MaximAlert
Technology. Transformation. Trust.

XDR

Extended detection and response (XDR) is a cybersecurity technology that monitors and mitigates cyber security threats.

According to Gartner:

Extended detection and response (XDR) delivers security incident detection and automated response capabilities for security infrastructure. XDR integrates threat intelligence and telemetry data from multiple sources with security analytics to provide contextualization and correlation of security alerts. XDR must include native sensors, and can be delivered on-premises or as a SaaS offering. Typically, it is deployed by organizations with smaller security teams.

—Gartner, 2023 Market Guide for Extended Detection and Response

Enterprises increasingly operate in multicloud and hybrid environments, where they encounter an evolving cyberthreat landscape and complex security challenges. In contrast to targeted systems like endpoint detection and response (EDR), XDR platforms expand coverage to protect against more sophisticated types of cyberattacks. They integrate detection, investigation, and response capabilities across a wider range of domains, including an organization's endpoints, networks, cloud applications and workloads, email, and data stores. They also drive efficiency across security operations (SecOps) with advanced cyberattack chain visibility, AI-powered automation and analytics, and broad threat intelligence.

How can we help?

We can help you learn how XDR solutions vary in maturity, cohesiveness, vision and realization, and see which XDR solution is ideal for your enterprise. Plus, understand the advantages and risks you need to consider before choosing an XDR vendor.

- What criteria can help you evaluate XDR vendors
- Why XDR capabilities vary widely across different vendors
- Which factors to consider when choosing an XDR security solution
-

How to implement XDR

Getting the most value from an XDR platform requires careful planning, from creating a broad XDR strategy to measuring system performance. We at **MaximAlert** can help you with the below steps to help ensure a successful XDR implementation:

- Assess requirements - by evaluating and documenting your organization's specific security requirements. Identify areas of greatest risk, factoring in network size, data types, device types, and access locations. Also consider data protection and other regulations and requirements with which you must comply.
- Goal setting – by creating an XDR strategy and roadmap that support your organization's larger security strategy.
- Due research - Look for a robust XDR platform with advanced AI and automation capabilities and a user-friendly interface providing real-time visibility. Find a solution that is compatible with existing systems and can be quickly deployed and scale to accommodate growing data volumes.
- Implementation Plan - Develop a comprehensive plan for deploying, configuring, and managing the XDR system, including defining associated roles and responsibilities. Outline how to connect the system to existing infrastructure, tools, and workflows. Also, establish storage requirements for logging and telemetry data and create risk-assessment mechanisms for automated alert and incident prioritization.
- Phased rollout - Implement and test the system in stages to minimize operational disruptions. Begin by testing the XDR system with a selection of endpoints before deploying it across the entire technological environment. Once the system is up and running, run through automated scenarios in your incident response playbook and adjust rules as needed.
- Continuous improvement - Regularly build in time to fully assess the XDR system and its baseline data to help ensure accuracy. Also, adjust playbooks and rules as the system takes in more historical data and new cybersecurity risks emerge.

Strategic OEM alliances

MaximAlert
Technology. Transformation. Trust.

EDR

What is EDR?

Endpoint Detection and Response (EDR) is cybersecurity protection software that detects threats on end-user devices (endpoints) in an organization. Across a large, clamorous, worldwide arena of cybersecurity solutions, EDR stands out as a distinct category of telemetry tools that provide continuous monitoring of endpoints to identify and manage adversarial cyber threats such as malware and ransomware.

EDR technology is also sometimes referred to as endpoint detection and threat response (EDTR).

As a cyber telemetry tool, EDR solutions collect data from endpoints as part of threat monitoring and can correlate data from across an entire infrastructure, including its endpoint tools and applications. So EDR tools can be very powerful as threat protection and attack context technologies and formidable endpoint security measures.

How Does EDR Work?

EDR analyzes and monitors all ongoing activities for devices connected to your network and provides real-time threat detection and visibility for automated threat response for security teams for threat hunting.

