Advanced Persistent Threat (APT)

In an APT attack, a threat actor uses the most sophisticated tactics and technologies to penetrate a high-profile network. APTs aim to stay ‘under the radar’ and explore the network while remaining undetected for weeks, months, and even years. APTs are most often used by nation-state threat actors wishing to cause severe disruption and damage to the economic and political stability of a country. They can be considered the cyber equivalent of espionage ‘sleeper cells’.

Advanced Threat Protection (ATP)

Advanced Threat Protection (ATP) are security solutions that defend against sophisticated malware or hacking attacks targeting sensitive data. Advanced Threat Protection includes both software and managed security services.

Adware

Adware bombards users with endless ads and pop-up windows and causes a nuisance to the user experience. Adware can also pose a real danger to devices and the unwanted ads can include malware or redirect user searches to malicious websites that collect personal data about users. Adware programs are often built into freeware or shareware programs, where the adware operator collects an indirect fee for using the program. Adware programs usually do not show themselves in the system in any way. Adware programs seldom include a de-installation procedure, and attempts to remove them manually may cause the original carrier program to malfunction. Read more

Anti-Botnet

Anti-Botnet tools automatically generate botnet checks when a user browses a website. If a risk is detected, it sends back a warning message to the device. The most common anti-botnet solution is CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). Read more on Allot’s solutions for Home Security.

Anti-Malware

Anti-Malware is a program designed to protect computers and networks against any threats or attacks from viruses such as adware, spyware, and any such other malicious programs

Anti-Phishing

Anti-Phishing protects users from fraudulent websites, often perfect replicas of legitimate websites, undetectable to the human eye. Protection is enforced by detecting fraudulent emails, and by blocking phishing websites. Read more

Anti-Virus

Anti-Virus solutions integrate the latest generation of virus detection technology to protect users from viruses, spyware, trojans, and worms that can infect equipment through email or internet browsing.

Attack Vector

An Attack Vector is the collection of all vulnerable points by which an attacker can gain entry into the target system. Attack vectors include vulnerable points in technology as well as human behavior, skillfully exploited by attackers to gain access to networks. The growth of IoT devices and (Work from Home) have greatly increased the attack vector, making networks increasingly difficult to defend.

Authentication

Authentication is the process of verifying the identity of a user or piece of information and the veracity of the information provided. In computing, it is the process of identifying a person or system with a username, password, etc. Authentication helps individuals and systems gain authorization based on their identity and prevent unauthorized access.

Backdoor

Attackers use a Backdoor to gain access to a computer or a network. A programmer may bypass security steps and gain access to a computer through trapdoor programs, in the event of an attack on the computer system or networks. Attackers may also use such mechanisms to enter computers or networks without proper permission.

Banker Trojan

A Banker Trojan is a malicious computer program that intercepts sensitive personal information and credentials for accessing online bank or payment accounts. Read more

Blacklist, Blocklist, Denylist

Blacklist, Blocklist, or Denylist is a basic access control mechanism that allows elements such as email addresses, users, passwords, URLs, IP addresses, domain names, file hashes, etc. through the system, except those explicitly mentioned which are denied access.

Bot A Bot is a program that automates actions on behalf of an agent for some other program or person and is used to carry out routine tasks. Their use for malicious purposes includes spam distribution, credentials harvesting, and the launching of DDoS attacks.

Botnet

A Botnet is a collection of compromised computers running malicious programs that are controlled remotely by a C&C (command & control) server operated by a cyber-criminal. Cybercriminals exercise remote control through automated processes (bots) in public IRC channels or websites. (Such websites may either be run directly by the 'bot herder,' or they may be legitimate websites that have been subverted for this purpose.) Read more on Allot's solutions for Home Security.

Brute Force Attack

This is a method for guessing a password (or the key used to encrypt a message) that involves systematically trying a high volume of possible combinations of characters until the correct one is found. One way to reduce the susceptibility to a Brute Force Attack is to limit the number of permitted attempts to enter a password – for example, by allowing only three failed attempts and then permitting further attempts only after 15 minutes.

Business Continuity Plan

A Business Continuity Plan is an organization's playbook for how to operate in an emergency situation, like a massive cyberattack. The business continuity plan provides safeguards against a disaster and outlines the strategies and action plan on how to continue business as usual in the event of any large-scale cyber event. Read more on Allot's solutions for Business Security.

Business Disruption

The term Business Disruption refers to any interruption in the usual way that a system, process, or event works. Cyberattacks cause disruption to business operations and the associated risk of losses to the organization. Read more on Allot's solutions for Business Security.

