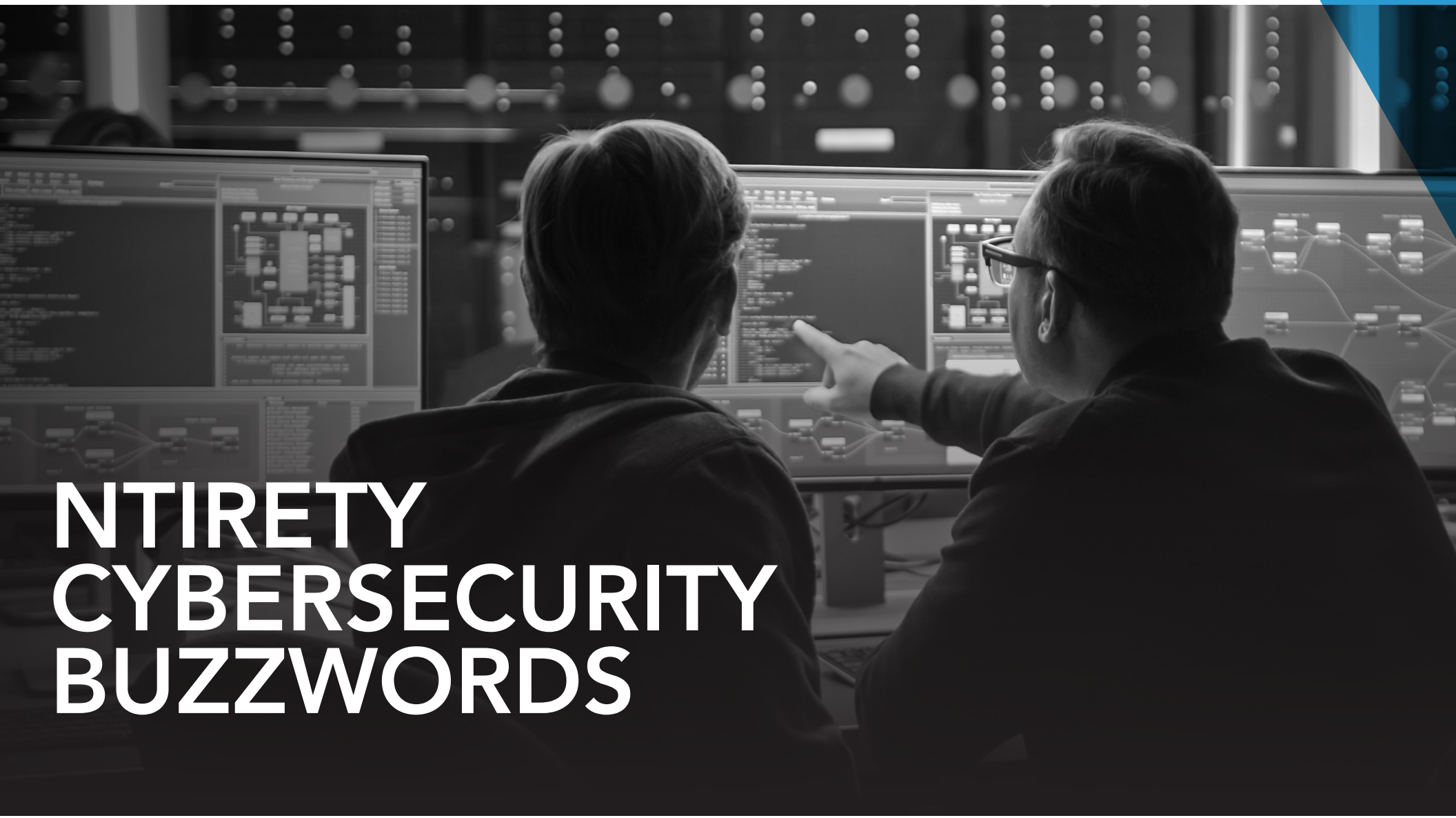
Ntirety



# NTIRETY CYBERSECURITY BUZZWORDS

# LEARN THE TERMS TO SECURE YOUR ENTERPRISE

Cybersecurity threats can feel even more daunting when they are described and identified by acronyms, abbreviations, and industry buzzwords not used in everyday conversation. But when it comes to protecting business IT and sensitive data, knowledge is power. Build a better defense vocabulary using the definitions and meanings of critical cybersecurity terminology below.

