Digital Security
Progress. Protected.

PREVENTION FIRST:

5 Ways to Stop an Attack Before It Starts

Prevention First: 5 ways to Stop an Attack Before It Starts

1-10-60 Security experts recommend meeting the 1-10-60 rule: 1 minute to detect, 10 minutes to investigate and 60 minutes to remediate.

CHANGING THREAT-ACTOR TACTICS CALL FOR MULTIPRONGED PREVENTION

As of five years ago, the most notorious and damaging cyberattacks were launched and spread purely by fully automated software payloads. As cyber defenses evolved to prevent them, threat-actor tactics predictably shifted. Today, the most damaging cyber incidents are more likely to be interactive, human hands-on-keyboard attacks in which an intruder succeeds in infiltrating the network.

Multilayered prevention that works across all levels of the computing environment greatly lowers the likelihood that adversaries can gain a toehold and also limits the damage they can cause. It makes the difference between a security team that spends the majority of its time on remediation and recovery from attacks and one that has the time to proactively monitor the network, detect intrusions and block them early on.

Here, we look at the various points when preventive measures come into play.

25% of malicious cyberattacks leave systems inoperable, while 24% involve ransomware.[1]

PREVENTION AT THE ENDPOINTS

Endpoint protection has evolved beyond simple malware prevention or the so-called "next-gen antivirus." Modern endpoint platforms apply behavioral analysis to investigate whether a sample is malicious, apply artificial intelligence to investigate and more accurately classify suspicious samples at scale, and integrate with other security tools and technologies to make the entire effort more seamless and manageable.

Look for an endpoint protection platform that:

- Goes beyond signature-based detection by applying behavioral analysis and stopping fileless exploits executed via scripts
- Continuously updates and communicates in real time to guard against new, late-breaking threats
- Applies multiple layers of protection, including scanning network traffic and blocking suspicious files on removable drives
- Protects and manages multiple operating systems and mobile devices, as well as desktops, laptops and servers, all from a single pane of glass

82% of breaches involve data stored in the cloud, whether public or private. In 39% of breaches, attackers gained access to multiple cloud environments.[1]

PREVENTION IN THE CLOUD

Organizations that use the cloud for storage and access to applications can't take the security of those platforms for granted. While Microsoft and Google do provide some security tools, a full-featured security solution that offers multiple layers of protection will safeguard cloud-hosted email, collaboration and storage.

Look for an integrated cloud email security or cloud-native, API-enabled email security solution that:

- Combines spam filtering, anti-malware scanning, anti-phishing and behavioral analysis
- Is easily managed through a central console that issues notifications and provides access to information about detected threats
- Automatically scans all new and changed files in shared online storage to stop malware from executing or spreading between devices

1 Ponemon Institute, Cost of a Data Breach 2023

15% of breaches are triggered by compromised or stolen credentials as the initial attack vector. These incidents take the longest time to resolve, at 328 days.[1]

PREVENTION AT LOGINS

With compromised credentials available for sale on the dark web and individuals reusing passwords and otherwise practicing poor password hygiene, logins are a point of vulnerability that can easily bypass endpoint prevention measures. Multifactor authentication (MFA) protects against misuse of credentials for individual user logins and is also recommended for administrative access to network resources.

Look for an MFA solution that:

- Works smoothly on all Android and iOS smartphones and integrates with device biometrics
- Supports push authentication for one-tap user convenience, without having to re-key the one-time password
- Natively supports virtual private networks, Remote Desktop Protocol, Outlook Web Access, VMware Horizon View and RADIUS-based services
- Supports hard tokens in addition to SMS when extra security is required.

5% of breaches originate from known vulnerabilities that have yet to be patched.[1]

PREVENTION AT THE OS AND APPLICATION LEVELS

With nearly 200,000 published common vulnerabilities and exposures (CVEs) and multiple thousands more added every year, keeping up with patching systems is a colossal burden for IT departments, which often fall behind due to more pressing issues and resource shortages. Automated vulnerability detection, patch application and management can keep systems protected against exploits and lift the burden.

Look for a vulnerability and patch management solution that:

- Automatically scans systems and installed applications for vulnerabilities and applies patches according to a defined patching strategy
- Prioritizes the most critical vulnerabilities and assets for immediate patching while allowing others to run at off-peak times to minimize disruption
- Supports and tracks exceptions for selected applications
- Provides comprehensive reporting and tracking of patches, including name, CVEs, severity/importance and affected applications

1 Ponemon Institute, Cost of a Data Breach 2023

2/3 of breaches are reported by a benign third party or attackers. Only one-third are discovered by the targeted organizations' internal security teams.*

* Ponemon Institute, Cost of a Data Breach 2023

PREVENTION ACROSS THE NETWORK

The role of an extended detection and response (XDR) solution is primarily to detect, investigate and thwart attacks that have successfully penetrated the network, but it has a key role in prevention as well. It detects suspicious activity early on and provides security analysts with tools to shut down an attack, as well as allowing them to investigate newly uncovered potential threats and verify that the environment is well defended against them.

Look for an XDR solution that:

- Works well with and is tightly connected to the endpoint protection platform
- Includes a library of detection rules for speedy initial setup
- Detects patterns of related activity and automatically flags them by creating cyber incidents for investigation
- Blocks lateral movement with one-click isolation from the rest of the network
- Allows for filtering of raw data to support automated threat hunting

About ESET

AI-NATIVE PREVENTION FOR TOMORROW'S THREATS

Stay one step ahead of known and emerging cyber threats with our **AI-native, prevention-first approach**. ESET combines the power of AI and human expertise to make protection easy and effective.

Developed over 30 years, ESET's best-in-class protection is powered by our **in-house global cyber threat intelligence**, including our **extensive R&D network** led by industry-acclaimed researchers.

ESET PROTECT, our scalable, cloud-first XDR cybersecurity platform combines next-gen prevention, detection and proactive threat-hunting capabilities with a wide range of security services, including **managed detection and response** (MDR). Our highly customizable, integration-ready solutions support all deployment methods, include local support and have minimal impact on performance. They identify and neutralize known and emerging threats before they can be executed, support business continuity, and reduce the cost of implementation and management.

Our mission isn't just to stop attacks in their tracks; it's to prevent them from ever happening. ESET protects your business so you can unlock the full potential of technology.