WHITEPAPER

Endpoint Security in an Age of Digital Transformation

LevelBlue

Your Network is Changing

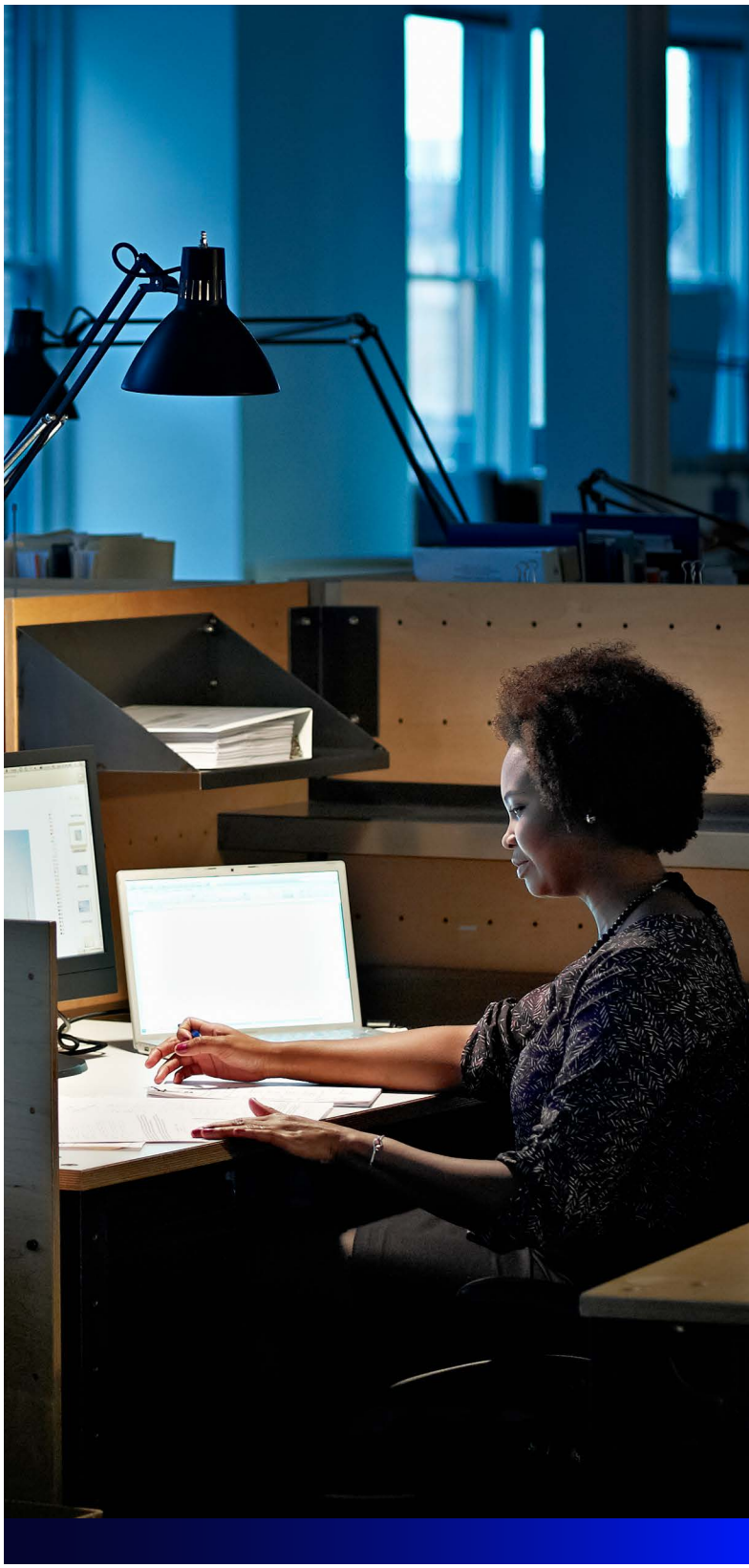
Success in today's digital age demands that organizations transform with confidence and speed. Organizations that understand how changes to the network, endpoints, and business operations may impact their cyber risk posture are well-positioned to innovate faster and with greater confidence. In this whitepaper, we will explore elements of digital transformation that most impact the endpoints and the security elements to help protect them.

Factors Accelerating Transformation

5G

5G brings ultra-fast speeds and ultra-low latency to deliver unprecedented connectivity for data-intensive applications. This includes highly interactive video, augmented/virtual reality (AR/VR), artificial intelligence (AI), and many other new and emerging technologies that are driving digital transformation across industries. 5G also provides robust reliability for supporting mission-critical apps and services. But these capabilities have also made it possible for a massive increase of new devices to connect to a single network, creating more endpoints that need to be protected.

