ZERO TRUST: THE KEY TO UNLOCKING VALUE FROM SECURITY PROJECTS

Digital Security
Progress. Protected.

Author: **Phil Muncaster**

March 2023

Table of Contents

Introduction

One of the great truisms of cybersecurity is that organizations are only as strong as their weakest link. It's often a user. But it could also be unpatched endpoint, a misconfigured cloud account, a poorly enforced policy, or any number of other elements. The challenge for CISOs is that as IT modernization efforts continue, the number of potentially weak links threatens to grow. In this context, legacy security tools and approaches are no match for today's threat actors.

Your adversaries have another major advantage: they only need to get lucky once – putting the odds in their favor from Day Zero.

This is not just a theoretical risk. Across the globe, hacktivists, financially motivated cybercrime groups and state-backed operatives are waltzing past traditional defences with ease. Continuous cybercrime innovation and collaboration has put tools and knowledge once confined to a few APT groups in the hands of the masses. And at the same time, digital transformation and changing working patterns are expanding the corporate attack surface.

In short, there are more ways than ever to compromise your organization, and more threat groups ready and willing to do so. One vendor blocked 64 billion cyber threats in the first half of 2022 alone. The stakes for getting cybersecurity wrong are also rising. An average breach costs nearly $4.4 million globally today, but rises even higher in some jurisdictions. The top five regions were the US ($9.4m), the Middle East ($7.5m), Canada ($5.6m), the UK ($5.1m) and Germany ($4.9m).

So if legacy approaches are failing, what is the answer? Even organizations with big budgets are at a heightened risk of suffering a serious security breach – often because of failures of basic cyber hygiene such as poor patch management. That's why an idea first touted over a decade ago is now beginning to take root inside organizations: Zero Trust. With a US Presidential mandate behind it, the momentum is beginning to build among federal government agencies and suppliers – with more organizations likely to follow around the world.

ESET not only helps to support Zero Trust deployment for customers through its products and services – we also rely on the model to mitigate serious financial, reputational and regulatory risk for our own business.

We know Zero Trust inside out, and in this paper we'll explain:

1. how the approach works
2. why its popularity is finally surging
3. how your organization can get started

What is Zero Trust?

In 2009, Forrester developed a new information security model, called the Zero Trust Model, which has gained widespread acceptance and adoption.

The central idea is that no internal or external entity should be trusted unless authenticated. Instead, anyone who wants to enter the network from the outside must prove that they are doing so via the correct, secured path, and that they are also the person they claim to be.

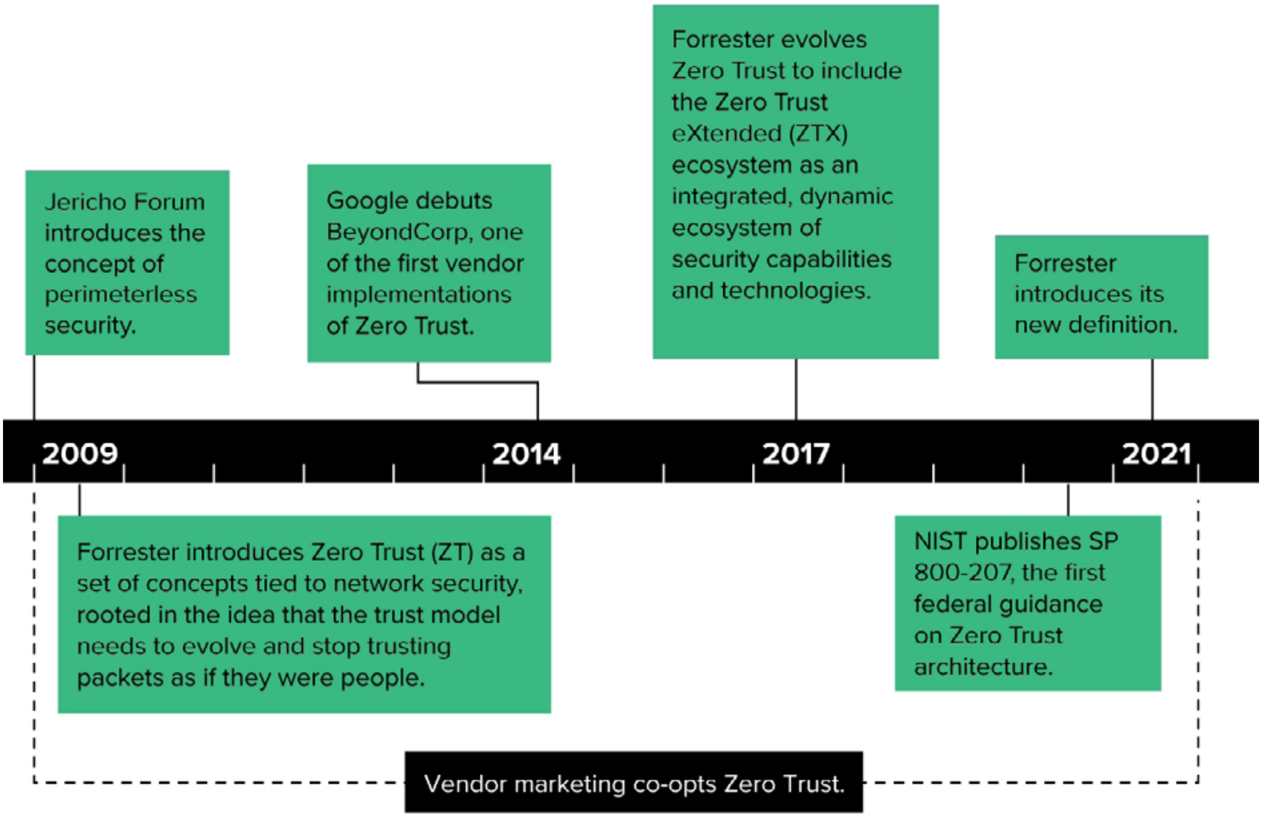
Security professionals must continually audit and secure all resources, restrict and strictly enforce access controls, and rigorously audit and log network traffic. This is often boiled down to the mantra: “never trust always verify,” and is centered around three core principles:

TREAT ALL NETWORKS AS UNTRUSTED

This should include the home and public Wi-Fi networks used by remote workers, as well as local corporate networks. Threat actors are too capable of accessing these networks for us to assume they are safe. In fact, under Zero Trust, there are no longer any “trusted zones” to secure. Instead, security must be applied to every entity interacting with enterprise resources.

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

If all networks are untrusted, then all users must be too. Even legitimate accounts and “identities” may have been hijacked by malicious actors. Employees should be given just enough permissions and time to do tasks specific to their roles – and no more. Thereafter, access rights should be reviewed regularly and any rights that are no longer appropriate should be removed periodically.



Jericho Forum introduces the concept of perimeterless security.

Google debuts BeyondCorp, one of the first vendor implementations of Zero Trust.

Forrester evolves Zero Trust to include the Zero Trust eXtended (ZTX) ecosystem as an integrated, dynamic ecosystem of security capabilities and technologies.

Forrester introduces its new definition.

Forrester introduces Zero Trust (ZT) as a set of concepts tied to network security, rooted in the idea that the trust model needs to evolve and stop trusting packets as if they were people.

NIST publishes SP 800-207, the first federal guidance on Zero Trust architecture.

Vendor marketing co-opts Zero Trust.

Source: "The Definition Of Modern Zero Trust", Forrester, January 24, 2022

ASSUME BREACH

Breaches are inevitable. A cursory look in the media will reveal new compromise virtually daily. You should therefore cultivate a culture of vigilance, backed by Zero Trust controls, policies and processes.

Early iterations of Zero Trust were heavily network focused. But the approach has evolved over the years to become more holistic. At its heart is the critical enterprise data or business processes that must be protected. You must then consider four key related elements:

1. **The people who access that data**
2. **The devices that store and access it**
3. **The networks the data flows through**
4. **The workloads (data and applications) which power modern businesses**

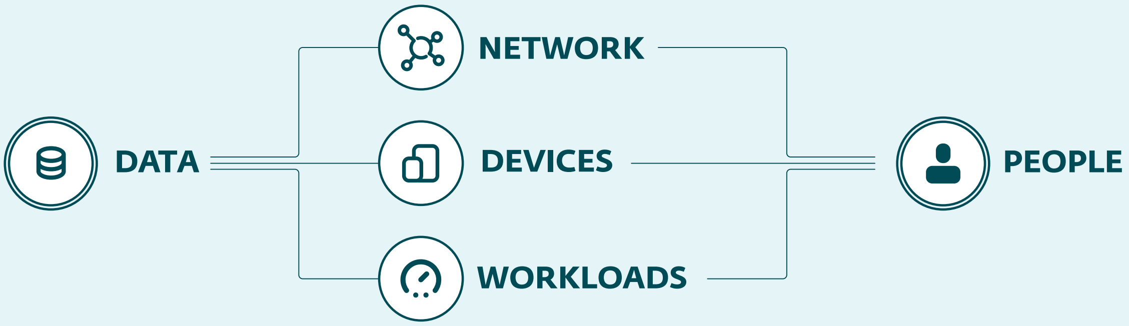
Forrester now also argues for an additional automation and orchestration layer integrated into all control points – to monitor and analyze traffic and events in real time, and make automated data-driven decisions to enforce policy. This supports continuous verification throughout the user journey, rather than once at the perimeter, and means your organization can be more agile, adaptive and dynamic in how it handles Zero Trust security.

