Ntiva

Your Success. Secured.

NTIVA ADVANCED ENDPOINT DETECTION AND RESPONSE (EDR)

Solution Sheet

7900 Westpark Drive, Suite A100 | McLean, VA 22102
1-888-996-8482 | www.ntiva.com

Modern antivirus software protects your assets from the simplest attacks, but isn't much help when you're facing a determined attacker or modern hacking techniques.

Ntiva's Advanced Endpoint Detection and Response (EDR) uses powerful artificial intelligence techniques to stop attackers in their tracks.

WHAT IS NTIVA ADVANCED ENDPOINT DETECTION AND RESPONSE?

Ntiva's Advanced Endpoint Detection and Response (EDR) is a state-of-the-art adaptive protection solution for your desktops, laptops, and servers.

PROTECTION ANYTIME, ANYWHERE WITH AI & HUMANS WORKING TOGETHER

Traditional security such as firewalls and anti-virus software are no longer enough to protect your business from modern-day hackers.

For starters, most organizations conduct business away from the office (outside of the firewall) a great deal of the time, from hotels, airports and just about anywhere that has Wi-Fi. And because of the evolution of cyber threats, antivirus software no longer offers the same protection that it did in the '90s. Attackers are becoming much more sophisticated - every machine that is connected to the Internet is at risk.

The power of Ntiva's EDR solution is in the agent that lives on each user's computer, which automatically detects and stops potential attacks that have slipped past your antivirus software. EDR will detect that activity and contain the adversary before they can move laterally throughout your network.

Ntiva offers two separate EDR solutions to fit the needs and budgets of your business.

EDR Core is our standard solution that is suitable for most businesses. This highly automated solution uses sophisticated artificial intelligence (AI) software to detect potential attacks in their earliest stages and responds with automated routines to halt those attacks.

EDR Advanced is for organizations that require more protection, especially for those who manage very sensitive information. EDR Advanced offers the same state-of-the-art software as EDR Core but with another layer of protection - a team of security experts who operate around the clock to further analyze the data. As long as the computer has an Internet connection, the software agent will report back to the 24x7 Security Operations Center (SOC) to alert the team that trouble has been spotted. The team then analyzes trends and digs deeper into the root causes of alert to look for signs of the most advanced and persistent attackers, adding a human element on top of the AI software in order to uncover any threats that might have remained undetected.

HOW DOES EDR ADVANCED WORK?

Our unique approach to Endpoint Detection and Response wraps your business in three layers of protection.

The first layer detects potential attacks in their earliest stages and respond with automated routines to halt those attacks before a compromise occurs.

Standard anti-virus works by comparing a potential attack against a list of known profiles. New (Day Zero) exploits and sophisticated attacks don't appear on those lists, and so attackers can slip past anti-virus software.

We use a critically acclaimed artificial intelligence (AI) solution to identify activities that are something an attacker would try. It gathers information about how your computer behaves ordinarily and looks closely at items outside of standard behavior.

Most importantly, it acts in real-time to stop the attack or isolate a compromised machine to keep it from infecting others.

The second layer consists of seasoned security experts who review the alerts and investigate them more deeply. They've seen hundreds of attacks in all kinds of organizations, and they know how hackers think. They use this knowledge to leverage the forensic capabilities built into the agent to create a complete picture of an attack.

The third layer are skilled technicians who take the information provided by the security experts and put it into practice. Ntiva's technicians help hundreds of organizations run smoothly every day. They understand how to implement security measures without interrupting your business.

WHY CHOOSE NTIVA FOR EDR

As a top-notch IT services provider for more than a decade, Ntiva has seen the security landscape evolve and is excited to introduce a set of solutions oriented specifically toward small and mid-sized businesses (SMBs).

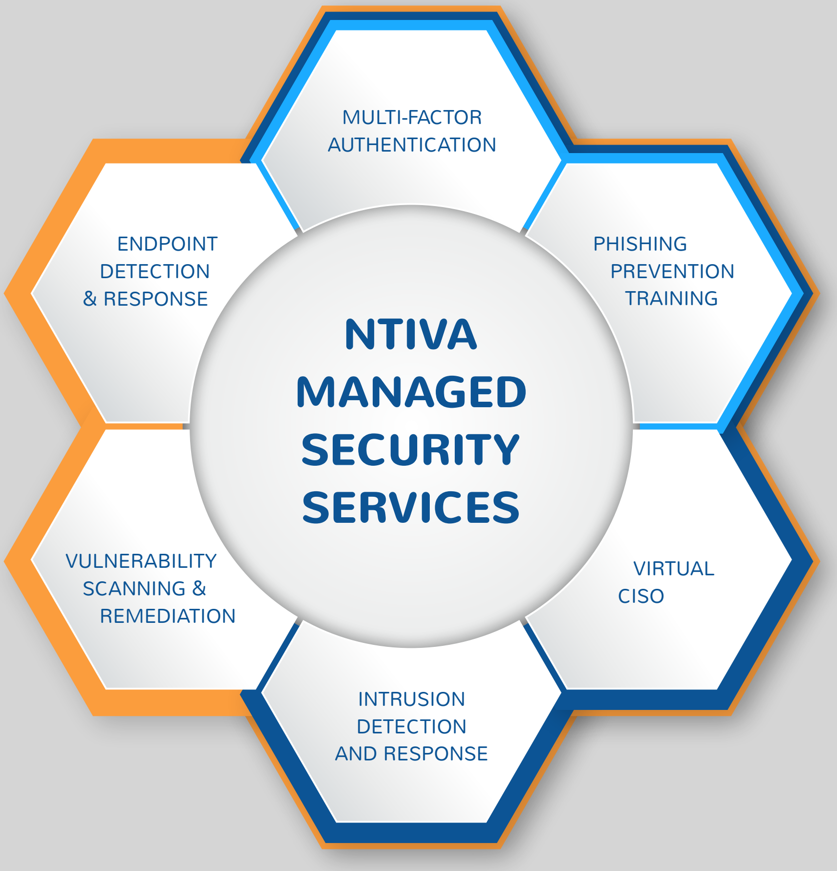
Unlike with most security providers, we work with SMB clients each day. We have technicians and security experts on staff who are all deeply familiar with the SMB world--our client portfolio is rich with associations, non-profits, consulting, legal, and financial firms.

We understand the SMB environment, risks and budgets, and have created an affordable solution that lets us offer sophisticated cyber-security services to organizations that could not afford to stand up this type of service themselves.

No business, large or small, is safe from the risk of a data breach in today's world. Ntiva's cyber security services can provide you with a competitive advantage, safeguard your data, meet your compliance requirements, and most importantly protect your reputation.

While cyber security needs vary based on organizational size and the type of data being protected, every organization needs foundational IT management and security.

Ntiva offers a comprehensive suite of Managed Security Services that can meet the needs and budgets of almost every organization. Below is a high-level guide, however, there is seldom a one-size-fits-all approach when it comes to cybersecurity. Please consult with us to determine which solutions are the best fit for you!


NTIVA MANAGED SECURITY SERVICES
MULTI-FACTOR AUTHENTICATION
PHISHING PREVENTION TRAINING
VIRTUAL CISO
INTRUSION DETECTION AND RESPONSE
VULNERABILITY SCANNING & REMEDIATION
ENDPOINT DETECTION & RESPONSE

Small organizations, fewer than 50 people and without large amounts of personally identifiable information or health information.

Organizations with 100-200 employees or that have large amounts of personally identifiable information or health information.

Organizations of 200+ employees, defense and federal contractors.

Contact Us to Consult with an Ntiva Security Expert