Managed Cybersecurity Services

Gain access to top cybersecurity services to protect your business and close your IT security gap

Ntiva

Your Success. Secured.

Cybersecurity Services and Solutions for Business

Ntiva provides a wide range of cybersecurity consulting and fully managed cybersecurity services. We protect your business from unrelenting attacks around the clock.

With Ntiva, you get 24/7 security monitoring, management, and remediation provided by a dedicated team of cyber experts. You enjoy layered protection, starting with a security assessment and offering high-availability security operations centers (SOC), SIEM, and more. And you gain access to skilled cybersecurity consultants — including virtual CISO services and cloud security services.

To jump to a specific section, click on one of the links below.

What Are the Types of Cybersecurity Services Offered by Ntiva?

Ntiva offers cybersecurity solutions and cybersecurity consulting services for businesses of all sizes. Our solutions are comprehensive — and affordable. Our in-house team of cybersecurity consultants protects your data, makes sure you meet compliance requirements, and gives you confidence that your business is protected against the latest threats.

Cybersecurity Risk Assessment

A cybersecurity risk assessment provides your business with an in-depth look at your current security posture. Our IT security services team identifies all your assets that could be affected by an attack, understands the risks associated with each element, helps you define what needs the most protection, and then provides a customized road map with short- and long-term milestones.

Virtual Chief Information Security Officer (vCISO)

A vCISO is a service designed to make top-tier security experts available to you on an as-needed basis. Our vCISO talent can bring both strategic and operational leadership to those who can't afford (or don't need) a full-time resource but do need someone to provide consistent security expertise.

Multifactor Authentication (MFA)

Passwords alone are no longer enough to protect your company against cyberattacks and data breaches. MFA protects your online data by ensuring that only verified users can access your business applications and services.

Intrusion Detection and Response (IDR)

Ntiva's IDR solution (also known as SIEM) actively monitors your network 24/7 for signs of attack before they happen. It consists of three important layers, including an automated threat detection system, skilled security experts who review these alarms, and remediation that happens in near real time, without interrupting your business. Intrusion detection systems are considered a must have!

Endpoint Detection and Response (EDR)

Antivirus software may protect you from the simplest attacks, but it's unlikely to be capable of protecting against sophisticated modern hacking techniques. Ntiva's Endpoint Detection and Response service uses powerful AI to stop attackers in their tracks—even when your devices are outside the office firewall—backed by a 24/7 SOC that further analyzes any additional undetected threats.

Phishing Prevention Training

Most security incidents start with a phishing attack aimed at employees. Ntiva's cybersecurity services include managed antiphishing training, providing you with an automated, 12-month campaign that steadily increases your employee's abilities to recognize, report, and block attempted phishing attacks.

Vulnerability Scanning

Ntiva's Vulnerability Scanning solution scans your network for the kinds of vulnerabilities attackers target most, including missing security patches, insecure settings, and unneeded services. The findings are analyzed, prioritized, and addressed, closing loopholes before attackers can exploit them.

IT Governance, Risk and Compliance (GRC)

GRC refers to a strategy for managing an organization's overall governance, enterprise risk management, and compliance with regulations. Ntiva's cybersecurity services team can help you create a well-planned governance, risk, and compliance strategy, which includes creating, auditing, and managing a clear framework that aligns your IT and business strategies.

Professional Dark Web Monitoring

What is dark web monitoring? Dark web monitoring can help keep data protected, so you can ensure sensitive information is kept secure. Our dark web monitoring services monitor the dark web for information that's being sold or traded to protect you from threats you might not have recognized.

Penetration Testing

To outfox cyberattackers, you need to know how they think — and how they make their attacks. Penetration testing from Ntiva allows you to safely identify your security gaps long before the wrong people find them.

How Does Ntiva Deliver IT Cybersecurity Solutions?

Managed Security Services

Ntiva offers Managed Security Services packages for small- and medium-size businesses (SMBs) who cannot afford to hire an in-house team to handle their cybersecurity.

We'll Guide You Through the MSP Onboarding Process

When you partner with Ntiva for your cybersecurity, we start our working relationship with a proprietary, four-stage onboarding process. Our dedicated Ntiva Onboarding Team (including a dedicated project manager and onboarding engineer) guides you through each stage. We start with discovery of your IT infrastructure, proceed to IT data collection, conduct an internal information review, and finish with implementation and go-live. Here's what this looks like in detail.

Phase 1: Managed Services Definition

The definition of services is a crucial part of the onboarding process. We discuss every service outlined in the signed Service Agreement to ensure our team has an in-depth understanding of your business prior to on-site data gathering, process documentation, and ongoing support.

Phase 2: IT Data Collection

Our technicians visit your site to gather information about your IT environment and to begin the documentation process. Their extensive engineering checklist covers such things as network investigation, security assessment, backup verification, server room inspections, and policy documentation.

Phase 3: Internal Information Review

The primary goal of this phase is to ensure your IT environment will meet your needs now and as your business grows. We review the information collected in Phase 2 with your dedicated team alongside our specialized senior technicians if needed.

