DELL Technologies

# Endpoint security is an essential element of your Zero Trust journey

## Three recommendations for getting Zero Trust ready



DELL Technologies

## Executive summary

Zero Trust is a long-term journey. It's not a product or solution that organizations implement: it's a strategic framework for managing security that is built over time. This eBook offers practical guidance for IT decision makers navigating a Zero Trust transformation, focusing specifically on the role endpoint device security plays in creating a modern, truly secure foundation for our work-from-anywhere world.

## Table of Contents

Cyber state of the union ..... 3
Implications for our work-from-anywhere world ..... 4
Security strategies need to change ..... 5
Understanding the fundamentals of Zero Trust ..... 6
Activating Zero Trust principles ..... 7
Three recommendations for getting Zero Trust ready ..... 8
Key takeaways ..... 11
Take the next step ..... 11

# Cyber state of the union

Security threats are growing, driven by our increasingly remote/hybrid and cloud work world.

The complexity of protecting the data assets of an organization has grown tremendously in the last few years. The cloud has been game-changing for business productivity as remote/hybrid work use grows, but it's not without cost. The transition from managing only on-premises infrastructure to encompassing cloud has created a larger attack surface for adversaries, with expanding consequences. For instance, if an attacker is successful, they can affect not just one customer but potentially every customer of that cloud service and their customers all the way across the supply chain. The payoff for threat actors – both nation states and common criminals – can be enormous, and as a result they will continue to find new vulnerabilities to exploit.



The cost of global damages from cybercrime is expected to climb to **USD 10.5 trillion by 2025**[i]

There were **5,200** confirmed data breaches reported by Verizon in a 2022 study – **up 1.3x from the prior year**[ii]



# Implications for our work-from-anywhere world

Organizations must find a way to get ahead of the evolving threat landscape.

**So, what are the implications of the increasingly remote work world? Two things:**

**All organizations are vulnerable, ...**

> "[I]f a focused entity really wants to get into your system, they have a really high probability of success."
>
> — *Admiral Michael Rogers, former director of the National Security Agency and the former commander of U.S. Cyber Command*[iii]

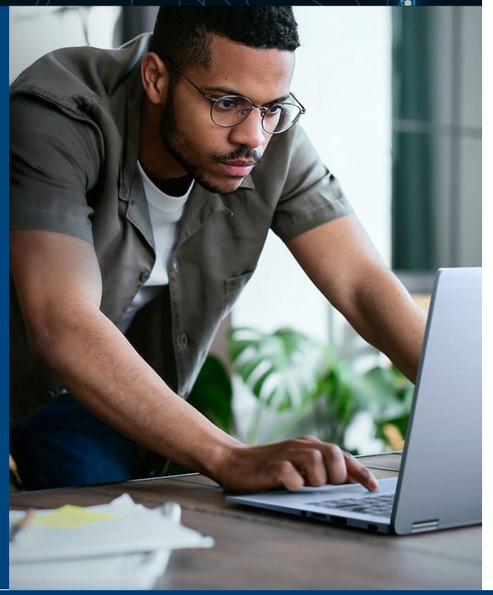
**...and the cost of getting it wrong can be crippling.**

> "Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022, [up 12.7% from 2020]."[iv]

**Attack vectors are growing, attack surfaces are expanding and no company can ever be completely secure. Organizations must assume a worst-case scenario and shore up their defenses for the inevitable attack.**



**69% of organizations** have experienced some type of cyberattack because of some poorly managed internet-facing asset.[v]



