Extending Zero Trust to Every Endpoint

LevelBlue

An Evolving Threat Landscape

Organizations are experiencing massive growth in the number of employee devices connecting to the corporate network. The increase in hybrid and remote work presents a unique challenge for both endpoint and network security strategists. Companies are reevaluating how they grant access to corporate data and applications for employees across different locations and devices.

This effort is further complicated by the continuously evolving threat landscape and recent increase in compliance requirements. Endpoint devices continue to be a top target for attacks, with phishing attacks becoming increasingly frequent in number and more difficult for users to identify. Social engineering attacks including phishing account for **54%** of security events according to a recent ESG survey.

Unmanaged devices in a bring-your-own-device model (BYOD) create additional complexity when managing how corporate applications and data is accessed by employees. Security teams often lack centralized visibility across the corporate network and various endpoint types. As organizations seek to ensure secure access, they must adopt a zero trust strategy.

75%

of organizations have experienced at least one cyberattack caused by an unknown, unmanaged, or poorly managed device.[1]

Zero Trust Challenges

Growing number of devices connected to the corporate network

Threats targeting endpoint devices are increasing in complexity and frequency

Siloed endpoint and network security tools and teams

Identifying the right solutions for your organization

Transforming your strategy to meet compliance requirements

As threats evolve, so must your **security strategy**

1. ESG Research Report: Managing the Endpoint Vulnerability Gap

What is Zero Trust?

Zero trust is a security framework that eliminates the concept of implicit trust within an organization's network. Instead, it requires every user, device, and system to be continuously assessed for risk based on the user identity and context.

A common misconception is that zero trust describes a single product or tool that delivers secure access, but zero trust is not a single technology. Zero trust is a strategic approach and requires alignment between tools and teams.

Zero trust relies on two core principles:

- **Least privilege access:** Employees are granted access to the data and applications they need in alignment with their identity and role.
- **Continuous assessment of risk:** Zero trust requires continuous monitoring and assessment of trust levels, using this context to determine user access.

Zero trust is built on the idea **"never trust, always verify,"** which means that trust is never assumed, even for those already inside the network.

Four Key Areas of Zero Trust

1. Visibility and Inventory

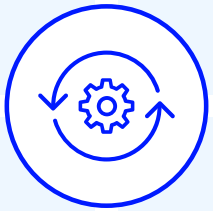
Inventory hardware devices, applications, and other assets that access corporate IT systems.

Assess current security posture.

2. Microsegmentation

Isolate workloads and set up granular security controls.

Employ next-gen firewall, segmentation, or other technology to set up micro-perimeters.



3. Least Privilege Access

Enforce context-based least privilege access policies.

Incorporate strong user authentication controls.

4. Continuous Monitoring

Incorporate technology that enables continuous assessment of risk and trust levels.

Use continuous risk assessment to determine user access.

The Role of Network Security in Zero Trust

Zero trust network access (ZTNA) is an important technology in a zero trust strategy which applies "never trust, always verify" at the network level. It replaces traditional VPN technology with a more secure, identity-based approach that grants users access to specific applications or resources rather than the entire network. ZTNA brings together multiple network security controls, including next-generation firewall and identity and access management capabilities, to deliver secure access for users regardless of location.

ZTNA protects sensitive data through perimeter controls, internal network monitoring, and continuous user authentication and authorization, in order to prevent unnecessary lateral movement.

A mature zero trust strategy incorporates ZTNA along with web application and cloud access technologies to bring security controls closer to the data being accessed. ZTNA is part of security service edge (SSE) solutions that also include next generation firewall capabilities, secure web gateway (SWG) and cloud access security broker (CASB). Together, these technologies deliver secure access regardless of location.

In addition to these network security technologies, endpoint device protections are increasingly important for organizations experiencing massive growth in the number of users and endpoints. Supplementing SSE solutions with a comprehensive endpoint security strategy enables zero trust to be realized at every access point across the network, device, and application levels.