BYOC

Bring Your Own Computer (BYOC) is a fairly recent enterprise computing trend by which employees are encouraged or allowed to bring and use their own personal computing devices to perform some or part of their job roles, specifically personal laptop computers.

BYOD

Bring Your Own Device (BYOD) is a policy of the organization allowing, encouraging or requiring its employees to use their personal devices such as smartphones, Tablet PCs, and laptops for official business purposes and accessing enterprise systems and data.

BYOL

Bring Your Own Laptop (BYOL) is a specific type of BYOC by which employees are encouraged or allowed to bring and use their own laptops to perform some or part of their job roles, including possible access to enterprise systems and data.

CAPTCHA

A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a challenge-response test commonly used by websites to verify the user is a real human and not a bot. They can include simple arithmetic and questions about images, that bots have difficulty answering.

Clickjacking

Clickjacking involves tricking someone into clicking on one object on a web page while they think they are clicking on another. The attacker loads a transparent page over the legitimate content on the web page so that the victim thinks they are clicking on a legitimate item when they are really clicking on something on the attacker's invisible page. This way, the attacker can hijack the victim's click for their own purposes. Clickjacking could be used to install malware, gain access to one of the victim's online accounts, or enable the victim's webcam.

Clientless

Clientless refers to a program that is run entirely from the network, without requiring any installation of software on the endpoint device running the program. Code Injection Code Injection is commonly used by malware to evade detection by antivirus and anti-malware programs by injecting malicious code into a legitimate process. This way the

legitimate process serves as camouflage so all anti-malware tools can see running is the legitimate process and thus obfuscates the malicious code execution.

COTS (Commercial off-the Shelf)

Commercial off-the Shelf or Commercially Available off the Shelf (COTS) products are packaged solutions that are then adapted to satisfy the needs of the purchasing organization, rather than the commissioning of custom-made, or bespoke, solutions.

Critical Infrastructure

Critical Infrastructure represents the fundamental systems of an organization that is important for its survival and where any threat to such basic systems would endanger the entire organization.

Cryptojacking

Cryptojacking consists of hackers using the computing power of a compromised device to generate or “mine” cryptocurrency without the owner’s knowledge. Mining can be performed either by installing a malicious program on the target computer or through various kinds of fileless malware. Sometimes attackers take over part of the computer’s processing power when a page containing a special mining script is opened. Cryptojacking has been known to occur when viewing online ads or solving a CAPTCHA.

Cyberbullying

Cyberbullying is the use of electronic means, primarily messaging and social media platforms, to bully and harass a victim. Cyberbullying has become a major problem, especially affecting young people, as it allows bullies to magnify their aggressive behavior, publicly ridicule victims on a large scale, and carry out damaging activities in a way that is difficult for parents and teachers to detect.

Cybersecurity

Cybersecurity relates to processes employed to safeguard and secure assets used to carry information of an organization from being stolen or attacked. It requires extensive knowledge of possible threats such as viruses or other malicious objects. Identity management, risk management, and incident management form the crux of the cybersecurity strategies of an organization. Read more

Dark Web

The Dark Web is encrypted parts of the internet that are not indexed by search engines, most notoriously used by all types of criminals including; pedophiles, illicit human and contraband traffickers, and cyber criminals, to communicate and share information without being detected or identified by law enforcement. Malware of all types can be purchased on the dark web. A subset of the deep web, which can be accessed by anyone with the correct URL, dark web pages need special software (ex. Tor) with the correct decryption key and access rights and knowledge to find content. Users of the dark web remain almost completely anonymous due to its P2P network connections which makes network activity very difficult to trace.

Data Breach

A Data Breach is the event of a hacker successfully exploits a network or device vulnerability and gains access to its files and data.

Data Integrity

Data Integrity is a broad term that refers to the maintenance and assurance of data quality. This includes the accuracy and consistency of data over its entire lifecycle. Data Integrity is an important part of the design, implementation, and use of any data system that stores, processes, or retrieves information. The term is broad in scope and may have widely different meanings depending on the specific context

Data LossPrevention (DLP)

Data Loss Prevention (DLP) is an umbrella term for a collection of security tools, processes, and procedures that aim to prevent sensitive data from falling into unauthorized or malicious hands. DLP aims at preventing such occurrences through various techniques such as strict access controls on resources, blocking or monitoring email attachments, preventing network file exchange to external systems, blocking cut-and-paste, disabling the use of social networks and encrypting stored data.