# Security strategies need to evolve

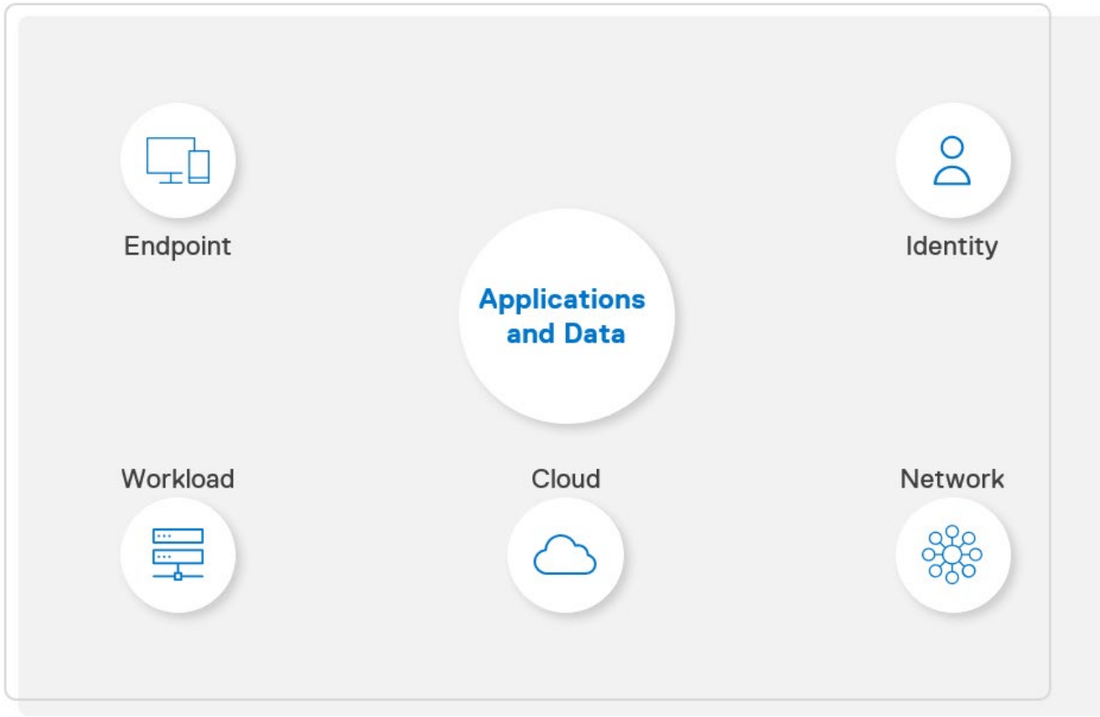
We must embrace the cloud-based environment. That's where Zero Trust comes in.

Traditional security models no longer work. Here's why.

For any organization to have an effective security posture, they must account for five control points: Endpoint, Workload, Identity, Network and Cloud. The goal is to protect the applications and the data.

Traditional approaches are often siloed, making organizations which use them more susceptible to attacks.

Next...