Network Security Tools for Zero Trust

Next-Gen Firewall and Microsegmentation

Monitor network traffic and set up access controls

Identity and Access Management Solutions (IAM)

Identify users who connect to the corporate network

Zero Trust Network Access (ZTNA)

Ensure secure authentication for users from any location

Threat Detection and Response

Incorporate behavioral monitoring, including network detection and response (NDR)

The Role of Endpoint Security in Zero Trust

It's not enough to have protections only at the network level. Continuous verification at the endpoint and application layer monitoring are essential for comprehensive security.

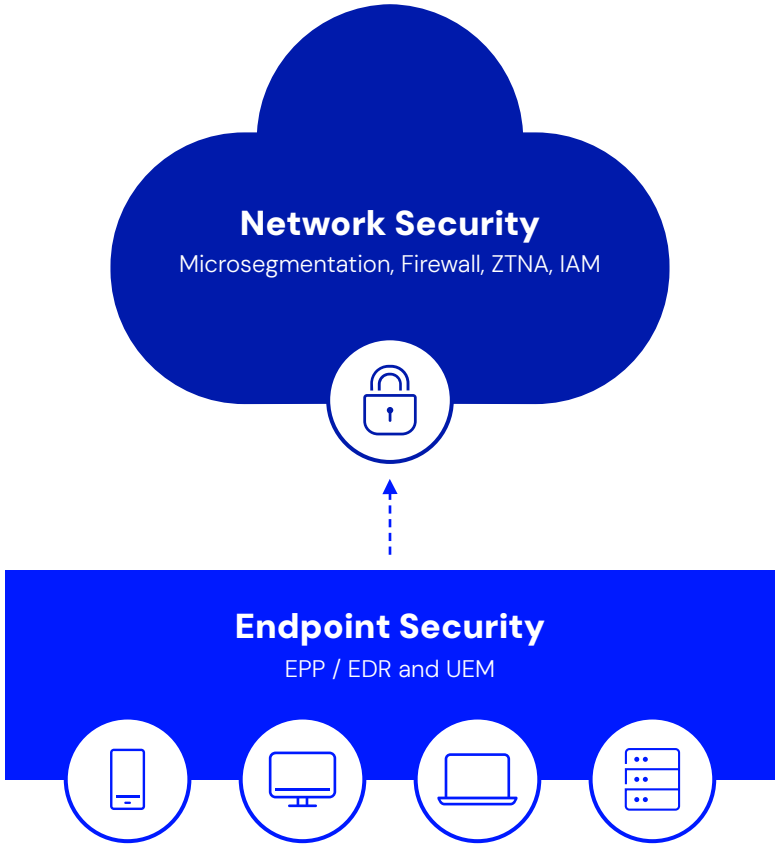
Incorporating endpoint security is essential to gain visibility across mobile devices, workstations, and the cloud, and protect against threat actors targeting these endpoints. This requires continuous monitoring at the device and application levels.

Endpoint Security Technologies that Enable Zero Trust

Endpoint Protection Plaforms (EPP):
Endpoint protection platforms (EPP) protect laptops, desktops, and servers with a suite of anti-malware, data loss prevention (DLP), and encryption tools. Modern EPP solutions incorporate endpoint detection and response (EDR) capabilities to continuously monitor endpoints for suspicious behavior and rollback infected endpoints.

Unified Endpoint Management (UEM):
Unified endpoint management (UEM) tools deliver centralized visibility across laptops, IoT, and mobile devices to more easily manage policies. When paired with mobile threat defense (MTD), this enables enhanced protection that proactively targets key mobile threats including phishing attacks.

Bringing Together Network and Endpoint Security to Deliver Zero Trust



Protect sensitive data wherever it is accessed, with network monitoring, strong authentication controls, and endpoint security at the device and application levels.

How Endpoint Security Plays into your Zero Trust Strategy

Incorporating endpoint security into your zero trust model can be a complex task. To begin, it is important to take an inventory of current assets, policies and procedures before determining what additional tools will best meet your organization's needs.

