KEEPING A WATCHFUL EYE.

NEXT-GENERATION SECURITY: INTRUSION PREVENTION SYSTEMS

THE CHALLENGES | THE SOLUTION | THE BENEFITS

Security threats are changing before your very eyes, evolving in number, type and sophistication. CDW can help you refocus with an intrusion prevention system. It does more than block potential breaches. The system helps you to SPOT THE SIGNS OF AN EXISTING BREACH SOONER.
NOW YOU SEE IT. **NOW YOU DON’T.**

It can happen in the blink of an eye: Your sensitive data goes missing. Gone without a trace. It’s not hard to see how. Organizations must secure more entry points than ever before while dealing with an increasing number of intelligent attacks like advanced persistent threats (APTs). Without eyes in the back of their heads, IT managers may lose sight of security.

**93%**

OF LARGE ORGANIZATIONS EXPERIENCED A SECURITY BREACH IN 2013.¹

**66%**

OF BREACHES ARE DISCOVERED MORE THAN ONE MONTH AFTER THEY OCCUR.²

PINPOINTING THE PROBLEMS

These are the security challenges that are keeping organizations in the dark:

**LACK OF BREACH-DETECTION PROCEDURES**

Many organizations lack proper procedures for detecting security breaches. Embarrassingly, outsiders tend to detect them before organizations do themselves. In fact, 69% of all breaches were first spotted by an external party, and 9% were first spotted by customers.²

**UNREGULATED ENTRYPONTS**

Today’s workers are taking network security into their own hands. Unregulated personal devices, unsanctioned applications and unsecure remote connections can put your data into the wrong hands.

**INCREASINGLY DYNAMIC THREATS**

As data becomes increasingly important to your organization, threats are taking more dynamic routes to infiltrate it — growing in number, type and sophistication. You need to take more complex steps to protect it.
THE SOLUTION

TO OBSERVE AND PROTECT.

Today’s security solutions must do more than block new breaches; they need to be able to identify existing ones, too. An intrusion prevention system (IPS) does just that. It analyzes network activity more deeply than a traditional firewall can. Here’s how it works:

SCAN. The IPS examines the payload on network packets for signs of network attack, misuse or anomalies that might indicate malicious intent.

ROUTE. After analyzing the packet, the IPS is alerted if there is a security breach and can choose to block or allow it, depending on designated security policies.

LEARN AND PREVENT. A next-generation IPS looks deep into network activity and even application traffic to identify and stop threats before they run rampant. Multiple IPSs can share their findings with one another to compile data about known attacks and attackers to prevent future strikes.

THE BIG PICTURE

IPS technologies are a critical part of a modern security plan. Without the human component, you're only seeing half the security picture. When implementing a comprehensive security plan, don't forget these two important steps:

FOSTER A CULTURE OF SECURITY
Educate your users on security threats and best practices to cultivate a respect for security. When they know what activities to avoid, users can be part of the solution.

IMPLEMENT THE RIGHT POLICIES
Organizations should be able to define appropriate levels of security. This helps inform policies and ensure that access to the most sensitive data is limited to essential personnel.

THE BENEFITS

WATCH IT GO.

The ideal IPS provides your organization with ways to watch, learn about and react to issues that arise on a daily basis. It can help with:

COMPREHENSIVE NETWORK SECURITY
No matter what device is connecting and generating traffic, IPS solutions sit in line with your network traffic to make sure it’s all getting inspected — preventing malicious activity from going unnoticed.

BUILT-IN DAMAGE CONTROL
The primary function of IPS is to keep attacks from happening, not just to seek threats out. By investing in IPS, you’re investing in technology that not only prevents attacks, but stops them once they’re already in motion.

ADAPTIVE SECURITY
IPS solutions regularly update their threat detection methods to account for new threat types, ensuring your security learns from changing threats and always stays up to date.
WHY CDW?

WE’VE GOT IPS INSIGHTS.

THE PEOPLE: Our dedicated account managers receive regular training in next-generation security. Our experienced security solution architects have deep knowledge and can guide you through every stage of your IPS investment, from preparation through deployment.

THE PARTNERS: Our partnerships with industry-leading security vendors grant you access to some of the best next-generation security products on the market, and our vendor-agnostic status guarantees that you get the right IPS solution for your unique situation.

THE PLAN: Our security experts are there for you throughout the entire lifecycle of your IPS investment. We can help you assess your network with security evaluations like our Rapid Vulnerability Assessment, Comprehensive Vulnerability Assessment and CDW Threat Check.

OUR PARTNERS

STANDOUT PARTNERS IN SECURITY.

McAfee Host Intrusion Prevention for Server proactively secures against known and new zero-day attacks. It boosts security and lowers costs by reducing the frequency and urgency of patching. Host Intrusion Prevention integrates with the McAfee ePolicy Orchestrator (ePO) platform for centralized reporting and management that’s accurate, scalable, easy to use and compatible with other McAfee and non-McAfee security products.

Cisco Intrusion Prevention Systems (IPS) solutions provide protection against sophisticated threats such as targeted attacks, Advanced Persistent Threats (APTs), botnets, SQL injection attacks, malware targeting application and OS vulnerabilities.

AWARDS & CERTIFICATIONS

• Cisco Certified Internetwork Expert (CCIE): Security
• McAfee Corporate Reseller Partner of the Year, North America – 2012
• Certified Information Systems Security Professional (CISSP)
• Certified Secure Software Lifecycle Professional (CSSLP)
• Certified Information Systems Auditor (CISA)
• Certified Information Systems Manager (CISM)
• Certified Ethical Hacker (C|EH)
• Global Information Assurance Certification (GIAC)
• GIAC Certified Incident Handler
• GIAC Security Essentials Certification (GSEC)
• HIPAA Academy Award
• Homeland Security Award
• PCI Approved Scanning Vendor (ASV)

To learn more about our IPS solutions, contact your account manager, call 800.800.4239 or visit CDW.com/security