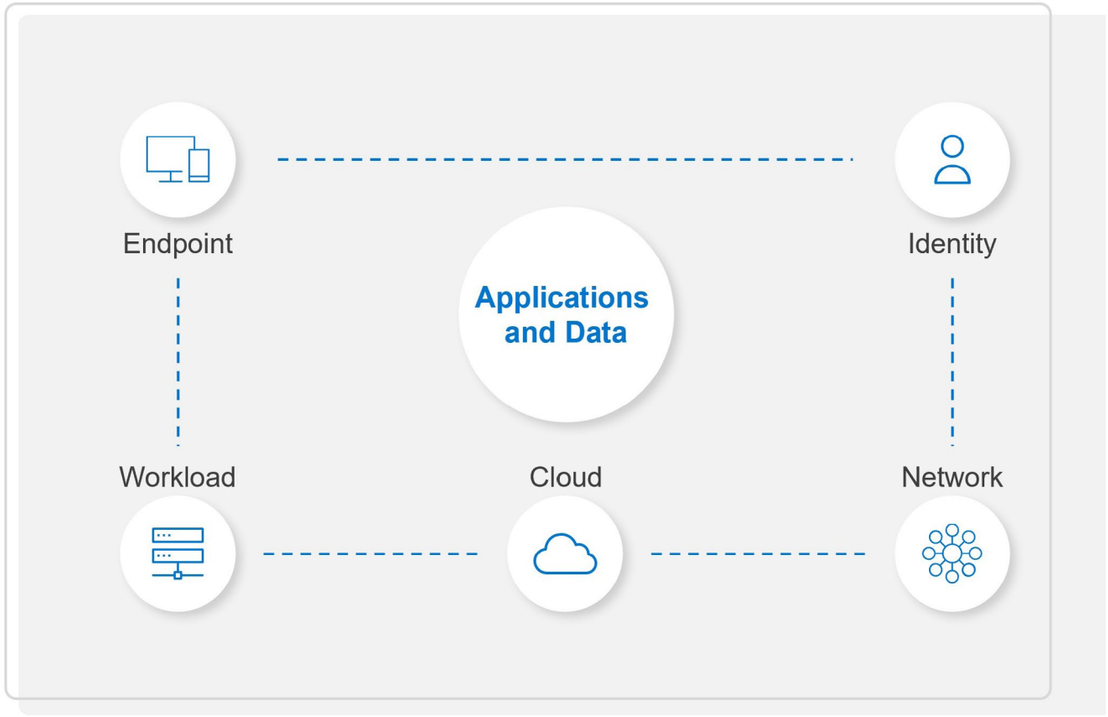


# Security strategies need to evolve

We must embrace the cloud-based environment. That's where Zero Trust comes in.

Modern approaches have moved towards greater control, with better communication between the control points. But, as we adopt an increasingly remote/hybrid work environment, we need to further strengthen the perimeter.

Next...

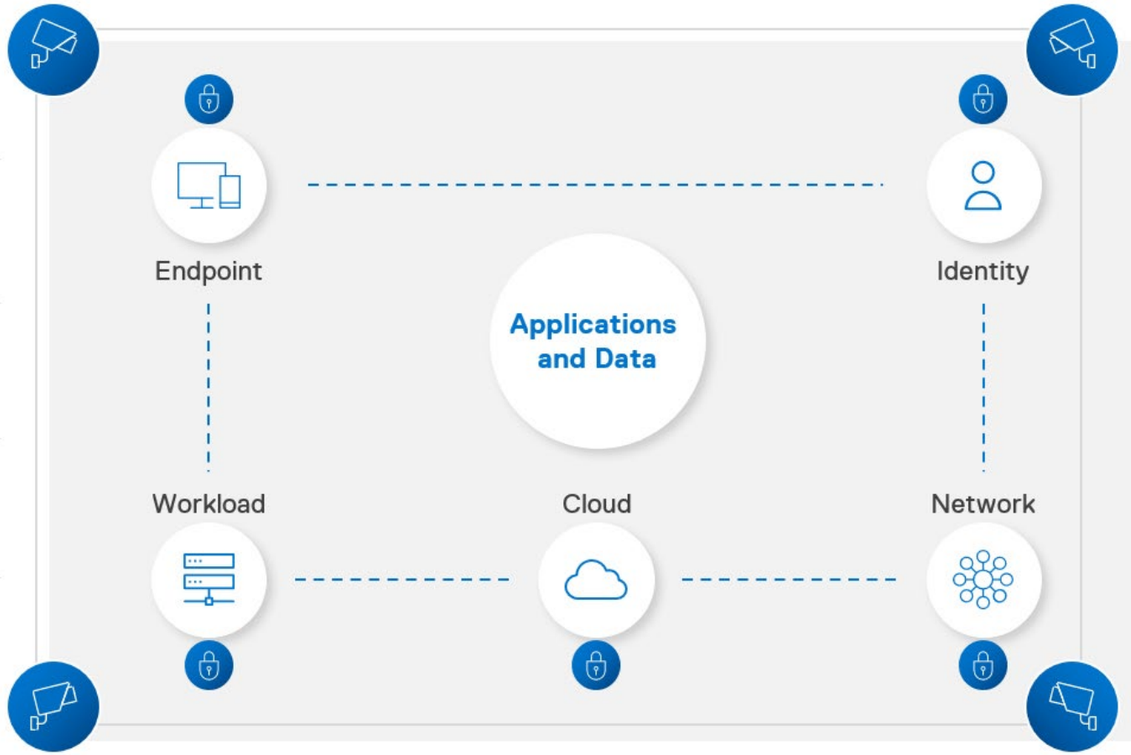


# Security strategies need to evolve

We must embrace the cloud-based environment. That's where Zero Trust comes in.