Understanding what new endpoints are being introduced into a network and the type of access they have will be important. But possibly less obvious, the fast speeds and low latency can also work to the advantage of cybercrime. Once an endpoint is compromised, if a threat is not identified quickly, it could move laterally across a business network at machine speed causing exponential damage.



Public Cloud and Cloud-First

Another factor driving digital transformation that impacts endpoints is the use of public cloud infrastructure. This adoption was accelerated by the pandemic which forced many CIOs to face their fears around cloud adoption head-on. Public cloud adoption has clearly crossed the chasm and gone mainstream as organizations across industries and of all sizes realize the benefits of scalable, on-demand infrastructure for their business workloads.

Securing those cloud IaaS resources remains a top concern and challenge for enterprises. In the past, confusion about security and the delineation of responsibility between the customer and cloud service provider (CSP) reigned. The industry has taken steps to promote the Shared Responsibilities Model, which aims to balance cloud accountability between the provider and its users. Yet, the headlines illustrate there is still much work that lies ahead in securing cloud instances and containers. It is incumbent on organizations to take steps in securing these critical facets of their business operations.

Containers, Kubernetes, and Microservices

Just as public cloud adoption has gone mainstream, so too, perhaps unsurprisingly, has the use of cloud containers. Containers and microservices go hand-in-hand, so to understand the uptake of containers is to understand how microservices have played a role in digital transformation.

Microservices are an architectural approach to application development that accelerates innovation. Simply put, a large monolithic business application is broken down into various components, each with its own innovation cadence. For example, an e-commerce site might have microservices for the product catalog, shopping cart, payment portal, and so on. A team of developers can add items to the product catalog whenever they need, and push that update to a cloud image which in turn spawns a container running in the cloud without having to wait on the developers in charge of the payment portal to push their next release. Each team of developers operates independently at the release cadence of their choosing, without slowing the other down. In this way, innovation is accelerated, and the business can more easily adapt to market changes and opportunities.

So microservices can accelerate business agility, and each microservice runs from its own container. But what about the deployment and scaling of all those containers to meet the demand load placed on the app where it originates? Enter Kubernetes, an open-source container orchestration platform. Google developed Kubernetes (K8s) in-house to simplify container management and then donated it to the open-source community (CNCF).

To further simplify container orchestration, Google Cloud, Amazon Web Services (AWS), and Azure each offer their own managed Kubernetes services. Now businesses of all sizes have an even easier path to container orchestration, which leads to more rapid innovation and execution of its business strategy. For this reason, it is important not to overlook securing these critical endpoints from cyberattacks. Cybercriminals see these new cloud containers as potential weak spots to target.

Edge Compute

When people hear the term “edge compute,” self-driving cars are often the main use case that comes to mind. However, there are many use cases for this technology, with more emerging every day. Edge compute is as it sounds. It involves moving the compute power as close to the data source, or the edge, as possible. This extends cloud ecosystems and brings cloud services closer to the endpoints. By bringing the computing power to the edge, companies can dramatically reduce latency, which will ultimately usher in the next generation of applications that will further transform business operations and the customer experience.

Today, around 10% of enterprise-generated data is created and processed outside a traditional centralized data center or cloud. By 2025, Gartner predicts this figure will reach 75% because of the advancements in edge computing.[1]

Edge solutions serve as a gateway that can aggregate local data from network traffic signals and proximity sensors, host applications, and cache content for local subscribers. This is without having to send traffic through a congested backbone network to distant cloud resources. Some of these edge solutions also utilize existing cloud tools so that users can control workloads either on the edge or on the device without the need to learn new technology.

1 What Edge Computing Means for Infrastructure and Operations Leaders, Gartner.com

Other experiences that can be enabled with edge compute include real-time command and control in robotics, real-time analytics and inferencing through AI and machine learning (ML), and remote rendering for augmented reality. These technologies drive business innovation by capitalizing on the improved performance and efficiency of the edge. Some real-world examples of this are tracking drones with near-instant positioning or immersive training experiences using extended reality (XR), which combines real and virtual reality. These types of solutions allow for content rendering overlays, video streaming, internet of things (IoT) sensor alerts, and remote expert assistance in an experience that is optimized and virtually-realized. Such innovation will only continue as businesses capitalize on these new edge technologies.

IoT Driving Your Business Forward

At risk of overstating the obvious, digital transformation is about making the enterprise more competitive. IoT is no exception: capture the data, crunch the numbers, and take action. In a world where virtually anything can be connected, IoT initiatives drive productivity, operational efficiency, quality, throughput, and much more.

The global market intelligence firm IDC[2] forecast IoT spending of $805.7 billion for 2023, an increase of about $100 billion over 2020, and it is expected to surpass $1 trillion by 2026.

