your end-user response to phishing and vishing. You may also opt into targeted testing and assessments intended to further understand your security posture.

- **Red Teaming Services:** The best way to know if your defensive team is indeed prepared to protect your most critical assets is to run a realistic attack scenario within your organization. Over the course of several weeks, a CDW Red Teamer will simulate real-world covert cybersecurity attacks against your organization. You may also opt into targeted testing and assessments intended to further understand your security posture. After the exercise is complete, CDW will provide a written report and an interactive forum to walk through the exercise from start-to-finish and answer questions.

- **Work From Home (WFH) Security Assessment:** CDW assesses the security of custom developed or customized commercial applications through user interface and code review assessment.
CDW Amplified™ Information Security
Information Security (continued)

• **Application Security Assessment:** CDW security engineers can attempt to break into an application used by your organization, whether it be an off-the-shelf product or one developed by your team. We will then make recommendations for improving security.

  ![Application Security Assessment Image]

  **Security Consulting**

  • **vCISO:** CDW's Security Consultants are available to act as a virtual Chief Security Information Officer (vCISO) who helps you improve the maturity and scope of your existing security and advises you on your organization's security strategy and planning initiatives. In addition, the Security Consultant facilitates rollouts of security products solutions and services in alignment with your wider security, risk and compliance program. CDW offers three levels of engagement, depending on the needs of your organization.

  • **Framework Assessment:** CDW uses a standards-based approach based on the National Institute of Standards and Technology's (NIST) Special Publication 800-53 to security operational framework gap analysis. We will interview members of your organization and determine where improvements can be made.

  • **Security Maturity Assessment:** CDW conducts a two-day workshop with the goal of assisting you in developing a security plan and roadmap to improve your security posture and then providing implementation services to assist you with resolving high-priority items identified in the roadmap.

  • **Security Architecture Workshop:** Whether you are developing a segmentation or IoT security strategy, CDW can evaluate your business goals and your technology landscape to develop an architecture plan and roadmap that is right for your organization. We go beyond the typical considerations, such as focusing narrowly on your security goals, and provide a framework that considers business requirements, operational expectations, existing investments and applications.

  • **Security Remediation Workshop:** Using the results of an assessment, audit or penetration test, CDW will help you prioritize findings and provide guidance on how to fully utilize existing tools as well as suggestions for new tools and processes that can be implemented to improve security posture and reduce risk.

  • **Network Segmentation Workshop:** In a five-day workshop led by CDW Security Consultants, we focus on understanding your organization and its risk profile and establish a roadmap to successfully implement Network Segmentation in your environment.

**Custom Security Consulting Services**

• **Custom Security Enterprise License Agreement Advisor:** CDW will provide a security advisor to help facilitate the rollout and alignment of security products and to ensure that your organization is getting the most benefit out of your ELA.

• **Custom Solution Evaluation:** Whether you are implementing a new solution or upgrading an existing one, CDW can help you evaluate your current environment, deployed tools and business and security objectives to determine gaps and identify tools that might be required to fulfill objectives.

• **Custom Security Advisory Services:** CDW provides a technology-neutral Security Consultant to support your security strategy and planning. This engagement also facilitates efficient rollout and alignment of security products and services with your wider security, risk and compliance program.

**Next Steps**

An in-depth discussion with CDW can provide you with more insight into the importance of this work and help determine how much effort will be required. Contact your CDW account manager to speak with one of our security solution architects.