Today, employees work from everywhere – home, cafes, hotels – often using unsecured Wi-Fi with limited to no connectivity back to firewall-protected offices and data centers. The default may be a direct connection from their devices to the internet where they're connecting to cloud file servers and software-as-a-service (SaaS) applications – and working with enterprise data.

With the growing sophistication of attacks and number of attack vectors, traditional security strategies built on implicit trust no longer works. That's where Zero Trust comes in.

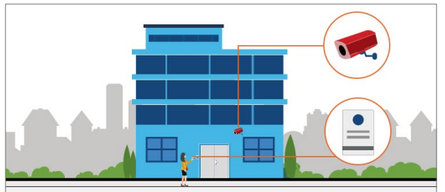


# Understanding the fundamentals of Zero Trust

Zero Trust is a new way of thinking about security. It replaces *implicit* trust – i.e., once authenticated, users roam freely about the network. Zero Trust flips the paradigm to give organizations explicit control of the IT environment.

Let's illustrate Zero Trust with a well-known concept: building security protocols.

You work in a corporate office. When you were hired, you received a badge and learned the security protocols. Every day, you walk into the building. Cameras are positioned everywhere. You badge in at multiple points. Once you sit at your desk, you unlock your computer with a password.



An employee arrives at their office building and gets their badge out to gain entry.

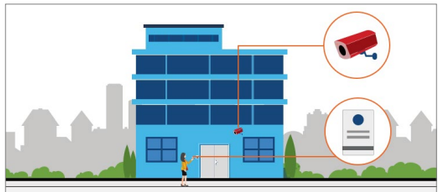
Next...

# Understanding the fundamentals of Zero Trust

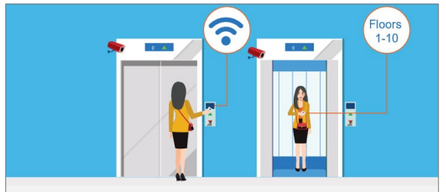
Zero Trust is a new way of thinking about security. It replaces *implicit* trust – i.e., once authenticated, users roam freely about the network. Zero Trust flips the paradigm to give organizations explicit control of the IT environment.

Let's illustrate Zero Trust with a well-known concept: building security protocols.

You work in a corporate office. When you were hired, you received a badge and learned the security protocols. Every day, you walk into the building. Cameras are positioned everywhere. You badge in at multiple points. Once you sit at your desk, you unlock your computer with a password.



An employee arrives at their office building and gets their badge out to gain entry.




They use their badge to gain access to the elevator assigned to their floor.

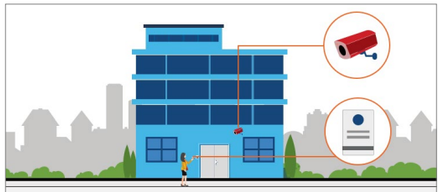
Next...

# Understanding the fundamentals of Zero Trust

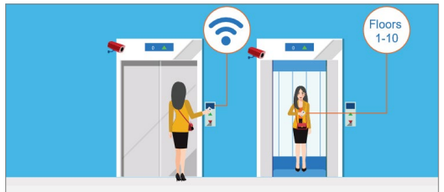
Zero Trust is a new way of thinking about security. It replaces *implicit* trust – i.e., once authenticated, users roam freely about the network. Zero Trust flips the paradigm to give organizations explicit control of the IT environment.

Let's illustrate Zero Trust with a well-known concept: building security protocols.