HOW CAN ZERO TRUST BENEFIT YOUR ORGANIZATION?

With the Zero Trust model, your organization could derive several key benefits that include:

- Comprehensive and continuous protection against all threat types including APTs, ransomware and more
- Enhanced IT security on your company's own network and the external devices of remote workers
- Consistent protection of data and applications on your network and in the cloud
- Reduction of security gaps through continuous risk monitoring and mitigation

Thanks to these benefits, Zero Trust can help to mitigate the risk of financial and reputational damage stemming from a serious security breach. By providing greater assurance about the security of IT systems and processes – and delivering dynamic, automated controls – it can also drive user productivity and digital transformation projects.



Why we need Zero Trust now

Zero Trust was originally born out of a growing concern about the unsuitability of the classic perimeter model of security. This "castle-and-moat" approach posits that no one on the outside of a network can access its resources, but everyone on the inside can. It was suited to a simpler time when enterprise networks were largely contained within the four walls of the corporate office – and perimeters were therefore fixed and clearly defined.

However, as far back as 2004, CISOs were growing increasingly anxious about the "de-perimeterization" of modern IT architectures. It's why a group of security leaders formed the Jericho Forum – an organization devoted to enhancing risk mitigation in the face of dissolving network boundaries and open, cloud-based systems. It promoted new ways to "secure assets where they are" through encryption, authentication, secure protocols and more. In many ways, it was the genesis of Zero Trust.

WHY DIDN'T IT CATCH ON FOR A LONG TIME?

However, it took several years before Zero Trust caught on. That's down to several factors:

1. Many IT teams were overwhelmed by the complexity of Zero Trust requirements
2. Companies didn't have the technical and financial resources to adopt the model
3. Cyber-attacks were not as sophisticated then as they are today – meaning organizations didn't have a strong enough reason to change the status quo
4. A misunderstanding about what Zero Trust meant in this context led some would-be proponents to reject it. Some mistakenly thought the model was an implicit critique of employees – that they couldn't be "trusted" to be secure

Other more pragmatic issues also played a part in Zero Trust's slow uptake and implementation in the years' immediately following its introduction. These included the fact that, under the model:

- **All data sources and services are considered resources** – but identifying all of these in an organization is challenging, especially when they are continuously being created and destroyed
- **Least privilege governs all access to data and applications** – but defining the necessary permissions for each user can be problematic, and runs the risk of impeding user productivity and the user experience (UX) if IT teams get it wrong
- **Access to resources is granted on a per-session basis** – but what happens when sessions are temporarily halted before specific actions/ tasks are completed? Or when tasks have to be interrupted at short notice but the session then stops automatically as a result?
- **Access to resources is determined by dynamic policies** – but organizations often didn't have the right tools to set and enforce these policies
- **Organizations must collect as much data as possible to continuously improve their security posture** – but this requires extra budget for sufficient storage space, tools and manpower

THE RIGHT MODEL AT THE RIGHT TIME

These calculations have changed somewhat in recent years – thanks to an evolving threat landscape, changes to the way companies work, and innovations in corporate security technology. These factors have made Zero Trust an increasingly attractive option for mitigating corporate risk.