Along with this massive increase in IoT devices comes massive amounts of data… data that will help drive productivity, decision making, and new customer experiences. However, IoT device data and communications must also be monitored for potential cyber threats.

Practical Application of AI and Machine Learning

Artificial intelligence and machine learning will help automate the baselining and analysis of this data as well as help identify anomalous behavior. These technologies help security analysts deal with the scale of cybersecurity change that comes with digital transformation. The ability to detect and respond to threats becomes increasingly complex as computing power moves closer to the device and the number of connected devices increases exponentially. AI and machine learning bring a more proactive approach to cybersecurity.

This is especially important for highly sophisticated attacks that can spread and mutate faster than a human can respond or neutralize. These "machine-speed attacks" have increased in recent years as malicious actors have begun turning to AI and ML to execute their attacks. Businesses can use the same technology in their defense to such attacks. Utilizing AI and ML to detect new patterns in user behavior helps identify, detect, and respond to these attempts. These technologies can automate the analysis of the abnormal behavior to offer additional information about the threat event so analysts can make more appropriate responses.

Artificial intelligence and machine learning can bring many benefits to the fight against cybercrime that also help drive business outcomes. A recent report[3] showed that 64% of business leaders surveyed said AI lowers the cost to detect and respond to breaches. With AI, the overall time taken to detect threats and breaches is reduced by up to 12%. Dwell time – the amount of time threat actors remain undetected, drops by 11% with the use of AI.

2 Worldwide Spending on the Internet of Things is Forecast to Surpass $1 Trillion in 2026, IDC.com

3 Reinventing Cybersecurity with Artificial Intelligence, Capgemini

Securing the Digital Transformation

With each of these elements of digital transformation comes considerations on how to properly secure the underlying technology and data within. Here are some recommendations on what to look for as you consider securing the organization's digital transformation.

Enable Agility

Adoption of the best security strategy for business should be made with agility in mind. This will not only aid in adoption, but it can also help ensure there is a system in place that is both flexible and sustainable as the business changes and grows.

There are a few factors to consider when searching for the vendor and solutions that are the best fit:

- **Automation** is a fundamental tenet of agility. Give appropriate consideration to the judicious use of automation to liberate already over-stretched security personnel.
- **Multi-tenant** architecture helps ensure that the business has the flexibility it needs to deliver the right policy-based governance to different groups of users and endpoints.
- **Ease-of-use** aids in adoption to support an efficient and effective strategy.

Build the Right Platform and Ecosystem

All too often, well-intentioned security teams choose a cadre of point-specific solutions to satisfy their needs. They choose this solution for endpoint protection, and that solution for endpoint detection and response. Or even this solution for Windows and that for Linux and/or macOS. Too many tools and interfaces, often with overlapping functions, can create waste, increase complexity, and place a drag on the security team's performance.

Rather than building a complex stack of security solutions that may or may not have interoperability issues, we recommend giving careful consideration to solutions that can solve for multiple problems.

They should also address the security of cloud workloads, endpoint security, and IoT from a single platform. In addition, it's also recommended to consider ease-of-integration.

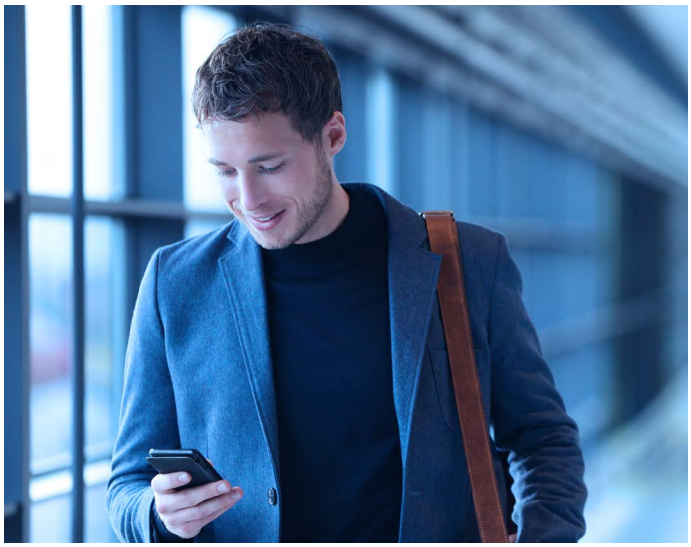
This includes:

- Looking for **API-first** security solutions to promote interoperability and integration among the security stack
- Considering a **solution platform** that provides a solid foundation for data ingestion and analysis, and the ability to deliver actionable insights from all the noise

Know What is on Your Network

As organizations accelerate their digital transformation, their IT strategy can become increasingly intricate. An abundance of user endpoints, operational technology (OT), cloud workloads, and IoT devices may be strewn across multi-site, microsegmented network topologies. Knowing what is actually connected to the network at any given moment can seem a Herculean challenge. Yet, modern device discovery and fingerprinting technology have risen to this task.