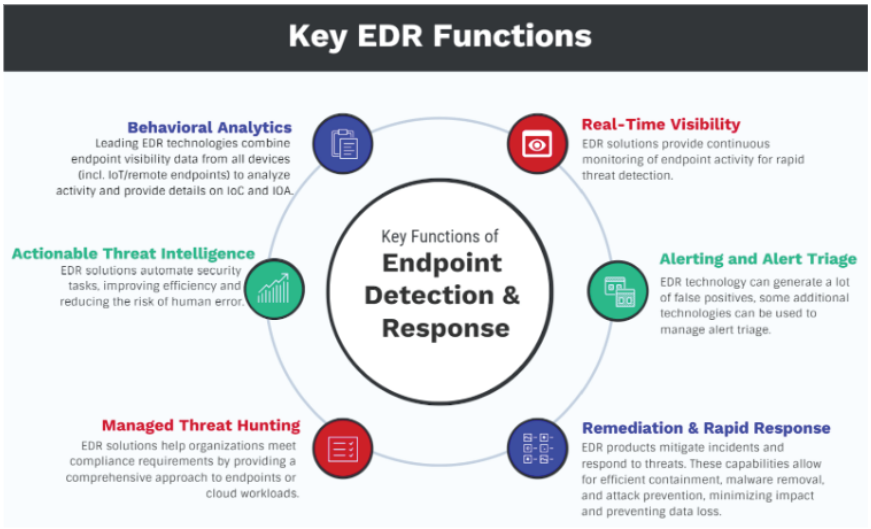
EDR Security: Definition, History, and Fundamental Purpose

EDR Tools were first named in 2013 by Gartner and defined specifically as endpoint protection deployed to:

- Record and store endpoint system-level behaviors
- Use various data analytics techniques to detect suspicious system behavior
- Provide contextual information
- Block malicious activity
- Provide remediation options in response to threats to restore affected systems

MaximAlert
Technology. Transformation. Trust.

EDR technology is a class of endpoint monitoring software that is uniquely trained to detect suspicious and/or anomalous activity on endpoints. Early on, this type of detection immediately separated EDR from antivirus (AV) tools and EPP (Endpoint Protection Platforms) – AV/EPP tend primarily to identify and act on specific signatures and hashes of malware (known-good and known-bad signature instances). AV and EPP solutions block or quarantine known-bad objects and files. But EDR monitors and correlates anomalies and suspicious activity on endpoints, then raises a detection alert with context and severity details that the security teams, cyber threat intelligence teams, and threat hunting teams can use for investigation and remediation/response.



How to Choose the Right EDR Security Vendor

Selecting the right Endpoint Detection and Response (EDR) vendor is critical for organizations looking to bolster their cybersecurity posture. We at MaximAlert can help you with the vital factors to consider to ensure you choose the best EDR security vendor for your needs:

Detection and Response Capabilities

The heart of an EDR system lies in its ability to detect and respond to threats effectively. Assess the vendor's capabilities in identifying a wide range of threats, from malware and ransomware to sophisticated, state-sponsored attacks. Look for advanced features like behavioral analysis, anomaly detection, and AI-driven insights. The system should offer real-time response capabilities, allowing you to quickly isolate infected devices, block malicious activity, and remediate threats.

attacks. Look for advanced features like behavioral analysis, anomaly detection, and AI-driven insights. The system should offer real-time response capabilities, allowing you to quickly isolate infected devices, block malicious activity, and remediate threats.

Integration with Existing Systems

Your EDR solution should seamlessly integrate with your existing security and IT infrastructure. This includes compatibility with other security solutions (firewalls, antivirus, and SIEM systems) and IT management tools. Proper integration enhances visibility across your network and streamlines response efforts. Check if the vendor supports standard integration protocols and provides APIs for custom integrations.

Scalability and Performance

Consider how well the EDR solution can scale with your organization. It should handle an increasing number of endpoints without significant performance degradation. Evaluate the impact of the EDR software on endpoint performance, ensuring it does not interrupt day-to-day operations or reduce system efficiency.

Usability and Management

The usability of the EDR platform is crucial for effective threat hunting and incident response. Look for a user-friendly interface that provides clear, actionable insights. The platform should offer comprehensive reporting and visualization tools for threat analysis and decision-making. Additionally, assess the system's management features, such as policy configuration, alert customization, and automated response actions.

Support and Training

Strong vendor support and comprehensive training are essential to successfully deploying and operating an EDR solution. Investigate the vendor's support structure, including availability, response times, and types of support offered (phone, email, online chat). Inquire about training resources and programs to ensure your team can use and maintain the EDR system effectively.