Schedule a consultation to see how compliant security will protect and optimize your business by visiting **ntirety.com/get-started** today.

## A:

**AD DS (Active Directory Domain Services)** A server function within Active Directory, the Microsoft developed service that lets administrators store and manage information about resources from a network and application in a distributed database.

**AI (Artificial Intelligence)** The simulation of human intelligence processes by machines, especially computer systems, to solve complex problems.

**Alarm** An observable event that could cause harm or a potential compliance violation detected through threat sensors or log collection appliances deployed within a computer system's environment.

**Amazon S3** "Simple Storage Service" from Amazon Web Services (AWS) that offers data storage.

**Analytics** The ability to utilize data to make informed decisions on potential security threats or vulnerabilities.

**Anomaly Detection** The ability to monitor for unusual events or trends in network traffic.

**Antivirus (of software)** Software designed to detect, prevent, and eliminate malware.

**API (Application Programming Interface)** Programming code that allows for the communication between two or more computers or computer programs.

**APTs (Advanced Persistent Threats)** A prolonged and targeted cyberattack in which an intruder gains access to a network to steal data and remains undetected for an extended period of time.

**Automation** The use of a wide array of technology and applications to automatically carry out processes based on certain events or triggers, while reducing human intervention.

**AWS (Amazon Web Services)** A cloud computing platform from Amazon that offers compute power, database storage, content delivery, and more.

**Azure** A cloud-based service designed by Microsoft that provides tools needed for a business to run virtual operations, such as data storage or analytics.

**Click on the terms below to take you to the page where the term is.**

## TYPES OF CYBERATTACKS AND THREATS

# B:

**Blockchain** A database that holds encrypted blocks of data and chains them together, making it difficult for hackers to make changes in the system.

**Botnet** A network of private computers infected with malicious software and controlled as a group without the owners' knowledge.

**Breach** Any incident that results in unauthorized access to computer data, applications, networks, or devices.

**BYOD (Bring Your Own Device)** A policy within an organization that permits the usage of personal devices—smartphones, personal computers, tablets, or USB drives—to connect to the organization's network and conduct work-related activities.

# C:

**CASB (Cloud Access Security Broker)** An on-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed.

**Case (or incident)** A correlation of alarms that harm an information system, violate acceptable use policies, or circumvent standard security practices.

**Castle Mentality** An outdated approach to cybersecurity based on the idea that securing the perimeter of an IT environment (i.e., building castle walls and digging a moat) is enough. It is outdated because it ignores activity within the environment that may be malicious, and it is becoming more and more difficult to secure the perimeter of more advanced cloud and hybrid environments.

**CCPA (California Consumer Privacy Act)** A state statute intended to enhance privacy rights and consumer protection for residents of California, U.S.A. It gives consumers more control over the personal information that businesses collect about them.

**Channel Partner** A channel partner is a company – such as a reseller, service provider, vendor, retailer or agent – that partners with another organization to market or sell their services, products or technologies.

**CHD (Card Holder Data)** Personal details from a person with a debit or credit card.

**CIS (Center for Internet Security)** A nonprofit organization whose mission is to "identify, develop, validate, promote, and sustain best practice solutions for cyber defense and build and lead communities to enable an environment of trust in cyberspace."

**Cloud-based (also cloud computing)** Applications, services, or resources made available to users on demand via the internet from a cloud computing provider's server.

**Colocation** A data center facility in which a business can rent space for servers and other computing hardware.

**Compliance** Actions that provide proof of abidance to internal policies and external laws.

**Compliance Management** The process of ensuring employees and activities across an organization are in line with laws, regulations, and requirements.

