Prevention first:

How Proactive Defense Can Minimize the Attack Surface and Close Compliance Gaps

Digital Security
Progress. Protected.

Table of Contents

Introduction

The following paper will explore exactly what risks organizations are facing across multiple threat vectors. And it will explain how a multi-layered prevention-first strategy could work in practice.

As IT complexity increases and threats continue to grow in volume and sophistication, the best way to manage these challenges is from a single, unified platform and pane of glass. When change is the only constant, finding a cybersecurity partner you can trust will be critical.

The world is changing fast. And technology is the agent of this change—transforming how global businesses work and interact with their customers. Across virtually all verticals, the direction of travel is cloud-first services, applications and infrastructure. It is distributed IT environments designed to support agile remote working. And increasingly, it is AI-driven innovation designed to optimize productivity and deliver outstanding customer experiences.

But the cost of this digital transformation is a quickly expanding cyberattack surface. Emails inboxes, endpoints, SaaS applications, mobile devices, networks and other assets present growing targets for threat actors. Many organizations are struggling to manage a dynamic set of risks. One estimate claims that one in 10 internet-facing assets had an associated unpatched vulnerability in 2023, and that 70 billion files were exposed to potential theft or ransomware. Another reveals that over half (52%) of organizations don't know how much of their attack surface is secured—and **none are confident that they are fully in control of that attack surface.**

More than

52%

of companies

don't know how much of their attack surface is secured.

Threat actors thrive in these conditions. Just five years ago, the most serious cyberattacks were delivered via fully automated software payloads. But as defenses evolved, offensive tactics did, too. Today, the most damaging threats are hands-on-keyboard attacks, which may involve sophisticated social engineering, fileless malware and more. **Network defenders must evolve their threat protection, detection and response efforts in tandem.**

WHAT DOES THAT MEAN IN PRACTICE?

A prevention-first approach comprised of multiple layers will reduce the chances of an adversary gaining a foothold in the corporate network, and limit the damage they can cause if they do. That will **shift the focus** for security teams **from remediation and recovery to proactive network monitoring**, intrusion detection and attack surface risk management.

A proactive, prevention-first approach will help organizations to:

- **Mitigate the risk from advanced threats such as ransomware, zero-day threats**
- **Identify and neutralize emerging threats before they can be executed**
- **Lay foundations for a zero-trust framework**
- **Reduce costs and impact of potential data breaches**
- **Minimize the time security teams spend on incident response and remediation**
- **Close compliance gaps and meet rigorous cyber-insurance requirements**
- **Ensure business compliance**

Layering Up Protection Across Attack Vectors

Organizations are faced with daily attempts to steal sensitive internal, customer or employee data, hijack IT assets or encrypt critical systems. With the help of unified cloud platforms, they must mitigate these cyberthreats across multiple facets of their attack surface.

ENDPOINT

The endpoint represents the intersection of human and machine. That makes it a popular target for attack, as threat actors look to exploit vulnerabilities in endpoint devices/machines, or human fallibility (via phishing), to gain a foothold into networks. Fileless malware is particularly dangerous as it doesn't leverage traditional executable files—meaning there's no signature for traditional AV to detect. A 2023 study recorded a 1400% increase in these attacks over a six-month period.

1 PREVENTION AT THE ENDPOINT LEVEL

Endpoint protection must go beyond traditional AV to feature AI-powered behavioral analysis, which can help stop fileless exploits executed via scripts. Such technology can investigate and classify suspicious samples at scale to streamline threat prevention. Look for solutions that **continuously update in real time** to protect against new threats, and **apply multiple layers of protection**, including network traffic scanning and blocking of threats on removable drives. Endpoint protection should also work across multiple operating system and machine or device types, including desktops, laptops and servers.

Detecting vulnerabilities and eliminating them, or mitigating their exploitation, by installing the latest patches for apps and operating systems remain crucial prevention measures. Actively tracking and fixing vulnerabilities across all your endpoints is a relatively time-consuming task, and IT teams tend to fall behind with patching. Organizations should prevent any potential risk caused by postponed patching, and **seek an automated solution** that continuously detects vulnerabilities and simplifies the patching process by prioritizing critical assets across all applications and operating systems.