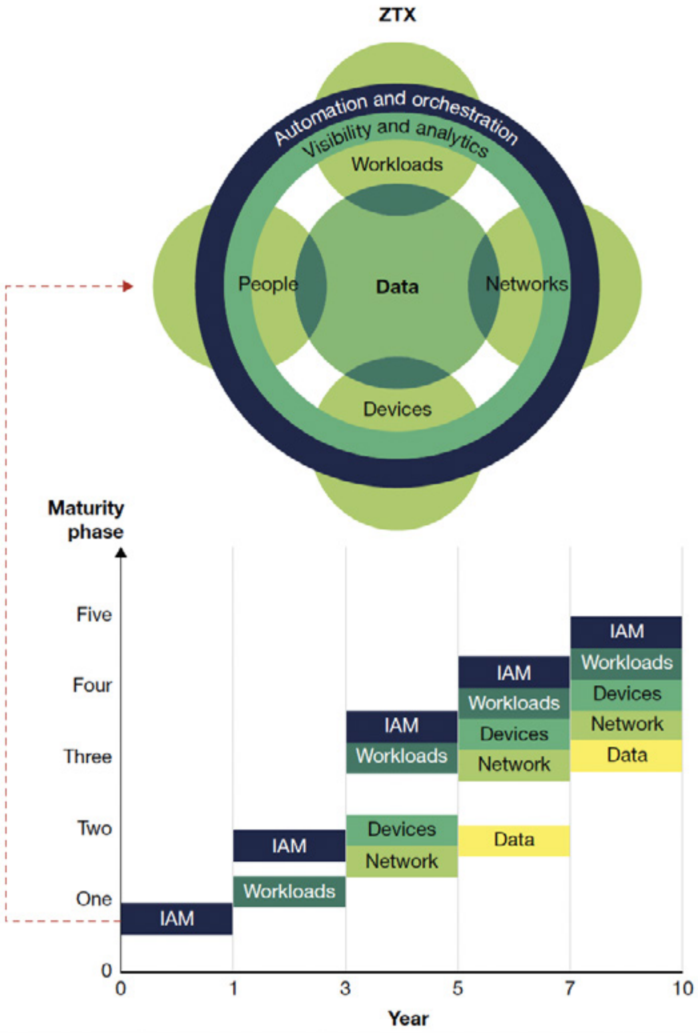
THE NEW HYBRID WORKING WORLD

Take the corporate IT environment. Times have changed considerably since the days when "castle-and-moat" security was the preeminent model. After the digital disruption the pandemic forced on the world – accelerating digital transformation in some sectors by several years – today's organizations are more reliant on cloud and mobile computing. These fluid, distributed IT environments couldn't be a better fit for Zero Trust – a model based on the premise that workers could be located anywhere, and networks can be local, in the cloud or a blend of the two.

Hybrid working practices are increasingly the norm in many sectors, with 68% of global workers preferring to work partially remotely. Yet home working can also add security risk for your organization, because:

- Distracted home workers are more likely to fall for phishing links
- Personal laptops and devices, home networks, and smart home devices may be less well secured than their corporate equivalents
- Vulnerable Virtual Private Networks (VPN) and other unpatched software may be running on home systems
- Poorly configured Remote Desktop Protocol (RDP) connections on endpoints could be hijacked via leaked or easily guessed passwords
- Cloud services with weak access controls (poor passwords and no multi-factor authentication) represent an attractive target for threat actors

Organizations are also investing in emerging technologies like IoT and edge computing to gain an advantage in a post-pandemic world. This all creates additional risk, expanding the cyberattack surface and providing more opportunities for threat actors. According to one study, over two-fifths (43%) of global organizations believe their attack surface is "spiralling out of control."



The Zero Trust Maturity Phases
A Practical Guide To A Zero Trust Implementation. Forrester, 2021.

THE THREAT LANDSCAPE EVOLVES

Second, threats are also evolving to the point that no organization of any size and in any sector is safe today. Ransomware is a good example. An "as-a-service" model distributed via dark web sites has lowered the barriers to entry for many budding cybercrime groups. Some pre-purchase network access to enterprise victims from other third parties on the cybercrime supply chain, known as initial access brokers (IABs). Or they might buy enterprise credentials from a readymade supply on the dark web, or else target phishing emails to steal them – still a popular technique for password theft. They use legitimate tools to stay hidden inside networks whilst exfiltrating data and deploying the ransomware payload. It's a slick, streamlined business that generates billions of dollars annually.

CISOs know they need to respond. But a global industry shortfall of 3.4 million security professionals is limiting their ability to do so. In fact, skills shortages perpetuate misconfigurations in the cloud, arguably one of the biggest security risks today. Patching vulnerabilities has also become virtually impossible without automated risk-based systems. There were over 20,000 CVEs disclosed in 2021 – a record high. But coverage isn't 100% even with the right tools, due to endpoint visibility gaps.