## BYOD
### (Bring Your Own Device)

A policy within an organization that permits the usage of personal devices—smartphones, personal computers, tablets, or USB drives—to connect to the organization's network and conduct work-related activities.

**Compromise** The disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

**Configuration** The way in which parts are organized in a computer system.

**Configuration Management** An engineering process in which a product's performance consistency is maintained.

**Container** A software package that "contains" an application's code that holds files and libraries needed to run.

**CPQ (Configure, Price, Quote)** A business software application designed for sales teams to provide product options and prices with accuracy.

**CSM (Customer Success Manager; also, Client Success Manager or Customer Service Manager)** An employee within an organization who supports customers from prospects to active users, with a focus on generating customer loyalty and fostering long-term customer relationships through positive experiences.

**CSP (Cloud Service Provider)** A third-party company offering a cloud-based platform, infrastructure, application, or storage services.

**Cyberattack** A malicious and deliberate attempt by an individual or organization to breach computer information systems, computer networks, infrastructures, or personal computer devices of another individual or organization.

**Cybersecurity (also cyber security, computer security, or IT security)** The practice of deploying people, policies, processes, and technologies to protect organizations, their critical systems, and sensitive information from digital attacks.

# D:

**DaaS (Desktop as a Service)** A cloud computing offering where a service provider delivers virtual desktops to end users over the internet, licensed with a per-user subscription.

**Data Cleansing** The process of identifying and eliminating inaccurate data from a database.

**Data Protection** The process of safeguarding important information from corruption, compromise, or loss.

**Database** A collection of data that is organized, stored, and accessed through a computer system.

**DDoS (Distributed Denial-of-Service) Attack** A malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.

**Development** A process of establishing a group of hardware and software components and their interfaces to create the layout for the buildout of a computer system.

**Disaster Recovery** The process of maintaining or reestablishing vital infrastructure and systems following a natural or human-induced disaster, such as a storm or battle, employing policies, tools, and procedures.

**Distributed Database** A database that consists of multiple databases across different physical locations.

**DNS (Domain Name System)** A hierarchical and distributed naming system for computers, services, and other resources on the internet or other internet protocol networks.

**Click on the terms below to take you to the page where the term is.**

## COMPLIANCE LAWS,RULES, AND REGULATIONS

- CCPA (California Consumer Privacy Act)
- FERPA (Family Educational Rights and Privacy Act)
- GDPR (Geometric Data Protection Regulation)
- HIPAA (Health Insurance Portability and Accountability Act)
- Internet Protocol Security

**DOS (Denial of Service Attack)** An attack where machine or network sources are inaccessible to their intended users because a cyber-criminal has shut down the system.

**DRaaS (Disaster Recovery as a Service)** A cloud-based offering that lets an organization store its data in a third-party cloud computer infrastructure.

**DW (Data Warehouse)** A system used for reporting and analyzing information from different sources into a single data storage unit.

# E:

**EDR (Endpoint Detection and Response; also, ETDR – Endpoint Threat Detection and Response)** A set of cybersecurity tools which are designed to detect and remove any malware from device endpoints or any other form of malicious activity on a network.

**Encryption** The process of converting information or data into a code, especially to prevent unauthorized access.

**Engagement** User interactions over an interface, such as the number of times a webpage is viewed, or time spent on a site.

**EPP (End Point Protection)** Software deployed at endpoints or entry points of end-user devices, such as desktops, laptops, and mobile devices to prevent those devices from being exploited by malicious actors or campaigns.

**EPTM (Endpoint Threat Management)** The authentication and supervision of the access rights of endpoint devices to a network.

**Escalation** A notification to a client that there is increased activity that warrants closer monitoring and/or response. In more serious cases, the SOC (security operations center) will email or call the client to follow up directly.