Reputation and Reliability

Research the vendor's reputation within the cybersecurity industry. Look for independent reviews, customer testimonials, and case studies. Consider the vendor's history, including how long they have been in business, financial stability, and track record for innovation and customer satisfaction.

MaximAlert
Technology. Transformation. Trust.

Compliance and Legal Considerations

Ensure the EDR solution complies with relevant regulations and industry standards, such as GDPR, HIPAA, or PCI DSS. The vendor should provide features that support compliance efforts, including data encryption, access controls, and comprehensive logging and reporting capabilities.

Cost and Return on Investment

Evaluate the total cost of ownership of the EDR solution, including initial purchase costs, implementation fees, and ongoing maintenance expenses. Consider the potential return on investment, factoring in the costs associated with data breaches and cybersecurity incidents. A higher-priced solution may offer more excellent value if it significantly reduces the risk of costly security breaches.

By carefully considering these factors, MaximAlert can help organizations choose an EDR vendor that meets their security needs and aligns with their business objectives, budget, and operational capabilities. The right EDR solution will enhance your cybersecurity defenses, enable rapid response to incidents, and provide valuable insights into threat activities on your endpoints.

Strategic OEM alliances

MaximAlert
Technology. Transformation. Trust.

NDR

What is network detection and response?

Network detection and response (NDR) is an emerging category of cybersecurity solution that ingests and analyzes network traffic to detect suspicious activity and understand security risks and exposure. NDR combines machine learning-powered detections, behavioral analysis, and signature-based detections for known IOCs. Best-in-class NDR solutions also use decryption and protocol decoding to uncover threats hiding in encrypted traffic. Streamlined workflows enable cybersecurity teams to quickly investigate down to packet-level context and respond with confidence.

Like endpoint detection and response (EDR), NDR security solutions do not prevent malicious activity. Instead, they identify attack activity in progress and provide the insight needed to stop attacks before they can do significant harm. NDR is distinct from EDR in that it does not use an agent to monitor east-west and north-south network traffic, relying instead on a network or virtual tap for analysis of network telemetry across on-premises and cloud workloads. NDR is also referred to as network analysis and visibility (NAV) by some independent analyst groups.

WHY CHOOSE NDR?

NDR picks up where other tools leave off

EDR and SIEM provide essential visibility into endpoints and logs, but both tools leave coverage gaps. EDR requires agents to be deployed on each endpoint, but not every endpoint can support an agent. IoT and personal devices are two examples. Sophisticated attackers can also bypass EDR by taking advantage of unmanaged devices — including the 37% of critical devices that are unmanaged. SIEM tools rely on logs, which are useful sources of data, but they lack the context of network packets and attackers can delete logs, wiping away any trace of their activities. Attackers can also avoid firewalls and legacy standalone intrusion detection systems (IDS), but because certain key activities in a successful attack occur on the network, NDR can detect those threats.

NDR complements EDR, SIEM, and IDS/IPS tools by filling coverage gaps and continuously monitoring and analyzing network traffic to provide actionable insight. NDR solutions don’t require agents to understand the ways endpoints, workloads, and services communicate with each other. NDR solutions also provide packet-level context, enabling security teams to dive deeper into the activities of assets and investigate down to ground truth.

MaximAlert
Technology. Transformation. Trust.

Benefits of NDR

NDR solutions offer a range of capabilities that can provide advantages over traditional signature-based threat detection tools. These capabilities include:

Real-time threat detection capabilities - NDR solutions provide real-time monitoring and analysis, enabling quicker identification and response to potential threats. Some NDR tools can also prioritize and raise alerts to security teams or security operations centers (SOCs) based on potential threat severity.

Comprehensive visibility at the perimeter and inside the network - NDR can offer visibility into all network activities on premises and in hybrid cloud environments. This comprehensive visibility can help organizations intercept more security incidents. Because NDR solutions monitor both north-south (exit and entry) and east-west (internal) network traffic, they can detect both intrusions at the network perimeter and lateral movement within the network. The ability to spot anomalies inside the network can help NDR catch advanced threats lying in wait. Some NDR tools can also detect threats hiding in encrypted traffic.