Benefits of a Unified Endpoint and Network Security Strategy

- Greater visibility across network, devices, and apps
- Protect sensitive data at the network and device level
- Address security gaps through seamlessly layering solutions
- Support a unified security strategy across teams

Incorporating Endpoint Security Into Your Zero Trust Strategy

ANALYZE

Take an inventory of all endpoints and existing security tools

Analyze and refine current access policies

ADOPT

Incorporate UEM and EPP across all managed devices

Employ strong authentication controls and context-based secure access for unmanaged devices

OPTIMIZE

Integrate SSE and IAM for granular visibility and identity management

Continuously assess risk and use risk evaluation to determine user access

LevelBlue Unifies Your Zero Trust Strategy

By integrating multiple security layers, LevelBlue helps deliver the next evolution of zero trust security that ensures robust, end-to-end protection across your entire digital landscape.

LevelBlue offers a full suite of network security solutions, designed with flexibility in mind to meet you where you are in your journey to zero trust. From next-generation firewall to security service edge (SSE) solutions, LevelBlue simplifies your network security strategy with unparalleled expertise and customized solutions.

In addition to helping secure your network, LevelBlue delivers a suite of endpoint security solutions to address threat exposures at every endpoint. LevelBlue Managed Endpoint Security with SentinelOne delivers advanced endpoint detection and response for workstations and cloud workloads, complete with 24/7 monitoring and threat hunting by the LevelBlue SOC.

When it comes to zero trust, creating a scalable strategy is more easily said than done. With unparalleled expertise in the industry, LevelBlue helps simplify your journey towards zero trust through expert consulting services and flexible security solutions.

Why LevelBlue?

- Comprehensive suite of managed network security solutions
- Fully managed endpoint security with 24/7 threat hunting and monitoring
- White-glove onboarding and deployment services
- Partnerships with industry-leading technology vendors
- Consulting services including zero trust readiness workshop

Enable Zero Trust With LevelBlue

LevelBlue Network Security

1. Microsegmentation
2. Firewall
3. Managed Zero Trust Network Access (ZTNA)
4. Security Service Edge (SSE)

LevelBlue Endpoint Security

1. Unified Endpoint Management (UEM)
2. Mobile Threat Defense (MTD)
3. Endpoint Protection Platform (EPP)
4. Endpoint Detection and Response (EDR)

LevelBlue Zero Trust Readiness Assessment

LevelBlue Consulting offers a zero trust readiness assessment and workshop designed to help organizations evaluate their current security posture and associated risks, and design a phased zero trust approach aligned with business goals.

LevelBlue analyzes an organization's security posture across users, network, devices, and cloud workloads in order to identify gaps and develop a roadmap. LevelBlue consultants deliver actionable recommendations tailored to your organization that address planning, budgeting, prioritization, time management, and implementation of strategic initiatives required to achieve zero trust.

Benefits

Align

Understand key risks, challenges, and connectivity/ security needs

Prioritize

Identify gaps in alignment with zero trust approach and capture opportunities for growth

Plan

Receive actionable recommendations and timelines for your zero trust strategy

Zero Trust Readiness Assessment

Benefit from expert guidance at every step in your zero trust journey

1

Discovery

Discover current state and information security program

Understand security posture and current risks

2

Capabilities Assessment

Analysis of people, process and technology respective of six pillars of zero trust

Analysis of tools and technologies

3

Maturity Assessment

Conduct maturity assessment for each pillar

Provide maturity assessment overview across pillars

4

Strategy and Roadmap

Develop a phased, programmatic approach aligned with zero trust architecture and concepts

Present findings and target next phase

5

Execution Support

Provide execution management and oversight as needed

vCISO or other team members as needed

Through partnerships with leading technology vendors, LevelBlue uniquely delivers a comprehensive set of network and endpoint security solutions to solve customer challenges around planning and implementing a zero trust strategy. Our advisory and support services help simplify secure access and data protection across an organization's entire attack surface.

LEARN MORE

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

LevelBlue