ESET OFFERS *ESET offers various, truly next-gen endpoint security capabilities. ESET LiveGuard® Advanced delivers proactive defense against zero-day and never-before-seen threat types, leveraging cloud sandboxing to analyze and isolate suspicious files en masse, and at speed. ESET Endpoint Security works across Windows, macOS and Linux—preventing file-based malware attacks, detecting malicious activity and providing investigation and remediation for rapid response to dynamic security incidents. ESET Vulnerability and Patch Management actively tracks vulnerabilities in operating systems and apps, delivering automated or manual patching across all endpoints to close security gaps and meet compliance requirements.*

MOBILE

The trend toward hybrid and remote working means that more users are accessing corporate resources from their mobile devices. But these are increasingly targeted with phishing attacks and mobile malware, and are at higher risk of loss or theft. One 2023 report recorded malware on 1 in 20 Android devices, and claimed 80% of phishing sites now target mobile devices.

2 PREVENTION AT THE MOBILE LEVEL

Organizations need multi-layered protection that works across all their corporate devices. Where possible, it should include **anti-theft** (including remote wipe and lock), **app control**, **web security** and **anti-phishing**, as well as the ability to remotely **enforce password policies**, and more. All of this must be manageable from a single console for enhanced visibility and control.

ESET OFFERS *ESET Mobile Threat Defense works across Android and iOS, and features cloud-based malware prevention and AI-powered multi-layered defenses—all managed from a single point with unparalleled performance. There's also support for multiple mobile device management (MDM) options for easy onboarding and fleet-wide protection.*

CLOUD PRODUCTIVITY APPS AND EMAIL

Email continues to be a popular conduit for threats such as phishing attacks, advanced ransomware, business email compromise (BEC) and more. In fact, phishing was the most common initial access vector in data breaches in 2023.

The most popular cloud email and productivity platforms, Microsoft 365 and Google Workspace, include a host of cloud-based productivity applications such as cloud storage and collaboration, which can be targeted for data theft and extortion.

Organizations shouldn't rely on the cloud providers' native security controls alone to keep them safe.

3 PREVENTION AT THE CLOUD APP AND EMAIL LEVEL

Best practice dictates enhancing Microsoft's or Google's built-in controls with dedicated, multi-layered protection for cloud-hosted email, collaboration and storage. **Integrated cloud email security** or a cloud-native, API-enabled email security solution should include **spam filtering**, **anti-malware scanning**, **anti-phishing** and **behavioral analysis**. It will automatically scan for any new and changed files in shared storage to prevent malware from executing or spreading. And ideally, it should be manageable from a single, centralized console.

ESET OFFERS *ESET Cloud Office Security provides advanced protection for Microsoft 365 and Google Workspace apps. New users are automatically protected by advanced adaptive scanning, cutting-edge machine learning, cloud sandboxing and in-depth behavioral analysis.*

4 PREVENTION AT THE ON-PREMISES EMAIL LEVEL

Organizations that, for various reasons, still operate on-premises mail servers must deploy comprehensive anti-phishing, anti-spam and anti-malware protections **to filter unsolicited or malicious messages**. In addition, they need to protect the server as a host. The best solutions combine AI with human expertise, and feature support for clustering, which allows products to communicate with each other and exchange configurations, notifications, greylisting and more, for enterprise-grade protection.

ESET OFFERS *ESET Mail Security provides advanced protection for MS Exchange servers, powered by 64-bit technology for accelerated email threat prevention. It also supports businesses that utilize Microsoft Exchange in a hybrid setup.*

HARDWARE & DEVICES

As endpoints proliferate, so does the attack surface. And very often, it's corporate data that threat actors are after. They may attempt to compromise machines via vulnerability exploitation, or—more frequently—by using legitimate credentials. Such a breach could cost, on average, $4.5m today, and risk the wrath of regulators.

5 PREVENTION AT THE HARDWARE LEVEL

Organizations can put in place layered protection, but it's not 100% foolproof. If the worst-case scenario does occur, they also need **strong encryption of data** to render it useless to any would-be thief. This will also help to ensure compliance with GDPR, CCPA and other regulations and cyber insurance requirements. Organizations should look for a solution that applies 256-bit Advanced Encryption Standard (AES) to system disks, partitions and entire drives—ensuring that nothing is exposed. For ease of administration and utility, it should work across Windows/macOS, and enable management of multiple devices from a single console.

ESET OFFERS *ESET Full Disk Encryption delivers powerful FIPS 140-2 validated 256-bit AES for system disks, partitions or entire drives. Single-click deployment and centralized management take the strain off IT teams whilst delivering peace of mind.*

IDENTITY

Increasingly, threat actors are dispensing with malware and vulnerability exploitation altogether, and using legitimate credentials to impersonate users and glide past endpoint defenses. One report notes a 71% annual increase in the volume of attacks using valid credentials and accounts in this way.

These credentials are often bought on the dark web, or stolen with infostealing malware. There was a 266% increase in use of the latter in 2023, according to the same report. The work of threat actors is made easier because of password reuse and poor password management.