You work in a corporate office. When you were hired, you received a badge and learned the security protocols. Every day, you walk into the building. Cameras are positioned everywhere. You badge in at multiple points. Once you sit at your desk, you unlock your computer with a password.



An employee arrives at their office building and gets their badge out to gain entry.




They use their badge to gain access to the elevator assigned to their floor.



The employee uses their badge again to activate their floor selection in the elevator.

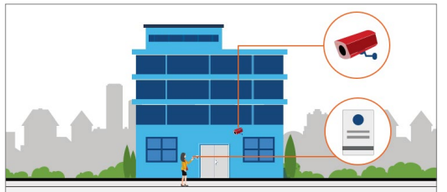
Next...

# Understanding the fundamentals of Zero Trust

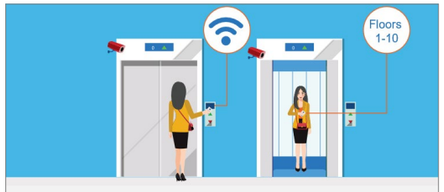
Zero Trust is a new way of thinking about security. It replaces *implicit* trust – i.e., once authenticated, users roam freely about the network. Zero Trust flips the paradigm to give organizations explicit control of the IT environment.

Let's illustrate Zero Trust with a well-known concept: building security protocols.

You work in a corporate office. When you were hired, you received a badge and learned the security protocols. Every day, you walk into the building. Cameras are positioned everywhere. You badge in at multiple points. Once you sit at your desk, you unlock your computer with a password.



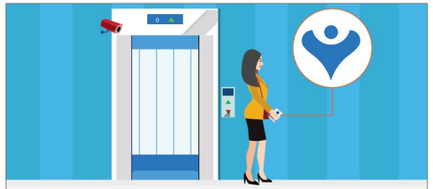
An employee arrives at their office building and gets their badge out to gain entry.




They use their badge to gain access to the elevator assigned to their floor.



The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

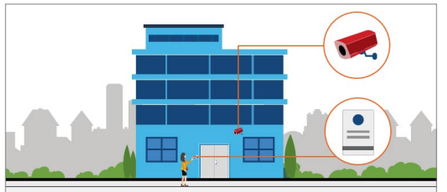
Next...

# Understanding the fundamentals of Zero Trust

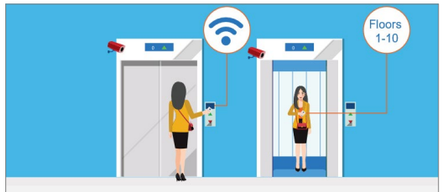
Zero Trust is a new way of thinking about security. It replaces *implicit* trust – i.e., once authenticated, users roam freely about the network. Zero Trust flips the paradigm to give organizations explicit control of the IT environment.

Let's illustrate Zero Trust with a well-known concept: building security protocols.

You work in a corporate office. When you were hired, you received a badge and learned the security protocols. Every day, you walk into the building. Cameras are positioned everywhere. You badge in at multiple points. Once you sit at your desk, you unlock your computer with a password.



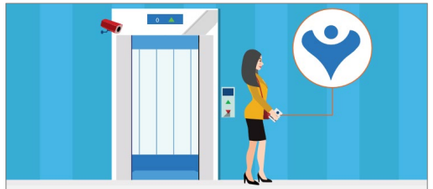
An employee arrives at their office building and gets their badge out to gain entry.



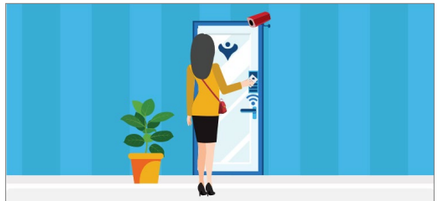

They use their badge to gain access to the elevator assigned to their floor.



The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.



They swipe their ID card to gain entry to their suite.