Phase 4: Orientation Meeting and Service Handoff

Your Ntiva team meets with you to review your new client manual. This review includes a discussion of all findings, including recommendations for additional changes. It also includes the final tailoring of support procedures if needed. We schedule any recurring on-site visits and set up the cadence for recurring meetings between you and your account manager.

Dr. Jerry Craig
Senior Director
of Security/CISO

Your Team of Cybersecurity Experts

Cybersecurity is a team sport, and on your team are some of the best talent in the business. Your team is headed by Dr. Jerry Craig, Ntiva's CISO. Jerry has been warding off cyberthreats since 2001, and he teaches information security at the university level.

Your team consists of a wide range of security specialists, from security analysts to software engineers, from penetration testers to security administrators, from network engineers to cybersecurity consultants. Working together, your cybersecurity team helps you close your IT security gaps with the latest cybersecurity expertise.

How Can Ntiva Improve Your Cybersecurity?

Cybersecurity is key to keeping your business not just healthy, but competitive. As a top-tier IT services provider for more than a decade, we've seen the security landscape evolve. That's why we've designed a set of solutions specifically to meet the needs of SMBs.

Unlike most security providers, Ntiva works with SMB clients every day. We understand your environment, your risks, your budget constraints. We've created a set of affordable solutions that together create a comprehensive cybersecurity program to safeguard your data, help meet your compliance requirements, and give you a significant competitive advantage.

Upgrade Your Network Security Infrastructure

Most legacy networks are not equipped to deal with the sophistication and frequency of today's cyberattacks. Assess your infrastructure thoroughly to determine network security viability, then create a prioritized plan to address any deficiencies. Next-generation firewalls provide more comprehensive threat protection, including application control, intrusion protection, antivirus, and deep packet inspection.

Perform Regular Software Updates and Patches

All applications, operating systems, and security software should be reviewed regularly, and software updates and security patches should be subsequently applied. Identify any software that the manufacturer or provider no longer supports, so it can be upgraded or replaced.

Secure the Network Edge

In today's digital business environment, applications, workflows, and information need to move seamlessly across environments — and your cybersecurity strategies must follow. As the "network edge" becomes more fluid and harder to clearly define, focus on closing vulnerabilities wherever they may be. This means quickly detecting compromises and responding to those compromises in a rapid, comprehensive, and appropriate way. To do so, you must have in place the right intrusion detection system and security incident response plan.

Improve Physical Security

The International Organization for Standardization (ISO) provides an excellent reference resource for securing data and physical assets. Although it's natural to focus on the "cyber" aspect of cybersecurity, physical security is still critical. Restricting or denying access to computers, servers, and data centers is an integral part of protecting digital assets, as is educating users on effective physical security protocols.

Implement Cybersecurity Awareness Training

From phishing to pharming to inadvertent acts of negligence, employees are often your biggest risk vector. Therefore, one of the most effective ways to protect your organization is to create a culture of cybersecurity, where training is an ongoing process and your staff understand exactly which behaviors to avoid or embrace.

Conduct Cybersecurity Risk Assessments

A structured risk assessment can help identify and address significant security gaps that may be putting your company's data, digital assets, and network at risk. A typical assessment involves defining the system, identifying threats, determining the potential impact, analyzing the environment, and finally calculating the associated security risk.

How Much Do Managed Cybersecurity Services Cost?

The short answer is that you should expect to spend 10% of your IT budget on security. The longer answer is that how much you invest depends on your industry, the size of your organization, your IT footprint, and the complexity of your infrastructure, networks, and data.

» Learn more about How Much Cybersecurity Should Cost Your Business.

Ntiva Managed Cybersecurity Case Studies

» **Achieving & Maintaining NIST 800-171 Compliance for GovCon**
Read the Case Study »

» **Contractor Finds CMMC Success with MSP**
Read the Case Study »

» **Paradyme Improves Cybersecurity with Managed Security Services**
Read the Case Study »

What Are Managed Cybersecurity Services?

Managed cybersecurity services are services offered by a third-party provider to help organizations stay ahead of the latest cyber threats. In other words, managed cybersecurity is outsourced cybersecurity. An organization outsources part or all its cybersecurity (such as MFA, intrusion detection and response, and vulnerability scanning and remediation) to a managed cybersecurity provider.

What Are Managed Cybersecurity Service Providers?

A managed cybersecurity services provider offers outsourced cybersecurity services to organizations. The key word is “managed.” Managed cybersecurity services providers manage cybersecurity for their customers. They typically offer a wide range of services and expertise, everything from cybersecurity hardware and software to training, from best practices development to threat detection, mitigation, and prevention.

Ntiva is a managed cybersecurity services provider that offers a full suite of affordable solutions that deliver comprehensive cybersecurity to safeguard your data, meet your compliance requirements, and maintain your competitive advantage.

Ready to Get Started With a Cybersecurity Service Provider?

Contact Us Today

About Ntiva

Ntiva is an IT services provider that provides businesses with advanced technology expertise and support, including managed IT services, strategic consulting, cloud services, cyber-security and telecom solutions. Ntiva helps you with your cloud journey, recommending various technologies and helping you choose the cloud services that are right for your business and budget. We have a team of world-class talent that genuinely cares about the relationships we build, and who understands that response and precision are keys to a successful partnership.