6 PREVENTION AT THE IDENTITY LEVEL

Multifactor authentication (MFA) is essential in preventing credential misuse, especially on privileged or administrative accounts. Solutions should support **mobile-based, one-tap authentication** that works seamlessly across Android and iOS devices, integrating with biometrics and supporting push authentication to enhance the user experience. Native support for network access, VPNs, Remote Desktop Protocol (RDP), Outlook Web Access, VMware Horizon View and RADIUS-based services would also enhance back-end efficiency. Comprehensive MFA solutions should also work with hardware tokens if the organization uses them.

ESET OFFERS *ESET Secure Authentication offers a one-touch, mobile-based MFA solution. Setup is easy, as no hardware is required. There's support for a variety of authentication methods, including mobile applications, push notifications, hardware tokens, FIDO security keys and custom methods.*

Go Beyond Endpoints Protection with XDR

Alongside protection at each of these points across the attack surface, organizations should consider the value of Extended Detection and Response (XDR). Contrary to popular belief, these capabilities aren't just designed to accelerate incident detection and response. They can also form part of a proactive, prevention-first approach. That's because their detections can reveal poorly configured systems, unpatched vulnerabilities and hidden threats—enabling organizations to take prompt action and build cyber-resilience. The benefits of XDR are:

- **Increased visibility into the company network**
- **Deeper investigations of security incidents, advanced threats and targeted attacks**
- **More efficient monitoring of unusual and suspicious incidents and activities**
- **More accurate execution of incident response**
- **Support of proactive threat-hunting, to stop attacks before malware is deployed**

ESET OFFERS ESET Inspect delivers unique behavior- and reputation-based detection, providing real-time insight to security teams, based on threat intelligence provided by the global ESET LiveGrid® Reputation System. It's capable of detecting and blocking advanced persistent threats, fileless attacks, zero-day threats, ransomware and corporate policy violations.

The Power of MDR

Managed Detection and Response (MDR) services free up customers' in-house teams to work on higher-value tasks. In so doing, they support not only accelerated threat detection and response, but also a prevention-first strategy, by revealing security weaknesses and blocking suspicious behavior and applications. MDR helps organizations to:

- **Strengthen security readiness with immediate threat detection, investigation and response capabilities with cybersecurity expertise**
- **Achieve cost-efficient, always-on, 24/7 expert-led threat hunting**
- **Reduce costs of maintaining in-house skilled workforces while minimizing the incident response times to minutes**
- **Get ready for compliance; EDR/XDR and MDR are becoming critical components of cybersecurity insurance and regulatory requirements**

ESET OFFERS ESET offers managed services for SMB and Enterprise customers. ESET MDR and ESET Detection & Response Ultimate are 24/7 threat management services, using AI and human expertise to deliver world-class ransomware protection without the need to maintain in-house security specialists. Depending on the required level of service, ESET provides access to experienced threat hunters who deliver proactive Threat Hunting and Threat Monitoring.

Conclusion: Why Unified Prevention Matters

Global organizations are struggling to contain risk across an expansive attack surface, which continues to grow with hybrid work and digital transformation investments. The answer is to **proactively focus on prevention**. Why? Because it will minimize the operational costs associated with threat detection or incident response, and optimize the productivity of security operations teams.

> **When an attack is prevented by the endpoint protection platform, analysts can spend time investigating how the threat penetrated their other lines of defense instead of cleaning up a mess at the endpoint.**

Source: *Forrester: The Forrester Wave™: Endpoint Security, Q4 2023.* Paddy Harrington, October 19, 2023.

The best way to operationalize prevention-first cybersecurity is via a single platform. This will ensure:

- **Fewer security silos between products, and fewer potential gaps in protection**
- **Cost savings on licenses that would otherwise be spent on point products**
- **A lower administrative burden for stretched security teams (as there's only one product/UI to learn)**
- **More efficient SecOps (less swivel-chair work)**

The **ESET PROTECT Platform** delivers exactly these benefits through a comprehensive range of next-generation threat prevention capabilities unified into a single offering.

It draws on ESET's three decades of experience in cybersecurity R&D and cutting-edge global threat intelligence to provide **seamless, automated protection across multiple attack vectors**. It is designed to combine high detection rates with low false positives and minimal IT impact, to **minimize the attack surface and regulatory risk,** and enhance business continuity.

Find out what makes **ESET's PROTECT Platform** a perfect fit for your business.

LEARN MORE

AI Native Prevention for Tomorrow's Threats

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

eset
Digital Security
Progress. Protected.