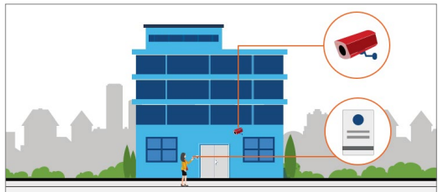
Next...

# Understanding the fundamentals of Zero Trust

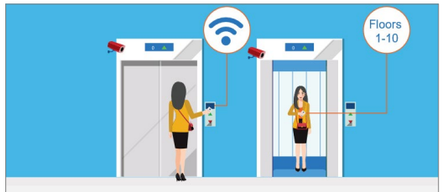
Zero Trust is a new way of thinking about security. It replaces *implicit* trust – i.e., once authenticated, users roam freely about the network. Zero Trust flips the paradigm to give organizations explicit control of the IT environment.

Let's illustrate Zero Trust with a well-known concept: building security protocols.

You work in a corporate office. When you were hired, you received a badge and learned the security protocols. Every day, you walk into the building. Cameras are positioned everywhere. You badge in at multiple points. Once you sit at your desk, you unlock your computer with a password.



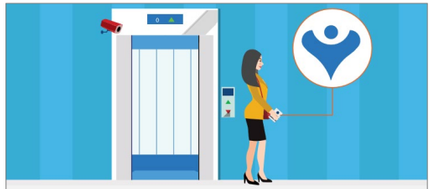
An employee arrives at their office building and gets their badge out to gain entry.



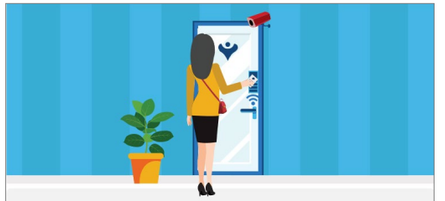

They use their badge to gain access to the elevator assigned to their floor.



The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.



They swipe their ID card to gain entry to their suite.



The employee arrives at their desk and unlocks their computer using a password.

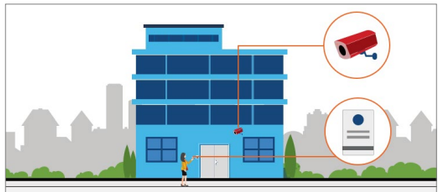
Next...

# Understanding the fundamentals of Zero Trust

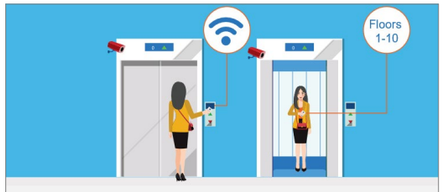
**This is how Zero Trust works.**

Your employer identified you on Day One. Every access you've requested since then has been verified to protect the assets of the organization (users, data, etc.). For an added layer of safety, security guards watch all movement in the building on monitors. Any odd behavior – e.g., trying to access a suite you shouldn't be – is investigated.

Today, we find users, devices, apps and data more frequently outside their corporate networks than ever before. As a result, user identity has become a blind spot, with identity compromise being the key element in most breaches. Zero Trust course corrects this.



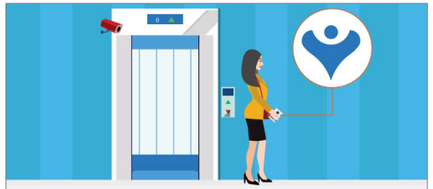
An employee arrives at their office building and gets their badge out to gain entry.



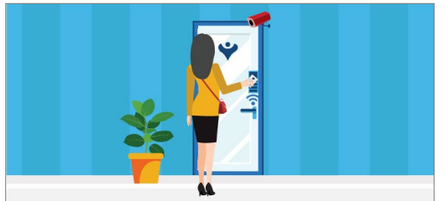

They use their badge to gain access to the elevator assigned to their floor.



The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.



They swipe their ID card to gain entry to their suite.



The employee arrives at their desk and unlocks their computer using a password.

# Activating Zero Trust principles

Endpoint security is a critical piece of a Zero Trust transformation.