**Exploit** A code that takes advantage of a software vulnerability or security flaw.

# F:

**FERPA (Family Educational Rights and Privacy Act)** A federal law that secures the privacy of student education information.

**Full Stack** Software development that is composed of code connecting front (UI) to backend (API, etc.) computer interfaces.

# G:

**GCP (Google Cloud Platform)** Cloud services offered by Google that provide data storage and analytics.

**GDPR (General Data Protection Regulation)** A European Union (EU) law that gives individuals control of their personal data.

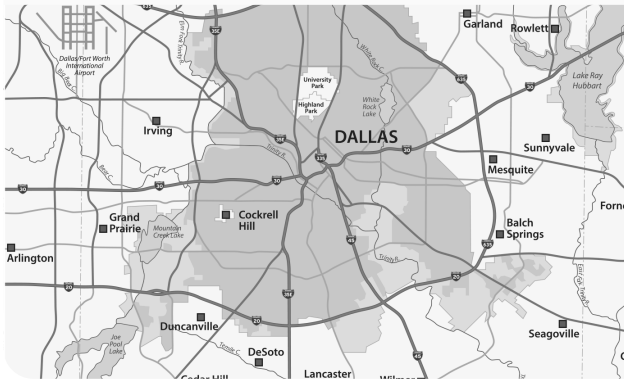
**Geo-blocking (or geoblocking)** A technology or service that provides the ability to restrict or allow access to the internet based upon the user's source IP's geographical location.

**GitHub** A web-based service that lets software developers collaborate and track project progress.

**GLA (Guidance Level Agreement)** A commitment between a service provider and a client that focuses on availability, performance, security, and cost with regards to a service provided.

## GEOBLOCKING

A technology or service that provides the ability to restrict or allow access to the internet based upon the user's source IP's geographical location.



# H:

**Hacker** A person that utilizes computers to gain unauthorized access to data.

**Half Stack** A partial software development that works on either the frontend or backend of a computer interface.

**HIPAA (Health Insurance Portability and Accountability Act)** A law that governs the use and release of an individual's health records.

**HITRUST (Health Information Trust Alliance)** An organization made up of representatives from the healthcare industry that helps healthcare groups and their providers with security and compliance matters.

# I:

**IaaS (Infrastructure as a Service)** A form of cloud computing that delivers fundamental compute, network, and storage resources on-demand, over the internet, and on a pay-as-you-go basis.

**IAM (Identity and Access Management)** A framework an organization uses to manage and protect its users and their identities

**ICB (Individual Case Basis)** When a change is made to a set of rules based on specific circumstances.

**IDS (Intrusion Detection System)** A device or software application that monitors a network or systems for malicious activity or policy violations and sends an alarm to an administrator

**Incident (or case)** A correlation of alarms that harm an information system, violate acceptable use policies, or circumvent standard security practices.

**Indicator of Attack** A focus on finding what an attacker's specific goal is to better prepare for future attacks.

**Indicator of Compromise** Evidence of potential attacks on a network.

**Interface** An interaction between a computer and another object or individual, such as a printer, another computer, or a human.

**IoT (Internet of Things)** A system of interrelated computing devices, mechanical and digital machines, provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

**IP (Internet Protocol; also, IP Address)** A numerical label that is connected to a computer network that uses internet protocol for communication. It serves two main functions: network interface identification and location addressing.

**IPsec (Internet Protocol Security)** A set of rules to establish secure communication over the IP networks.

**IPS (Intrusion Prevention System)** A network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

**IR (Incident Response)** An incident is an event that could lead to loss of, or disruption to, an organization's operations, services, or functions, and incident response is the steps used to prepare for, detect, contain, and recover from a data breach.

**Click on the terms below to take you to the page where the term is.**

## ORGANIZATIONS AND APPROACHES


» Castle Mentality

» CIS (Center for Internet Security)

» HITRUST (Health Information Trust Alliance)

» NIST (National Institute of Standards and Technology)

**IT Risk Management** An organized approach for identifying and proactively eliminating potential issues within computer systems.