Enterprises no longer need to deploy hardware or software dedicated to asset discovery. Due to device hardware and software limitations, not every IoT device on your network can accept an agent. But, a modern discovery solution can reveal your agent deployment gaps, and even close those gaps for proactive attack surface reduction.



This is how device fingerprinting is a solution. Once devices are fingerprinted, their roles understood, and agents are deployed where appropriate, artificial intelligence and machine learning turn to baselining and continuously monitoring network communications. When something unusual is identified, the security operations center (SOC) can isolate suspicious devices from critical infrastructure.

Features needed to understand what's on your network:

- Fingerprints any IP-enabled device connected to your network
- Builds real-time, global asset inventories in moments
- Requires no extra agents, hardware, or network changes
- Identifies and closes agents' deployment gaps
- Monitors network traffic for device-based threats
- Isolates suspicious or malicious devices with a click
- Integrates to your endpoint detection and response data lake for device threat hunting

Autonomous Endpoint Detection and Response at the Edge (EDR)

The speed, scale, and sophistication of modern attacks have left first-generation endpoint detection and response behind. Cutting-edge endpoint detection and response makes practical use of AI and machine learning right at the endpoint and no network connection is required. This is autonomous, adaptive endpoint security. The intelligence to detect a threat is built into the agent itself and does not rely upon a cloud connection. The automated response is governed by policy, configurable by tenant and per site.

An effective edge-based EDR solution should provide:

- Verifiable EDR performance from trusted third parties like MITRE Engenuity
- Work with or without a network connection
- An automated response, configurable by policy
- Extensive threat hunting capabilities, including multi-cloud workloads and device-based threats
- Comprehensive OS support across Linux, Windows, macOS

Establish Cloud Workload Security

Virtual machines (VMs) and containers, whether on-premises or in AWS, Azure, or Google Cloud, still require **runtime security** to protect workloads. Like endpoints, cloud workloads are just as vulnerable to cyberattacks, including through malware. Some malware is designed for specific types of attacks. For example, with the rise in price of cryptocurrency, cryptojacking – the act of hijacking cloud compute infrastructure to mine cryptocurrency, is also on the rise. Unknowingly, organizations end up playing host to computationally intensive cryptomining malware and paying the bill for their troubles.

Cutting-edge cloud workload security and EDR solutions readily identify malware to help protect from such malicious attacks. In addition, policies can automate the kill and quarantine of malware, preserving the immutability of cloud workloads.

In addition to runtime security, **configuration security** of cloud infrastructure is another opportunity to consider. Misconfigured cloud resources represent a major attack vector, as bad actors automate the probing of cloud infrastructure for open or vulnerable configs. Customer lists can be scraped and sold on the dark web, and intellectual property quietly exfiltrated. While the economic consequences are dire, the solution is within reach. The Center for Internet Security (CIS) publishes benchmarks for the secure configuration of cloud services. Configuration security assessments against these best practices can be automated to spotlight misconfigurations.

Other best practices include:

- Host OS protection for Linux and Windows Server
- Enterprise-grade EDR with remote forensics and threat hunting
- Container runtime security for self-managed and managed Kubernetes
- Cloud metadata ingestion to simplify hybrid cloud management
- Auto-scaling and resource efficiency

Understand Managed Threat Detection and Response

In today's digital-first environment, keeping up with changes to security needs can be a daunting task. Managed security service providers (MSSPs) can help businesses stay focused on running their business to augment or enhance their existing security teams. MSSPs can help create economies of scale as well as attract and retain quality cybersecurity talent. They should be utilized to help the business keep pace with digital transformation.

A qualified MSSP should:

- Provide certified security experts, available 24/7
- Utilize best-of-breed tools with deep integration to maximize efficiency
- Have the ability to maintain a real-time inventory of networked assets and monitor the security of those assets
- Deliver white glove onboarding and ongoing collaboration on achieving security and compliance goals

Conclusion

As innovation in technology continues, digital transformation is becoming more essential for businesses. While this does increase the number of endpoints and cyber risk, a proactive endpoint security strategy can enable a business to defend against cyberattacks. Knowing which devices are connected to the network, establishing security for the cloud, and building the right platform and ecosystem that are fit to the business are just a few things a company can do to take control of their cybersecurity. And with service providers that strive to understand the business and provide the additional support that is needed, cybercriminals will find the door shut to their network.

LevelBlue

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.

To learn more about LevelBlue endpoint security solutions, powered by SentinelOne, contact your LevelBlue business representative or visit LevelBlue.com.