AI-powered threat analysis - NDR leverages AI and advanced machine learning algorithms to analyze network data, identify patterns and spot potential threats, including previously unknown threats that traditional tools often miss.

Automated incident response - Some NDR solutions feature automated response capabilities—such as terminating a suspicious network connection—that can stop an attack as it's happening. NDR tools can also integrate with other security tools to execute more complex incident response plans. For example, after detecting a threat, an NDR might prompt a security orchestration, automation and response (SOAR) platform to run a predefined response playbook.

Integration with threat intelligence - Many NDR tools can integrate with threat intelligence feeds and databases such as the MITRE ATT&CK framework. These integrations can enhance behavioral models and improve the accuracy of threat detection. As a result, NDR tools can be less prone to false positives.

Threat hunting - NDR solutions provide contextual data and functionality that security teams can use for threat hunting activities that proactively search for previously undetected threats.

MaximAlert
Technology. Transformation. Trust.

What Features Should You Look for When Choosing Network Detection And Response Solutions?

Selecting the right Network Detection And Response solution could be crucial for your organization's network security. Having the right platform in place will deliver comprehensive and robust protection. The wrong solution, however, may give you a false sense of security. We recommend looking for the following features when selecting an NDR solution for your organization:

Anomaly Detection: The solution should be able to swiftly identify abnormal network behavior that might indicate a security threat. This includes new behaviors, and those that have been identified in other network systems.

Scalability: The ability to scale up as your organization's network infrastructure expands is crucial. This includes handling increased traffic and additional connected devices. You need to ensure that your platform has the capacity to handle your needs, ensuring that no area is overlooked.

Real-Time Alerts: The NDR solution should be capable of providing real-time alerts about potential security threats. These alerts should be targeted to relevant individuals, ensuring that they have access to the information that they need.

Deep Packet Inspection: It's important that your platform can inspect every detail of incoming and outgoing data to identify threats. If this analysis is not comprehensive, you may inadvertently permit access to dangerous material.

Automated Response: By definition, all NDR solutions should not only detect, but also respond to threats automatically. You need to ensure that this respose capability is effective and robust enough to counter the threats that you are facing. Having a high degree of automation reduces the scope for human error and slow response time.

Integration: The tool should easily integrate with your existing IT infrastructure, including other security tools, for seamless threat detection and response. This will assist in both the threat detection and remediation processes.

MaximAlert
Technology. Transformation. Trust.

Investing in an NDR solution can help secure your network, provide real-time threat detection, and ensure timely responses to any potential attacks. It's important to conduct thorough research when selecting an NDR platform, ensuring that it aligns with your organization's size, needs, and long-term security strategy.

Strategic OEM alliances

MaximAlert
Technology. Transformation. Trust.

Security Analytics

What is security analytics?

Security analytics is a cybersecurity approach that uses data collection, data aggregation and analysis tools for threat detection and security monitoring. An organization that deploys security analytics tools can analyze security events to detect potential threats before they can negatively affect the company's infrastructure and bottom line.

Security analytics combines big data capabilities with threat intelligence to help detect, analyze and mitigate insider threats, persistent cyber threats and targeted attacks from external bad actors.

Benefits of security analytics

Security analytics tools provide organizations with the following key benefits:

Security incident and anomaly detection and response. Security analytics tools analyze a wide range of data types, making connections between different events and alerts to detect security incidents or cyber threats in real time.

Regulatory compliance. Security analytics tools help enterprises comply with government and industry regulations, such as Health Insurance Portability and Accountability Act and Payment Card Industry Data Security Standard. Security analytics software can integrate a variety of data sources, giving organizations a single, unified view of data events across a variety of devices. This enables compliance managers to monitor regulated data and identify potential noncompliance.

Enhanced forensics capabilities. Security analytics tools provide companies insights into where attacks originated from, how their systems were compromised, what assets were compromised and whether there was any data loss. These tools can also provide timelines for any incidents. The ability to reconstruct and analyze incidents can help organizations shore up their cybersecurity strategy to prevent similar incidents from happening again.

Security analytics tools

Security analytics tools detect behaviors that indicate malicious activity by collecting, normalizing and analyzing network traffic for threat behavior.

Providers that specialize in security analytics offer machine learning tools for applying security models to traffic across a company's assets.