# K:

**Kill Chain** A framework to understand the process of cyberattacks.

# L:

**LAN (Local Area Network)** A collection of computers in a small area, such as an office or school.

**Logs** A record of the events occurring within an organization's systems and networks.

# M:

**Malicious Insider** An internal threat to an organization that comes from a person within the organization, such as an employee, former employee, contractor, or business associate taking advantage of their security access to inflict harm on the organization. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems.

**Malware (also malicious software)** Any software intentionally designed to cause damage to a computer, server, client, or computer network.

**Master Agent** A master agent works as a middleman between managed security service providers and clients to deliver the specialized security services clients need. Because they don't work for any specific provider, they have no incentive to promote one over the other, which makes them a trustworthy source for managed security service contract procurement.

**MDM (Mobile Device Management)** Security software that allows organizations to enforce company policy through the monitoring of employees' mobile devices.

**MDR (Managed Detection and Response)** A cybersecurity service that provides organizations with active monitoring, threat detection, and prevention.

**MFA (Multi-Factor Authentication)** An electronic confirmation method that requires a user to provide two or more pieces of identification information in order to be granted access to a resource.

**ML (Machine Learning)** A branch of artificial intelligence (AI) and computer science which focuses on the use of data and algorithms to imitate human learning, and process and analyze large datasets to make predictions or decisions.

**MPS (Messages per Second)** A measurement of throughput used to understand the volume of logs that an environment generates that will need to be collected by the SIEM (security information and event management) tool for analysis and storage.

# N:

**Next-Generation** A term often used in conjunction with firewalls to describe firewalls that have advanced features for enhanced security.

## MULTI-FACTOR AUTHENTICATION

An electronic confirmation method that requires a user to provide two or more pieces of identification information in order to be granted access to a resource.

**NFT (Non-Fungible Token)** Data that is stored on a blockchain that is unique and cannot be replaced.

**NIDS (Network Intrusion Detection System)** A device that manages a network for suspicious activity.

**NPS (Net Promoter Score)** A measure of customer loyalty focusing on word-of-mouth promotion, passiveness, or detraction.

**NPS (Network Policy Server)** A service that helps a user manage network access authentication and authorization.

**NIST (National Institute of Standards and Technology)** A United States agency whose mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." NIST offers cybersecurity standards, such as NIST 800-171, and maintains the most commonly used database for known vulnerabilities and their associated risks.

**NoSQL (Not only Structured Query Language)** A database that stores and retrieves data using unique key values such as numbers or characters rather than rows and columns.

**NTA (Network Traffic Analysis)** The process of intercepting, recording, and analyzing network traffic communication patterns in order to detect and respond to security threats.

# O:

**OSI (Open Systems Interconnection)** Guidelines on how different computer systems should communicate with each other.

# P:

**PaaS (Platform as a service)** A cloud computing offering that provides users with a cloud environment in which they can develop, manage, and deliver applications.

**PCI (Payment Card Industry)** Standards for electronic payment usage, such as credit or debit cards.

**Penetration Test** An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.

**PHI (Protected Health Information)** Information in medical records about health status, provision of healthcare, or payment of healthcare that can be traced back to an individual.

**Phishing** When an attacker tricks a user into revealing confidential information using false pretenses, usually through email.

**PII (Personally Identifiable Information)** Information that can be traced to an individual's identity.

**POC (Proof of Concept)** Evidence from an experiment that shows the feasibility of a concept.

# R:

**Ransomware** A form of malware that encrypts a victim's files, followed by an attacker demanding ransom from the victim in order to regain access to their data.

**RAT (Remote Access Tool/Trojan)** A type of malware that creates a backdoor for administrative control and unauthorized remote access to a

**Click on the terms below to take you to the page where the term is.**

## AS A SERVICES

- DaaS (Desktop as a Service)
- DRaaS (Disaster Recovery as a Service)
- IaaS (Infrastructure as a Service))
- PaaS (Platform as a Service)
- SaaS (Software as a Service)
- UCaaS (Unified Communications as a Service)

victim's machine. Attackers can use the exploited machines to perform various malicious activities, such as installing and removing programs, manipulating files, reading data from the keyboard, harvesting login credentials, and much more.