TECHNOLOGY ADVANCES, ZERO TRUST COMES OF AGE

Organizations are struggling to manage these challenges. The average time taken to identify and contain a breach now stands at 277 days, or around nine months. But increasingly they know that Zero Trust can help to mitigate the risk of future breaches – and any financial and reputational damage, including regulatory fines, that may result. In the first instance, Zero Trust can help to prevent unauthorized access to sensitive data and networks. And then, if malicious actors do get through defenses, it can limit the "blast radius" of attacks and quickly alert SecOps teams.

Your efforts to adopt Zero Trust are helped by a proliferation of emerging technologies that deliver critical capabilities – like encryption, multi-factor authentication, and security analytics. Key here is finding tools to continuously monitor your environment, spot suspicious events and then automate a response in line with policy – such as revoking access to a user/device or preventing lateral movement. This is where advanced detection and response tools/services can help.

How EDR supports Zero Trust

Endpoint detection and response (EDR) tools automatically detect suspicious behavior and security vulnerabilities within your network, by intelligently monitoring/evaluating all activities in the IT environment – including user, file, process, registry, storage and network operations. They supplement traditional anti-malware by using behavioral analysis to spot more advanced threats that legacy tools may miss, such as APTs and zero-day exploits.

Thus, EDR may detect suspicious activity – such as changes to files, logs and executed services – in real time, flag it for further inspection and/or trigger an automated response to stop an attack in its tracks. In so doing, it greatly restricts attacker options and provides serious firepower to enforce the "never trust, always verify" mantra. EDR can also be used to support post-attack forensic investigations – which can be an important method of enhancing cyber resilience going forward..

Getting started

Gartner predicts that by 2025, at least 70% of new remote access deployments will use Zero Trust Network Access (ZTNA) rather than traditional VPNs, up from less than 10% at the end of 2021. But access is just one piece of the puzzle. Zero Trust can be a complex undertaking, with no clearly defined end state. There is no single set of check box capabilities that can be easily followed to magically deliver your organization Zero Trust "compliance." Zero Trust is an approach rather than a standardized framework, which means it must evolve over time.

However, on the positive side, you may already be using many of the tools and techniques needed to get started in those five critical areas that underpin Zero Trust. These include the following:

People: Roles-based access controls, multi-factor authentication and account segregation top the list for managing human-shaped risk.

Workloads: Use cloud providers' native controls to reduce access to different workloads and enforce good policies. Cloud security gateways, workload asset management tools, and container/VM security configuration solutions are also useful.

Devices: Start with asset management to gain insight into what your environment looks like. Turn on endpoint security like host-based firewalls, EDR and mobile security to protect these assets and prevent lateral movement.

Networks: Micro-segmentation is a critical piece of the puzzle. Use network devices like routers and switches in combination with access control lists (ACLs) to limit who and what can talk to different parts of the network. Vulnerability management and network device configuration management are also important.

Data: Classify your data effectively then apply encryption to the most sensitive types at rest and in transit. File integrity monitoring and data loss prevention can enhance risk mitigation further.

On top of these efforts, add security orchestration and automation, and data analytics capabilities, to deliver situational awareness to SecOps and support a streamlined, real-time response to mitigate new risks.

Conclusion

According to one study, 41% of global organizations have plans to adopt Zero Trust and are in the early stages of doing so. An additional 39% have already begun rolling out Zero Trust solutions. They see the model as an important bulwark against cyber risk amidst continued digital transformation – and therefore critical to the future success of their organization.

While beginning the journey can be an intimidating prospect, it doesn't need to be if you tackle it in bite-sized pieces. Consider these three final tips:

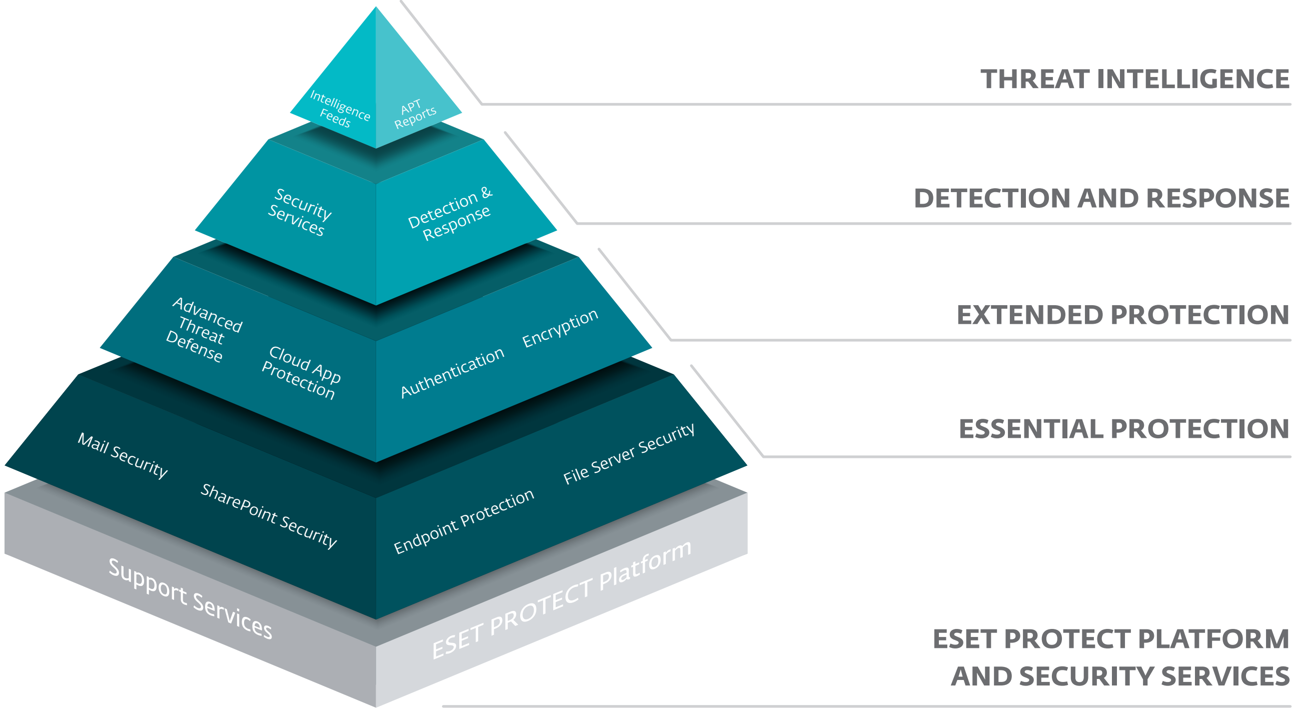
1. **Gain visibility:** Identify the devices, resources, assets and access points you want to protect and monitor. This visibility is crucial because you can't protect what you can't see.

2. **Set policies:** Take time to develop the right policies – with as much granular detail as possible. These will sit at the beating heart of your Zero Trust strategy. For example, set controls that allow only certain people to access certain resources under certain conditions.

3. **Automate as much as possible:** This will ensure policies are applied correctly and enable the organization to quickly respond to any policy non-compliance.

Improve your posture with ESET

The ESET PROTECT Platform enables you to significantly strengthen your cyber control. See how the individual technological protections from ESET help you build a formidable, highly resilient security stack.



THREAT INTELLIGENCE

Not necessarily a mandatory part of the Zero Trust model, but in case you want to get our best research to work for you, this is the best way. In-depth and actionable intelligence from ESET's world-renowned lab, provided via feeds and reports, which will fortify your organization against APTs, botnets, and other types of attacks.

DETECTION AND RESPONSE

Maximum protection, complete cyber risk management, and granular visibility into your IT environment via ESET's most comprehensive detection and response. Access world-leading expertise via ESET MDR and XDR via ESET Inspect. ESET experts help you fine-tune your security posture and provide 24/7 threat monitoring.

EXTENDED PROTECTION

Cloud-based threat defense against targeted attacks and new threat types, especially ransomware, plus dedicated protection for cloud office suites. Improved data and identity with easy-to-use multi-factor authentication and encryption solutions to harden access protection.

ESSENTIAL PROTECTION

Multiple layers of prevention and detection, leveraging ESET's unique technologies, which work together to protect your organization's endpoints, file servers, mail servers, and SharePoint. It includes a hardened browser and specialized controls to deflect RDP compromise. It also includes Mobile Device Management (MDM).

ESET PROTECT PLATFORM AND SECURITY SERVICES

Access tailored support appropriate to your needs, plus deployment and configuration assistance. ESET PROTECT, ESET's unified security management platform, delivers XDR and threat-hunting capabilities. It also enables you to implement a zero trust approach for the highest level of cybersecurity.

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide.

ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

To find out more about how ESET can help to advance your Zero Trust journey, please visit:
ESET enterprise page

Digital Security
Progress. Protected.