Security analytics use cases

Companies can deploy security analytics for a wide variety of reasons. Some common use cases are the following:

- Analyzing network traffic to detect patterns indicating potential attacks.
- Monitoring user behavior, including potentially suspicious activity.
- Detecting potential threats.
- Detecting Data exfiltration.
- Monitoring employees.
- Detecting insider threats.
- Identifying compromised accounts.
- Identifying improper user account usage, such as shared accounts.
- Investigating malicious activity.
- Demonstrating compliance during audits.
- Investigating cybersecurity incidents.

SIEM vs. security analytics

Security information and event management (SIEM) systems collect log data generated by monitored devices -- e.g., network equipment, computers, storage, firewalls, etc. -- to identify specific security-related events occurring on individual machines. They then aggregate this data to determine what's occurring across an entire system. This enables organizations to identify any variations in expected behavior so they can formulate and implement the necessary responses.

Legacy SIEM systems aren't built to handle modern continuous integration/continuous delivery (CI/CD) lifecycles based on frequent build and deployment cycles. As such, they can't handle the massive amounts of data these methods generate.

Unlike legacy SIEM systems, security analytics takes advantage of cloud-based infrastructure. And, since cloud storage providers can provide almost unlimited data storage that can scale according to an organization's needs, the company is not limited by the corporate data storage and retention policies. In addition, security analytics can collect and store data more efficiently. It's also better at handling modern DevOps practices and CI/CD systems.

MaximAlert
Technology. Transformation. Trust.

Big data security analytics

IT security professionals must ensure that their companies' systems are secure, that cyber threat risks are kept to a minimum and that they are complying with data governance regulations. Consequently, one of their primary responsibilities is monitoring and analyzing huge amounts of log and event data from servers, network devices and applications.

Big data security analytics refers to the techniques and strategies used to analyze vast amounts of security data. Big data security analytics can be divided into two functional categories: performance and availability monitoring (PAM) and SIEM.

PAM applications focus on managing operations data, while SIEM tools focus on log management, event management, behavioral analysis, database monitoring and application monitoring.

Big data security analytics tools can discover network devices and automatically collect each device's event and configuration data. Because big data analytics systems require a comprehensive view of the enterprise's security data, they have to integrate with other third-party security tools, as well as Active Directory or Lightweight Directory Access Protocol servers.

How can MaximAlert help in choosing the right platform:

Current state awareness

Be aware about the current state of your security analytics before you get on with selecting the right tool for your enterprise:

- Kind of technologies you’re currently using
- Your concerns and requirements
- Resources and expertise you have
- Do you have Playbooks?

The selection of the type of tool you need may vary with different use cases. There are a number of factors that need to be considered while selecting the right tool.

Size of the Organization

The size of the company and the type of the industry plays an important role in the buying decision. For instance, while a small scale security analytics software might be sufficient for a small to medium scale business, it may turn out to be absolutely useless for a medium to large scale company unless its capabilities can be scaled as the industry grows. Similarly, a large scale security analytics tool may not make sense financially for a small business.

Capabilities of the Tool

Security admins will need to first understand what are the capabilities of these tools. A detailed analysis should be made about what these tools can and cannot do. You should evaluate the objective of the tool based on the following quality metrics rather than the technique used by the tool:

- Anomaly detection — scope, detection and false positive rates
- Incident response — time to detect and time to remediate

Type of Deployment

You also need to consider the type of deployment the software supports. The cost of hardware, software or virtual appliances can factor heavily into which security tool is right for a business. The tool you pick should be designed to support complex architectures and have the capability to scale out to complex service provider scenarios without compromising on the features or the capability of the platform.

Types of Threats Faced by your Industry

Another factor that plays a major role in deciding the right tool is the type of threats a certain industry aces or is most likely to face. Some security analytics vendors specialize in specific types of attacks such as Advanced Persistent Threats (APT) whereas some others specialize in specific sectors such as finance and healthcare. Choose a vendor that caters to your industry specific threats. For example, the education industry may be prone to attacks from actors such as APT groups attempting to gain access to sensitive intellectual property, while organizations in the financial services and insurance sectors face cyber threats from enterprise-like cybercriminals..

Other Capabilities

Security analytics tools also extend the capabilities of other security tools. If they can't integrate with a business' existing tool set, you may want to consider taking a look at another vendor.