**RBL (Real-Time Blacklist)** A list of IP addresses that are known for sending spam messages or emails.

**Real-Time** Near instantaneous. And in security, this term is often used to describe intrusion prevention measures that can identify threats and stop them with little or no reaction time needed.

# S:

**SA (Solution Architect)** A solutions architect creates the overall technical vision for a specific solution to a business problem. They design, describe, and manage the solution. In many ways, this person builds the bridge between a business problem and the technology solution and outlines each of the phases and requirements required to make that solution work.

**SaaS (Software as a Service)** A cloud computing offering that provides users with access to a vendor's cloud-based software that can be accessed through the web or API.

**SASE (Secure Access Service Edge)** A technology used to deliver wide area network (WAN) and security controls as a cloud computing service directly to the source of connection rather than a data center.

**Secure Remote Access** A service that allows client IT staff to establish secure connections with a remote, non-public computer network.

**Security Posture Management** A service that continuously monitors cloud resources for security threats. Ntirety's security experts will provide recommendations on improving security posture within the cloud.

**Security Reporting** A service that provides metrics-based reporting of monthly or weekly events, granting visibility of trends and patterns, as well as common events and alarms within an infrastructure.

**Serverless Function** A task (programmatic function) written by a software developer to perform a single action.

**Service Level Agreement** A commitment between a client and a service provider to ensure clients are receiving the services they are entitled to.

**SIEM (Security information and Event Management)** A platform that combines information management with event management to provide real-time analysis of security alerts generated by applications and network hardware. It is also used to log security data and generate compliance reports.

**SmartResponse** Actions that are automated defensive or operational responses to triggered alarm rules.

**SOAR (Security Orchestration, Automation, and Response)** Technologies that enable organizations to collect inputs monitored by a security operations team. For example, alerts from the SIEM system and other security technologies—where incident analysis and triage can be performed by leveraging a combination of human and machine power—help define, prioritize, and drive standardized incident response activities. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.

## SaaS
### (Software as a Service)

A cloud computing offering that provides users with access to a vendor's cloud-based software that can be accessed through the web or API.

**SOC (Security Operations Center)** A centralized unit staffed by expert security personnel that deals with security issues on an organizational and technical level.

**SQL (Structured Query Language)** Domain specific language used in programming, management, and use of relational databases.

**SSL (Secure Socket Layer)** A protocol for transmitting private information via the internet using a cryptographic system that uses two keys to encrypt data – a public key known to everyone, and a private or secret key known only to the recipient of the message.

# T:

**TAM (Technical Account Manager)** A technical account manager is a customer service professional who teaches customers about how to use new products and services.

**Triage and Incident Management** When the SOC (security operations center) examines incoming alarms to determine false positives from threats and create cases to notify the client of any identified threats.

**Tuning** The process of configuring rules for alerts and notifications in a SIEM (security information and event management) to remove false positives in order to make alerts more meaningful and reduce noise.

# U:

**UBA (User Behavior Analytics)** A cybersecurity process involving detection of insider threats, targeted attacks, and financial fraud. UBA solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns—anomalies that indicate potential threats.

**UCaaS (Unified Communications as a Service)** A cloud-based offering that offers a variety of communication functions, such as instant messaging or video conferencing.

**URL Filtering** The monitoring and controlling of how users access the web over HTTP and HTTPS with the use of deep packet inspection.

**User Acceptance Testing** Software tested by its intended audience to determine if it is completing its functions correctly.

# V:

**vCISO Service (Virtual Chief Information Security Office Service)** A service performed by a cybersecurity expert who uses their vast cybersecurity and industry knowledge base to help organizations develop and manage an information security program that fits their business needs and goals.