To effectively enable a Zero Trust strategy, you must secure endpoints.

According to the MITRE ATT&CK® framework, today, there are nine “initial access techniques” that adversaries use to gain entry to networks *(see illustration)*.[vi] As research shows, in our cloud-based world traditional defenses can’t keep endpoints secure. An attacker needs just one point of entry. With endpoints, threat actors can exploit dozens of vulnerabilities across the entire lifecycle of a device.

As the number of devices on a network grows, endpoints become a larger and larger attack vector.

Security policies in a Zero Trust model define the “known good” in explicit detail – everything else is blocked. Threat management then monitors for any deviation from the known good, flagging unusual behavior and triggering the appropriate action to remediate the potential threat.

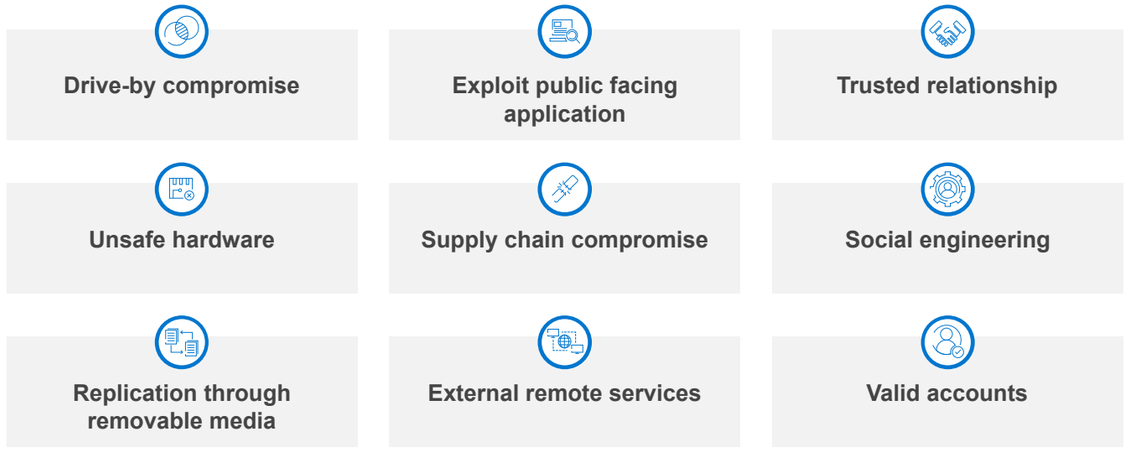



Illustration 1/3

# Activating Zero Trust principles

Endpoint security is a critical piece of a Zero Trust transformation.

To effectively enable a Zero Trust strategy, you must secure endpoints.

According to the MITRE ATT&CK® framework, today, there are nine “initial access techniques” that adversaries use to gain entry to networks *(see illustration)*.[vi] As research shows, in our cloud-based world traditional defenses can’t keep endpoints secure. An attacker needs just one point of entry. With endpoints, threat actors can exploit dozens of vulnerabilities across the entire lifecycle of a device.

As the number of devices on a network grows, endpoints become a larger and larger attack vector.

Security policies in a Zero Trust model define the “known good” in explicit detail -- everything else is blocked. Threat management then monitors for any deviation from the known good, flagging unusual behavior and triggering the appropriate action to remediate the potential threat.