MaximAlert
Technology. Transformation. Trust.

Cost of the Tool

Each vendor may charge differently so it is imperative for you to know what you are agreeing to. Many modern tools do not charge you a dime to get onboard. Once you know the upfront cost, your job doesn't end here, you need to look into what the ongoing costs will be like.

We at MaimAlert can help you with all the above and ensure you go with the right Security Analytics platform for your business.

Strategic Technology Alliances

MaximAlert
Technology. Transformation. Trust.

Malware Analysis

What Is an Advanced Persistent Threat (APT)?

An advanced persistent threat (APT) is a covert cyber attack on a computer network An Advanced Persistent Threat (APT) refers to a complex and covert cyber-attack executed by highly skilled threat actors, usually targeting high-profile organizations. APTs are often backed by nation-states or criminal organizations and can remain undetected within the victim's network for extended periods, ranging from months to years.

The primary objective of an APT attack is to infiltrate a network without authorization and maintain persistent access, while collecting valuable data or compromising vital systems. Organizations and governments face significant risks from these attacks, as they can result in considerable losses, including financial damage, tarnished reputations, and stolen sensitive data.

Who would launch an APT attack?

Numerous entities--large and small, public sector and private--can benefit from a successful advanced persistent threat. Many suspect that governments and nation states have used APT attacks to disrupt specific military or intelligence operations. Examples include the Titan Rain, Ghostnet, Stuxnet attacks and others. In addition, smaller groups are using simpler tools, such as social engineering, to gain access and steal intellectual property.

Why would someone launch an APT?

A successful advanced persistent threat can be extremely effective and beneficial to the attacker. For nation states, there are significant political motivations, such as military intelligence. For smaller groups, APTs can lead to significant competitive advantages or lucrative payouts.

Unique Characteristics of Advanced Persistent Threats

APTs are distinguished from other cyber threats by their unique characteristics, which include:

- **High level of sophistication:** APTs are characterized by their use of advanced tools, tactics, and techniques that are designed to evade detection and bypass security measures. This often involves custom malware, zero-day exploits, and advanced social engineering tactics.

Targeted attacks: APTs are usually aimed at specific organizations, industries, or countries. The attackers carefully select their targets based on strategic objectives, such as stealing intellectual property, compromising critical infrastructure, or gaining a competitive advantage.

State sponsorship or well-funded organizations: APTs are often attributed to nation-states or well-funded criminal organizations that have the resources, expertise, and motivation to carry out these advanced attacks.

Long-term approach: APTs are typically designed for long-term operations, with the attackers focusing on maintaining a persistent presence within the target network. This allows them to gather intelligence, exfiltrate data, or cause damage over an extended period.

Multi-stage and multi-vector: APTs usually involve multi-stage attacks that progress through various phases, such as reconnaissance, weaponization, delivery, exploitation, installation, command and control, and execution. Attackers may use multiple vectors to achieve their objectives, including spear phishing, supply chain compromise, and watering hole attacks.

Examples of Advanced Persistent Threats Attacks

Here are some recent examples of Advanced Persistent Threat (APT) attacks:

SolarWinds: The SolarWinds cyberattack was a significant supply chain attack attributed to APT29 (Cozy Bear), a Russian-state-sponsored APT group. The attackers compromised the SolarWinds Orion software platform, used by thousands of organizations for IT infrastructure management. This enabled the threat actors to infiltrate the networks of multiple high-profile targets, including U.S. government agencies and Fortune 500 companies.

Hafnium: Microsoft discovered a Chinese-state-sponsored APT group called Hafnium, which targeted Microsoft Exchange Server vulnerabilities to gain access to email accounts and exfiltrate sensitive data. Hafnium is known to target organizations in various sectors, including defense, healthcare, and higher education.

MaximAlert
Technology. Transformation. Trust.

UNC2452 / Nobelium: An APT group also involved in the SolarWinds attack, continued its cyber-espionage campaign targeting various organizations. In May 2021, Microsoft disclosed that Nobelium had launched a new wave of attacks using the USAID email system to distribute malicious phishing emails.

APT41: A Chinese-state-sponsored APT group which targeted various industries worldwide, including healthcare, telecommunications, and higher education. In 2020, the U.S. Department of Justice (DOJ) charged five Chinese nationals for their involvement in APT41 activities, including unauthorized access to protected computers and stealing sensitive information.