**VDI (Virtual Desktop Infrastructure)** A desktop environment that is hosted on a central server.

**Virtual Firewall** A network firewall service or appliance running entirely within a virtualized environment that provides the usual packet filtering and monitoring provided via a physical network firewall.

**VMware** A computer software company that provides cloud-based services allowing businesses to use multiple applications on one server.

## URL FILTERING

The monitoring and controlling of how users access the web over HTTP and HTTPS with the use of deep packet inspection.

**VPN (Virtual Private Network)** A network that lets users send and receive data from public networks while hiding a user's identity, making it more difficult for third parties to track online activity.

**Vulnerability** A weakness which can be exploited by a cyberattack to gain unauthorized access to and/or perform unauthorized actions on a computer system.

**Vulnerability Management** The process of minimizing risk created by vulnerabilities in an environment, often utilizing machine learning and automation to accelerate the process.

**Vulnerability Scan** An automated system that looks for weaknesses within network devices or software applications.

# W:

**WAAP (Web Application and API Protection)** Unlike a traditional firewall, a WAAP is a highly specialized security tool specifically designed to protect web applications and APIs. It protects against common threats, such as DDoS attacks and bots.

**WAF (Web Application Firewall)** The protection of web applications from potential attacks through filtering, monitoring, and blocking.

**WAN (Wide Area Network)** A form of telecommunication that extends over a large geographical location.

**WAR (Well Architected Review)** An architectural assessment based upon the Well-Architected Framework. The Well-Architected framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications.

**Workstation Patching** The process of distributing and applying updates to PC software. These patches are necessary to correct errors or update functionality.

# X:

**XDR (Cross-layered Detection and Response)** An advanced form of EDR (endpoint detection and response) that usually considers both endpoint and network security and is optimized for management through a SIEM (security information and event management).

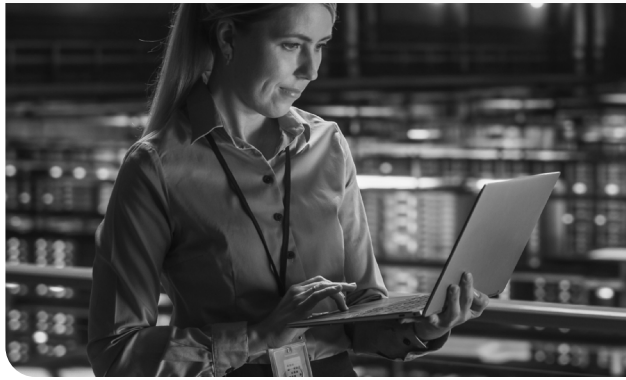
# Z:

**Zero Day** A computer-software vulnerability previously unknown to those who should be interested in its mitigation, such as the vendor of the target software. Until the vulnerability is mitigated, hackers can exploit it to adversely affect programs, data, additional computers, or a network.

**Zero Trust (also, ZTNA – Zero Trust Network Access)** A strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction, rooted in the principal of "never trust, always verify".


## WAN
### (Wide Area Network)

A form of telecommunication that extends over a large geographical location.

Ntirety™

Managing security and compliance is a strategic, economic imperative that directly impacts business outcomes. Ntirety is the only company that embeds compliant security throughout IT and company culture, protecting enterprises with a comprehensive compliant security solution. With over 20 years of experience and deep security expertise, Ntirety's three US-based security operations centers (SOCs) simplify risk management programs with a full protection, recovery and assurance suite of services. Learn more about Ntirety's award-winning and globally-trusted Compliant Security Solutions at ntirety.com.

## NTIRETY CERTIFICATIONS & STANDARDS

HITRUST CSF Certified

AICPA SOC

PCI

aws PARTNER Well-Architected Partner Program

HIPAA

ISO

NIST

www.ntirety.com | SALES 1.888.603.4678 or channelpartners@ntirety.com | SUPPORT 1.866.918.4678



Rev:0123