Data Theft

Data Theft is the deliberate theft of sensitive data by nefarious actors.

DDoS

A Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack is when one or more compromised systems launch a flooding attack on a remote target(s), in an attempt to overload network resources and disrupt service. Some DDoS attacks have caused prolonged, complete service shutdowns of major online operators. Learn more about DDoS attack types.

Decryption

Decryption is the process of decoding cipher text to plain text so that it is readable by humans. It is the reverse of encryption, the process of converting plain text to cipher text. Cybercriminals use decryption software and techniques to 'break' security encryption and gain access to protected information.

Detection and Response

Network Detection and Response is a security solution category used by organizations to detect malicious network activity, perform a forensic investigation to determine the root cause, and then respond and mitigate the threat.

Digital Forensics

Digital Forensics is the process of procuring, analyzing, and interpreting electronic data for the purpose of presenting it as legal evidence in a court of law.

Digital Transformation

Digital Transformation is the process of using digital technologies to create or modify business processes and customer experiences to keep up-to-date with current business and market requirements.

Domain Name Systems (DNS) Exfiltration

Domain Name System (DNS) Exfiltration is a lower-level attack on DNS servers to gain unauthorized access. Such attacks are difficult to detect and can lead to loss of data. Read more on Allot's DNS solutions.

Drive-By Download Attack

Drive-by Downloads or attacks are a common method of spreading malware. Cybercriminals look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script may install malware directly onto the computer of someone who visits the site, or it may take the form of an IFRAME that re-directs the victim to a site controlled by the cybercriminals. Such attacks are called 'drive-by downloads' because they require no

action on the part of the victim — beyond simply visiting the compromised website: they have infected automatically (and silently) if their computer is vulnerable in some way (e.g., if they have failed to apply a security update to one of their applications).

Encryption

Encryption is a process of maintaining data confidentiality by converting plain data into secret code with the help of an encryption algorithm. Only users with the appropriate decryption key can unscramble and access encrypted data or cipher text.

Endpoint Protection

Endpoint Protection refers to a system for network security management that monitors network endpoints, hardware devices such as workstations and mobile devices from which a network is accessed. Read more on Allot's Endpoint Protection solutions.

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) are tools for protecting computer endpoints from potential threats. EDR platforms comprise software and networking tools for detecting suspicious endpoint activities, usually via continuous network monitoring.

Exploit

An exploit is taking advantage of a vulnerability or flaw in a network system to penetrate or attack it.

Fast Identity Online (FIDO)

Fast Identity Online (FIDO) is a set of open authentication standards that enable a service provider to leverage existing technologies for passwordless authentication.

Fileless Malware

Fileless Malware (FM), aka "non-malware," or "fileless infection," is a form of malicious computer attack that exists exclusively within the realm of volatile data storage components such as RAM, in memory processes, and service areas. This differentiates this form of malware from the classic memory-resident virus which requires some contact with non-volatile storage media, such as a hard disk drive or a thumb drive. Normally picked up following visits to

malicious websites, fileless malware does not exist as a file that can be detected by standard antivirus programs. It lurks within a computer's working memory and is exceptionally difficult to identify. However, this type of malware rarely survives a computer reboot, after which the computer should work as it did prior to infection.

Firewall

A Firewall is a security system that forms a virtual perimeter around a network of workstations preventing viruses, worms, and hackers from penetrating.

Greylist

A Greylist contains items that are temporarily blocked (or temporarily allowed) until an additional step is performed.

Hacker

A Hacker is a term commonly used to describe a person who tries to gain unauthorized access to a network or computer system.

Honeypot

Honeypots are computer security programs that simulate network resources that hackers are likely to look for to lure them in and trap them. An attacker may assume that you're running weak services that can be used to break into the machine. A honeypot provides you with advanced warning of a more concerted attack. Two or more honeypots on a network form a honeynet.

Identity and Access Management (IAM)

Identity and Access Management (IAM) is the process used by an organization to grant or deny access to a secure system. IAM is an integration of workflow systems that involves organizational think tanks that analyze and make security systems work effectively.

Identity

Theft Identity Theft occurs when a malicious actor gathers enough personal information from the victim (name, address, date of birth, etc.) to enable him to commit identity fraud – i.e., the use of stolen credentials to obtain goods or services by deception. Stolen data can be used to create a new account in the victim's name (e.g., a bank

account), to take over an existing account held by the victim (e.g., a social network account), or to masquerade as the victim while carrying out criminal activities.