How can we help in your fight against APT

When organizations detect gaps in their security, they intuitively deploy a standalone product to fill that void. A solution filled with standalone products, however, will continue to have inherent gaps.

To avoid these gaps in security, organizations need to take a holistic approach. This requires a multilayered, integrated security solution. Deploying a portfolio of products that can seamlessly work together is the best way to enhance security.

We work with strategic vendors like Trellix, Trend Micro, Checkpoint, Palo Alto to name a few, who can help in protection against APT using a multi-layered approach.

To know more about APT campaigns:

https://www.mandiant.com/resources/insights/apt-groups

Strategic Technology Alliances

MaximAlert
Technology. Transformation. Trust.

Web and Email Security

What Is Web Security?

Web security is a broad category of security solutions that protect your users, devices, and wider network against internet-based cyberattacks—malware, phishing, and more—that can lead to breaches and data loss. It reduces the security risk to your organization when your users accidentally access malicious files and websites through some combination of sandboxing, URL filtering, and various other security and access controls.

What's the Purpose of Web Security?

The massive importance of the internet for modern enterprises—and the accompanying growth in the sophistication, frequency, and impact of cyberattacks—has made web security critical to business continuity. It's your first line of defense against threats that can lead to the exposure of sensitive data, costly ransoms, reputational harm, compliance violations, and a host of other consequences.

Once the domain of mostly small-time hackers, internet-borne threats have evolved into a massive black market business that touches the worlds of organized crime as well as state-sponsored espionage and sabotage. Some of the latest threats are incredibly sophisticated, able to easily fool the untrained eye or bypass legacy security. Plus, with an array of ready-made tools, exploit kits, JavaScript modules, and even fully developed campaigns for sale, even a novice actor can easily launch an attack.

Cybersecurity Ventures estimates that, by 2025, global cybercrime will cost US$10.5 trillion annually—a greater profit than the entire world's major illicit drug trade—and half the world's data will live in the cloud. Given what's at stake, it's easy to see why effective web security is so important today.

What Are the Benefits of Web Security?

For a modern enterprise, effective web security has broad technical and human benefits:

- Protect your business and stay compliant by preventing loss of sensitive data
- Protect customers and employees by securing their private information
- Avoid costly service interruptions by preventing infections and exploits
- Offer a better user experience by helping your users stay safe and productive
- Maintain customer loyalty and trust by staying secure and out of the news

MaximAlert
Technology. Transformation. Trust.

Great strides in cloud and mobility technology let your employees and customers connect with you with unprecedented ease and flexibility. Unfortunately, that cuts both ways, and attackers have more ways to approach your organization's wider attack surface. With the right web protections in place, you can spend more time taking advantage of the benefits, and less worrying about security threats.

What Does Web Security Protect Against?

Web security casts a wide net to protect users and endpoints from malicious emails, encrypted threats, malicious or compromised websites and databases, malicious redirects, hijacking, and more. Let's look at a few of the most common threats in more detail:

- Ransomware: These attacks encrypt data, and then demand a ransom payment in exchange for a decryption key. In a double-extortion attack, your data is also exfiltrated.
- General malware: Countless variants of malware exist that can lead to anything from data leaks, spying, and unauthorized access to lockouts, errors, and system crashes.
- Phishing: Often carried out through email, text messages, or malicious websites, these attacks trick users into things like divulging login credentials or downloading spyware.
- SQL injection: These attacks exploit an input vulnerability in a database server, allowing an attacker to execute commands that let them retrieve, manipulate, or delete data.
- Denial of service (DoS): These attacks slow or even shut down a network device such as a server by sending it more data than it can process. In distributed DoS—that is, a DDoS attack—this is carried out by many hijacked devices at once.
- Cross-site scripting (XSS): In this type of injection attack, an attacker introduces malicious code to a trusted website by entering it in an unprotected user input field.

How can MaximAlert help?

- We work with leading secure web gateway vendors that provide on-premise as well as cloud-delivered solutions, so it enforces security policies consistently, no matter where users connect, what endpoint devices they're using, or where applications are hosted.
- Our partner vendor solutions are built on a global multitenant cloud architecture for massive scalability, so it can inspect all encrypted traffic without degrading performance.
- Additionally, our partner vendors provide an integrated, cloud native platform that greatly reduces your operational complexity and costs.

