IMPROVE YOUR SECURITY POSTURE WITH THE LATEST TECHNOLOGIES.

EMBRACE ADVANCED IT TO UP YOUR PROTECTION ANTE

IT ORCHESTRATION BY CDW™

Visit CDWG.com/threatcheck
MANAGING MODERN SECURITY RISK

The rate and volume of cyberattacks will keep growing as hackers and cybercriminals become more advanced, using the latest technology to take advantage of increasingly mobile and cloud-dependent organizations. That's why it's imperative for these organizations to understand the significant risk they face on a daily basis.

The need for amped-up security measures is top of mind for organizations across all industries. Whether you’re a healthcare organization looking to protect patient data, an educational institution needing to shore up wireless security for online learning or a government agency pressed to safeguard classified information, if you’re not investing in the latest advancements in security technologies you’re leaving the door open to cyberattacks.

Considerations organizations across all industries should keep in mind when reviewing the state of their security:

- Do your current security measures sufficiently protect your institution’s most valuable assets?
- How easy is it for your IT staff to deploy new security protocols and manage network threats?
- Are your cloud and mobility platforms making it harder to protect data on every front?
- Do your security precautions help or hinder staffers when it comes to doing their jobs?
- How well can your workers access the data they need to do their jobs?
- When was the last time you tested and evaluated the effectiveness of your security platform?

It’s time to rethink how you approach the task of managing security and risk across your organization.

Source: kpmg.com, “Global CEO Outlook Infographic,” July 2017

50% of CEOs do not feel prepared for a cyberattack.¹
THE PRACTICALITY OF A PROACTIVE PROTECTION PROTOCOL

Staying a step ahead of today’s hackers and cybercriminals means keeping up with an ever-changing IT landscape and its newly emerging threats. Keeping current on the tools used to protect and defend your network is paramount, and there’s no better time to evaluate your current security measures to see if it’s time for a proactive protection upgrade.

Key Technologies to Consider

**Next-generation firewall.** Next-generation firewalls provide strong threat detection that protects users and the network. The latest firewalls are designed to help leverage the cloud, support virtual malware analysis and enable true IPS capabilities in a single architecture.

**Email security.** Email is the most popular attack method used by cybercriminals. Modern email security has evolved to provide more than just defenses against spam and viruses, enabling URL rewriting capabilities, sandboxing technologies and data loss prevention.

**Advanced endpoint protection.** Goes beyond traditional signature-based endpoint protection to provide more advanced protection against today’s threat landscape, and can include machine learning, behavior monitoring, threat analysis and automatic containment.

**Web security.** The internet is a cybercriminal’s playground. This tool helps mitigate the risks staff internet use can post by providing URL filtering, malware protection, advanced threat defenses and application control technologies.

**Identity and access management (IAM).** Organizations are increasingly challenged to maintain governance around identity and access, especially as workers are added, moved or promoted. IAM provides entity governance and administration, access including user authentication, single sign-on (SSO) and authorization enforcement, and identity log monitoring and reporting.


$7.7 Million
Cyber hacks and their consequences globally cost companies an average of $7.7 million.
PEOPLE WHO GET IT

Achieving a proactive security protocol to stop breaches and incidents before they occur requires comprehensive planning and insight into what systems and data are most vulnerable. At CDW·G, we’ll use our IT expertise and top technology partnerships to orchestrate a solution that helps you address and manage risk. In the process, you’ll benefit from:

Expert advice
Our extensive team of knowledgeable experts will work with you to understand your current needs and future goals, then help develop strategies to improve your infrastructure protection and, in turn, improve the experience of those you serve.

Comprehensive services
Our services help you focus on people instead of worrying about securing your IT infrastructure. We’ve been designing and implementing holistic security solutions for nearly 20 years, helping organizations achieve industry compliance and meet evolving security demands. In fact, CDW has partnered with Cisco and Tenable to offer CDW Threat Check. This complimentary service provides organizations with valuable insight into the state of cybersecurity defenses and includes:

- Passive network monitoring to analyze network traffic for potentially malicious activity and unpatched vulnerabilities
- Malware infection detection and botnet detection that inspects all traffic leaving and entering the network

Benefits from Working with CDW·G

- Help meeting a host of compliance regulations, including Payment Card Industry Data Security Standard (PCI DSS); Health Insurance Portability and Accountability Act (HIPPA); Federal Information Security Management Act (FISMA); Sarbanes-Oxley Act of 2002 (SOX); and the Gramm-Leach-Bliley Act (GLBA)
- Expertise that spans comprehensive security assessments, design and architecture of security solutions, as well as implementation and knowledge transfer to get the most out of your security solutions

Meet Our Partners

Our array of industry-leading vendor partnerships means you have, at your fingertips, the right technology to better secure your networks and infrastructure. Together, we’ll help you orchestrate a solution that improves data and network security across your organization.

Forcepoint™ safeguards users, data and networks against accidental or malicious insider threats to outside attacks, across the threat lifecycle.

The Juniper Networks® SRX1500 Services Gateway is a high-performance next-generation firewall and security services gateway that protects mission-critical enterprise networks.

Malwarebytes Endpoint Security eliminates zero-hour malware your anti-virus and firewall can miss, while protecting vulnerable programs against zero-day exploits.

Symantec™ Endpoint Protection provides outstanding protection, high performance and orchestrated response to stop threats regardless of how they attack your endpoint, so you can focus on your organization.

To learn more about CDW·G and how our solutions can help you combat security issues, call 800.808.4239. To sign up for your own CDW Threat Check, visit CDWG.com/threatcheck.