SOLUTION OVERVIEW

Cognizant Cyber Threat Defense

Managed security that is flexible, scalable and adaptable to today's digital demands.

Managed security for today's threats

Modern organizations deploy tens or even hundreds of thousands of devices, ranging from desktops, laptops, tablets and smartphones to servers, firewalls, routers and switches. The number and variety of these devices, and the software that runs on them, will only grow with the addition of more mobile devices and of sensors on the Internet of Things.

Keeping users, data, endpoints and applications secure is a never-ending battle. A typical enterprise uses 70+ security point solutions in an effort to keep pace. This creates enormous security infrastructures that are costly and difficult to manage, much less adapt to changing requirements or to popular cloud platforms. Many of the point solutions can't even communicate with each other or manage hundreds of gigabytes of daily security log data.

In addition, most companies lack the expertise and staff to analyze all that data, find the most critical events and effectively respond to them. As a result, they are becoming more vulnerable even as they spend more on security.

As the challenges escalate, enterprises are turning to managed security service providers (MSSPs) for the specialized tools and skills required to cost-effectively fight the rising range, volume and severity of threats. These MSSPs must do more, however, than merely transmit hundreds of thousands of alerts that overworked internal staffs struggle to evaluate.

A modern MSSP must provide an integrated, contextual view of threat data to find and prioritize attacks. It must provide automated analysis and correlation to find even targeted or "quiet" attacks spread over time or across devices. It must provide instant and clear understanding of not just the technical, but the business impact of various threats so the organization can focus on the most urgent. And it must provide detailed workflows describing how to find and fight those threats.

Cognizant cyber threat defense

Cognizant Cyber Threat Defense is a scalable, next-generation managed security service that goes beyond providing masses of log reports and alerts to actionable, business-oriented workflows that guide you through mitigating the most critical threats..

Cognizant®

It taps a wide range of sources for the latest threat intelligence, such as lists of suspect IP addresses and URLs to lists of malware hashes and indicators of compromise. We combine that with data from your devices, endpoints and applications and correlate it using artificial intelligence to fight even low-profile attacks. For example, if the system sees suspicious activity from an IP address it can determine if that address has been flagged as suspect by a third-party security service. If so, it can then trigger automatic reconfiguration of your routers or firewalls to block that address.

These capabilities are backed by a global network of security operation centers, best-in-class cloud providers and dedicated teams empowered to help meet your most pressing security challenges. Our years of consulting helps us choose the right security monitoring, orchestration, automation and integrated threat intelligence platforms for you, and to customize our solution to assure a faster return on investment.

Key features

- Our machine learning analysis eliminates much of the drudgery of assessing threats by adding context such as associating IP addresses with users and assets, tracking changes of configurations as well as histories of vulnerabilities and patches on assets. It can also associate geolocation log activity with user accounts and timelines to determine if an access attempt from an unusual location is suspicious or reflects the fact a legitimate user is traveling.
- Gathering data of from thousands of devices, endpoints and applications throughout your network, IBM QRadar Security Information and Event Management includes out-of-the-box analytics, correlation rules and closed-loop feedback that continuously improves threat detection and speeds the investigation process by 50 percent.
- Anomali's comprehensive threat detection, investigation and response platform collects intelligence from a wide range of premium feeds, applies machine learning to reduce false positives, normalizes disparate sources and enriches the data with additional context to allow your analysts to make better decisions more quickly.
- Our improved security information model pre-defines and models threat cases, minimizing the need for iterative tuning with "out of the box" threat detection. Rather than assessing severity only by the type of event, we map business value to risk ratings considering factors such as the affected users and services and the criticality of the affected assets.
- ServiceNow's Security Operations platform provides a security orchestration, automation, and response engine that helps quickly prioritize and respond to threats based on their business impact, and prevent attacks by identifying, prioritizing and remediating misconfigured software.
- Prebuilt connectors to your IT infrastructure speed orchestration without the need for custom scripts or configurations. This enables remote changes to configuration policies, approval workflows and audit histories and easy sharing of data among platforms including access management, authentication, networking, hosts, firewalls and intrusion prevention systems.

Benefits of cognizant cyber threat defense

- Reduced time to identify and mitigate threats.
- Industry-leading analysis of user behavior detects suspicious activity such as access attempts at unusual times or from unusual devices, or access to a spurious, temporary domain name that exists only to send malware to a downstream system or commands to malware running on it.
- Frees your security experts from the drudgery of monitoring devices and alerts to proactively search for malware or attackers, improve automated security processes and better find or prioritize possible attacks.
- Typically requires less cost and effort than maintaining your own security operations center.
- Instant, up-to-date visibility into your security posture through our Cyber Threat Defense portal.
- Faster, more cost effective and assured security compliance through improved audits, guidance on optimal device configuration and expert help from Cognizant security experts.
- Reduces the need to hire and manage in-house security staff.
- Fast, Flexible and thorough onboarding with dedicated advisory time
- Global security operation centers assure timely response to threats at any hour and in any region.
- Use of first-tier cloud platforms provides scalability to monitor increasing numbers of users, applications or devices.
- Expert guidance from experienced security experts improves everything from tool selection to creation of automated remediation workflows.

Where Legacy Enterprise Security Falls Short

- Lack of incident intelligence and business context makes it hard to prioritize threats.
- Enterprises get volumes of log information but few business-oriented insights or remediation plans.
- Disparate solutions are expensive to maintain and difficult to manage.
- Slow to scale and adapt to changing needs.
- Not suited to cloud models.

Contact us at to cognizantsecurity@cognizant.com learn more about how Cognizant Cyber Threat Defense can provide more flexible, scalable and adaptable security starting with a detailed evaluation of your security requirements.

Contact your Cognizant representative today

Cognizant Security helps you achieve better business outcomes by securing your digital transformation. We provide the security capabilities you need to address ever-changing threats, maintain compliance and reduce the unsustainable burden of managing security infrastructure.

To learn more visit our website, www.cognizant.com/security or feel free to contact us directly at cognizantsecurity@cognizant.com

About Cognizant Digital Systems & Technology

Cognizant Digital Systems & Technology works with clients to simplify, modernize and secure IT infrastructure and applications, unlocking the power trapped in their technology environments. We help clients create and evolve systems that meet the needs of the modern enterprise by delivering industry-leading standards of performance, cost savings and flexibility. To learn more, contact us at simplify@cognizant.com or visit www.cognizant.com/cognizant-digital-systems-technology.

About Cognizant

Cognizant (Nasdaq-100: CTSH) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 195 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at **www.cognizant.com** or follow us @Cognizant.

Cognizant

World Headquarters

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

1 Kingdom Street
Paddington Central
London W2 6BD England
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102

India Operations Headquarters

#5/535 Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060