Indicators of Compromise (IOC)

Indicators of Compromise (IoC) are bits of forensic data from system log entries or files that identify potentially malicious activity on a system or network. Indicators of Compromise aid information security and IT professionals in detecting data breaches, malware infections, or other threat activity.

In-line Network Device

An In-line Network Device is one that receives packets and forwards them to their intended destination. In-line network devices include routers, switches, firewalls, and intrusion detection and intrusion prevention systems, web application firewalls, anti-malware, and network taps. NetworkSecure delivers comprehensive in-line cybersecurity protection to CSP subscribers.

Insider Threat

An Insider Threat is when an authorized system user, usually an employee or contractor, poses a threat to an organization because they have authorized access to inside information and therefore bypass most perimeter-based security solutions.

Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is a network security system designed to prevent network penetration by malicious actors.

IoT

The term Internet of Things (IoT) is used to describe everyday objects that are connected to the internet and are able to collect and transfer data automatically, without the need for human interaction. The Internet of Things encompasses any physical object (not just traditional computers) that can be assigned an IP address and can transfer data: this includes household appliances, utility meters, cars, CCTV cameras, and even people (e.g., heart implants). Read more about solutions for IoT Security.

Keylogger

A Keylogger is a kind of spyware software that records every keystroke made on a computer's keyboard. It can record everything a user types including instant messages, email, usernames, and passwords.

Malvertising

Malvertising is the use of online ads to distribute malicious programs. Cybercriminals embed a special script in a banner, or redirect users who click on an ad to a special page containing code for downloading malware. Special methods are used to bypass large ad network filters and place malicious content on trusted sites. In some cases, visitors do not even need to click on a fake ad — the code executes when the ad is displayed.

Malware

Malware is a general term for any type of intrusive computer software with malicious intent against the user.

Man-in-the Middle Attack

A man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. For example, a victim believes he's connected to his bank's website and the flow of traffic to and from the real bank site remains unchanged, so the victim sees nothing suspicious. However, the traffic is redirected through the attacker's site, allowing the attacker to gather any personal data entered by the victim (login, password, PIN, etc.).

MITRE ATT&CK™ Framework

The MITRE ATT&CK™ framework is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk. The aim of the framework is to improve post-compromise detection of adversaries in enterprises by illustrating the actions an attacker may have taken.

Network-based (cyber) Security

Mass-market cybersecurity services (e.g., anti-malware, anti-phishing) that operate from within a CSP's network and not at the endpoint, such as a PC or a mobile device. Network-based services can protect any connected device regardless of model or operating system. This type of service, however, cannot be bypassed like other cybersecurity solutions and they can be implemented with no software installation, upgrades or configuration required on the part of the end user, leading to high rates of service adoption. Read more on solutions for Network Security.

Parental Controls

Parental Controls are features which may be included in digital television services, computer and video games, mobile devices, and software that allow parents to restrict the access of content to their children. These controls were created to help parents control which types of content can be viewed by their children.

Patch

A Patch provides additional, revised or updated code for an operating system or application. Except for open source software, most software vendors do not publish their source code. So, patches are typically pieces of binary code that are patched into an existing program (using an install program).

Pen Testing

Pen (Penetration) Testing is the practice of intentionally challenging the security of a computer system, network, or web application to discover vulnerabilities that an attacker or hacker could exploit.

Phishing

Phishing is a type of internet fraud that seeks to acquire a user's credentials by deception. It includes the theft of passwords, credit card numbers, bank account details, and other confidential information. Phishing messages usually take the form of fake notifications from banks, providers, e-pay systems, and other organizations. The phishing attempt will try to encourage a recipient, for one reason or another, to enter/update personal data. Common reasons given can include "suspicious login to the account," or "expiration of the password."

PII

Personal Identifiable Information (PII or PII) is a type of data that identifies the unique identity of an individual.

Process Hollowing

Process Hollowing is a security exploit in which an attacker removes code in an executable file and replaces it with malicious code. The process hollowing attack is used by hackers to cause an otherwise legitimate process to execute malicious code. This attack can be done while evading potential defenses, such as detection analysis software.

Ransomware

Ransomware is the name given to malicious programs designed to extort money from victims by blocking access to the computer or encrypting stored data. The malware displays a message offering to restore the system/data in return for payment. Sometimes, cybercriminals behind the scam try to lend credibility to their operation by masquerading as law enforcement officials. Their ransom message asserts that the system has been blocked, or the data encrypted, because the victim is running unlicensed software or has accessed illegal content, and that the victim must pay a fine. Read more on Allot's solutions for Business Security.