MaximAlert
Technology. Transformation. Trust.

Email Security

What is Email Security?

Email security is the practice of protecting email accounts and communications from unauthorized access, loss, or compromise. Organizations can enhance their email security posture by establishing policies and using tools to protect against malicious threats such as malware, spam, and phishing attacks. Cybercriminals target email because it is an easy entry point to other accounts and devices—and it relies in large part on human error. All it takes is one misguided click to cause a security crisis for an entire organization.

Why is email security important?

Email has been a primary communication tool in the workplace for more than two decades. More than 333 billion emails are sent and received daily worldwide—and employees get an average of 120 emails a day. This spells opportunity for cybercriminals who use business email compromise attacks, malware, phishing campaigns, and a host of other methods to steal valuable information from businesses. Most cyberattacks—94 percent—begin with a malicious email. Cybercrime cost more than USD$4.1 billion in 2020, with business email compromise causing the most damage, according to the FBI's Internet Crime Complaint Center (IC3). The consequences can be severe, leading to significant financial, data, and reputational losses.

The benefits of email security

Businesses of all sizes are realizing the importance of prioritizing email security. An email security solution that safeguards employee communication and reduces cyberthreats is important because it helps to:

- Protect a company's brand, reputation, and bottom line. Email threats can lead to devastating costs, operational disruption, and other severe consequences.
- Enhance productivity. With a robust email security solution in place, businesses can reduce potential disruptions to operations and downtime because of a cyberattack. An effective solution helps security teams streamline response and stay ahead of increasingly sophisticated threats.
- Ensure compliance with data protection laws such as the General Data Protection Regulation (GDPR) and help circumvent the many intangible costs of a cyberattack such as business disruption, legal fees, regulatory fines.

MaximAlert
Technology. Transformation. Trust.

Email security best practices

In response to the fast-changing email threat landscape, enterprises have established email security best practices to support communication and guard against threats. Top email security best practices include:

- Educate employees with periodic training to minimize the risk of human error and ensure that employees—often considered a company's first line of defense—understand the importance of email security.
- Invest in user awareness training so users can learn how to recognize the signs of a phishing attack and other indicators of malicious intent.
- Upgrade to an email security solution that provides advanced threat protection.
- Implement multifactor authentication (MFA) to prevent account compromise. Asking users to provide more than one way to sign into accounts is an easy way to help secure organizational data.
- Review protections against business email compromise attacks through methods like spoofing and impersonation.
- Move high-risk processes and transactions to more authenticated systems.

Types of email threats

- Data exfiltration: Data exfiltration is the unauthorized transfer of data from an organization either manually or through malicious programming. Email gateways help make sure businesses avoid sending sensitive data without authorization, which could lead to a costly data breach
- Malware: Malware is short for malicious software, and its primary aim is to damage or disrupt computers and computer systems. Common types of malware include viruses, worms, ransomware, and spyware.
- Spam: Spam is an unsolicited message sent in bulk and without the recipient's consent. Businesses use spam email for commercial purposes. Scammers use spam to spread malware, trick recipients into divulging sensitive information, or extort money.
- Impersonation: Impersonation occurs when cyber criminals pretend to be a trusted person or organization to secure money or data via email. Business email compromise is one example in which a scammer impersonates an employee to steal from the company or its customers and partners.
- Phishing: Phishing is the practice of pretending to be a trusted person or organization to trick victims into disclosing valuable information such login credentials and other types of sensitive data.

MaximAlert
Technology. Transformation. Trust.

How can MaximAlert help with email security services

Email security services help companies protect email accounts and communication from cyberthreats. The best way for companies to implement email security is to create and maintain a policy for using email and share that with employees so they are aware of email security best practices, Common email security services available for individuals, schools, communities, and organizations include:

- Detonation capabilities that scan incoming, outgoing, and internal email for malicious links and attachments.
- Data encryption to secure mail communications from being intercepted by cybercriminals.
- Image and content control capabilities to scan attached or embedded images and content for malware and blocks them from being downloaded.
- Spam filters that filter unwanted email like bulk and spam messages.
- Authentication systems to evaluate the validity of senders.

Strategic Technology Alliances