Remote Desktop Protocol (RDP)

RDP is a protocol for remotely connecting to computers running Windows. It enables interaction with desktop elements as well as access to other device resources. RDP was conceived as a remote administration tool. However, it is often used by intruders to penetrate targeted computers. By exploiting incorrectly configured RDP settings or system software vulnerabilities, cybercriminals can intercept an RDP session and log into the system with the victim's permissions.

Risktool

Risktool programs have various functions, such as concealing files in the system, hiding the windows of running applications, or terminating active processes. They are not malicious in themselves, but include cryptocurrency miners that generate coins using the target device's resources. Cybercriminals usually use them in stealth mode. Unlike NetTool, such programs are designed to operate locally.

Rootkit

A Rootkit is a collection of software tools or a program that gives a hacker remote access to, and control over, a computer or network. Rootkits themselves do not cause direct harm – and there have been legitimate uses for this type of software, such as to provide remote end user support. However, most rootkits open a backdoor on targeted computers for the introduction of malware, viruses, and ransomware, or use the system for further network security attacks. A rootkit is typically installed through a stolen password, or by exploiting system vulnerabilities without the victim's knowledge. In most cases, rootkits are used in conjunction with other malware to prevent detection by endpoint antivirus software.

Sandbox(ing)

In cybersecurity, a sandbox is an isolated environment on a network that mimics end-user operating environments. Sandboxes are used to safely execute suspicious code without risking harm to the host device or network.

Scareware

Scareware is malware that uses scare tactics, often in the form of pop-ups that falsely warn users they have been infected with a virus, to trick users into visiting malware-containing websites.

SECaaS

Security as a Service (SECaaS) is a type of cloud computing service where the provider offers the customer the ability to use a provided application. Examples of a SECaaS include online e-mail services or online document editing systems. A user of a SECaaS solution is only able to use the offered application and make minor configuration tweaks. The SECaaS provider is responsible for maintaining the application. Allot Secure is the first solution to offer SECaaS en mass to network service subscribers. Read more on Allot's solutions for Network Security.

Secure Socket Layer (SSL)

A Secure Sockets Layer (SSL) is the standard security technology for establishing an encrypted link between a web server and a browser. SSL was originally developed by Netscape to allow the private transmission of documents via the Internet.

Security Incident Response

Incident response is a planned approach to addressing and managing the reaction after a cyber attack or network security breach. The goal is to have clear procedures defined before an attack occurs to minimize damage, reduce disaster recovery time, and mitigate breach-related expenses.

Security Operations Center (SOC)

An Information Security Operations Center (ISOC or SOC) is a facility where enterprise information systems (websites, applications, databases, data centers and servers, networks, desktops, and other endpoints) are monitored, assessed, and defended by SOC analysts.

Security Perimeter

A Security Perimeter is a digital boundary that is defined for a system or domain within which a specified security policy or security architecture is applied.

SIEM (Security Information and Event Management)

Security Information and Event Management (SIEM) is a formal process by which the security of an organization is monitored and evaluated on a constant basis. SIEM helps to automatically identify systems that are out of compliance with the security policy as well as to notify the IRT (Incident Response Team) of any security-violating events.

SIM Swapping

SIM Swapping is a scam used to intercept online banking SMS verification codes. To get hold of one-time passwords for financial transactions, cybercriminals create or fraudulently obtain a copy of the victim's SIM card — for example, pretending to be the victim, the attacker might claim to have lost the SIM card and request a new one from the mobile operator. To protect clients from such schemes, most banks require that a replacement SIM card be re-linked to the account.

Sniffing

Packet sniffing allows the capture of data as it is being transmitted over a network. Packet sniffer programs are used by network professionals to diagnose network issues. Malicious actors can use sniffers to capture unencrypted data like passwords and usernames in network traffic. Once this information is captured, the bad actor can then gain access to the system or network.

SOAR (Security Orchestration, Automation and Response)

SOAR (Security Orchestration, Automation and Response) is a solution stack of compatible software programs that organizations use to collect data about security threats from across the network and respond to low-level security events without human assistance.

Social Engineering

Social Engineering is an increasingly popular method of gaining access to unauthorized resources by exploiting human psychology and manipulating users – rather than by breaking in or using technical hacking techniques. Instead of trying to find a software vulnerability in a corporate system, a social engineer might send an email to an

employee pretending to be from the IT department, trying to trick him into revealing sensitive information. Social engineering is the foundation of spear phishing attacks.

Spam

Spam is the name commonly given to unsolicited emails. Essentially unwanted advertising, it's the email equivalent of physical junk mail delivered through the post.

Spear Phishing

Spear Phishing is a phishing scam that targets a specific individual or organization, usually via a personalized email, SMS or other electronic communication to defraud them under the guise of a legitimate transaction.

Spoofing

A Spoof is an attack attempt by an unauthorized entity or attacker to gain illegitimate access to a system by posing as an authorized user. Spoofing includes any act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address.

Spyware

Spyware is software that is secretly installed on a user's device to gather sensitive data. Spyware quietly collects information such as credentials and sends it outside the network to bad actors. Spyware often comes in the form of a free download and is installed automatically, with or without user consent.

Threat Assessment

Threat Assessment is a structured process used to identify and evaluate various risks or threats that an organization might be exposed to. Cyber threat assessment is a crucial part of any organization's risk management strategy and data protection efforts.

Threat Hunting

Cyber Threat Hunting is an active cyber defense activity where cybersecurity professionals actively search networks to detect and mitigate advanced threats that evade existing security solutions.

Threat Intelligence

Threat Intelligence, or cyber threat intelligence, is intelligence proactively obtained and used to understand the threats that are targeting the organization. Trojan Trojans are malicious programs that perform actions that are not authorized by the user: they delete, block, modify or copy data, and they disrupt the performance of computers or computer networks. Unlike viruses and worms, Trojans are unable to make copies of themselves or self-replicate. Read more about Threat Intelligence Solutions.

Two-factor Authentification (2FA)

Two-factor Authentification combines a static password with an external authentication device such as a hardware token that generates a randomly-generated one-time password, a smart card, an SMS message (where a mobile phone is the token), or a unique physical attribute like a fingerprint.

Two-step Authentification

Two-step Authentification is commonly used on websites and is an improvement over single factor authentication. This form of authentication requires the visitor to provide their username (i.e. claim an identity) and password (i.e. the single factor authentication) before performing an additional step. The additional step could be receiving a text message with a code, then typing that code back into the website for confirmation. Alternatives include receiving an email and needing to click on a link in the message for confirmation, or viewing a pre-selected image and statement before typing in another password or PIN.

Virus

A Virus is a malicious computer program that is often sent as an email attachment or a download with the intent of infecting that device. Once the device is infected, a virus can hijack the web browser, display unwanted ads, send spam, provide criminals with access to the device and contact list, disable security settings, scan, and find personal information like passwords.

VPN

A Virtual Private Network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. It is essentially a virtual, secure corridor.

Vulnerability

Vulnerabilities are weaknesses in software programs that can be exploited by hackers to compromise computers.

WAF

A Web Application Firewall (WAF) is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service. By inspecting HTTP traffic, it can prevent attacks exploiting a web application's known vulnerabilities, such as SQL injection, cross-site scripting (XSS), file inclusion, and improper system configuration.

White Hat – Black Hat

White hat – Black Hat are terms to describe the 'good guys' and 'bad guys' in the world of cybercrime. Blackhats are hackers with criminal intentions. White-hats are hackers who use their skills and talents for good and work to keep data safe from other hackers by finding system vulnerabilities that can be fixed.

Whitelist, Allowlist

A Whitelist, allowlist, passlist is a list of permitted items that are automatically let through whatever gate is being used. Worm A Worm is a computer program that installs itself on a victim's device and then looks for a way to spread to other computers, causing damage by shutting down parts of the network. Read more on Allot's solutions for Whitelist/Allowlist.

Zero-day Exploit

This term is used to describe exploit code that has been written to take advantage of a vulnerability before the software vendor knows about it and can publish a patch for it. The result is that would-be attackers are free to exploit the vulnerability, unless proactive exploit prevention technologies have been implemented to defend the computer being targeted by the attacker.

Zero-touch Provisioning or Deployment

Zero-Touch Provisioning (ZTP) is an automatic device configuration process that frees IT administrators for more important tasks. The automated process reduces the possibility of errors when manually configuring devices and slashes the time it takes to set up devices for employee use, often without requiring IT intervention. Users can set up their devices with a few clicks, eliminating the need for administrators to create and track system images or manage

the infrastructure required to push those images to new or repurposed devices. Read more on Allot's solutions for Zero-touch provisioning.