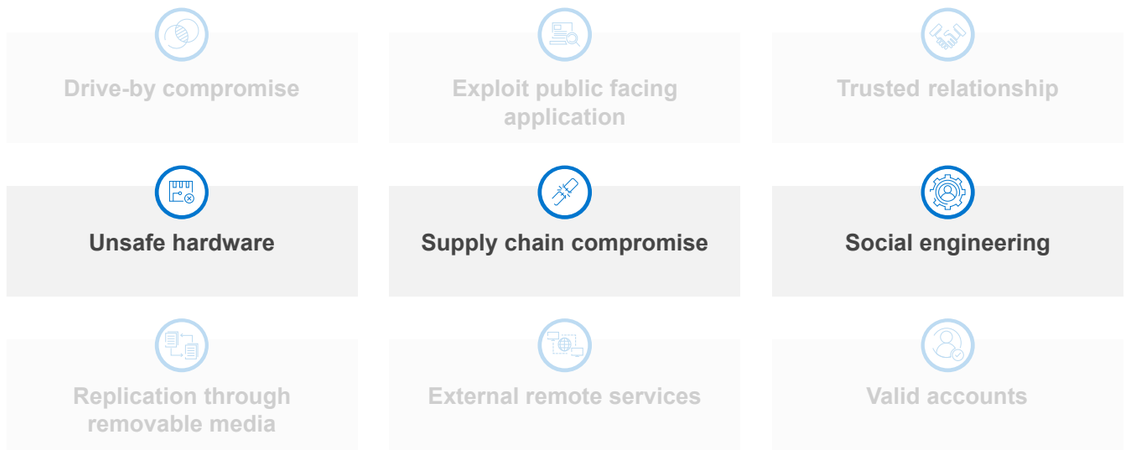



Illustration 2/3

# Activating Zero Trust principles

Endpoint security is a critical piece of a Zero Trust transformation.

To effectively enable a Zero Trust strategy, you must secure endpoints.

According to the MITRE ATT&CK® framework, today, there are nine “initial access techniques” that adversaries use to gain entry to networks *(see illustration)*.[vi] As research shows, in our cloud-based world traditional defenses can’t keep endpoints secure. An attacker needs just one point of entry. With endpoints, threat actors can exploit dozens of vulnerabilities across the entire lifecycle of a device.

As the number of devices on a network grows, endpoints become a larger and larger attack vector.

Security policies in a Zero Trust model define the “known good” in explicit detail -- everything else is blocked. Threat management then monitors for any deviation from the known good, flagging unusual behavior and triggering the appropriate action to remediate the potential threat.

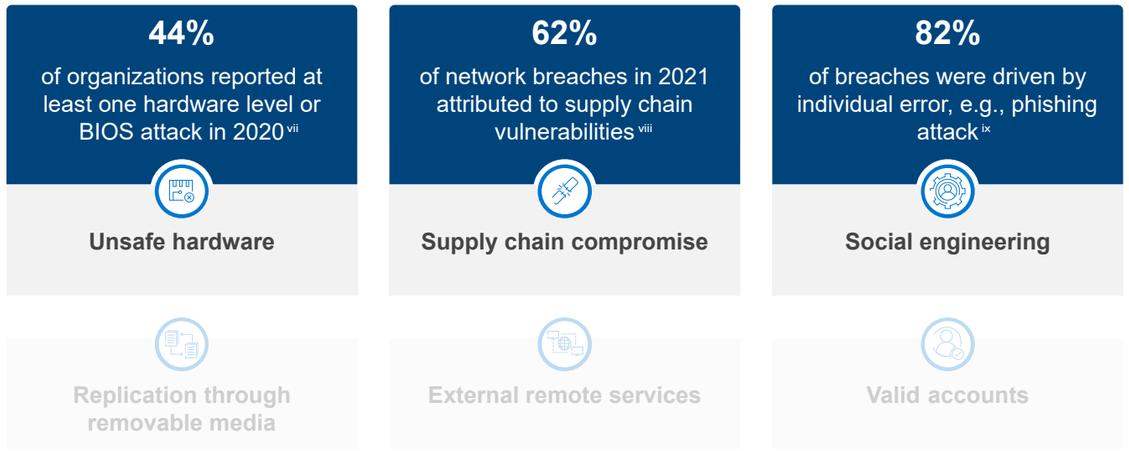



Illustration 3/3

# Three recommendations for getting Zero Trust ready

Position your organization for a successful Zero Trust transformation.

1

## Establish the right policies and controls that support your business priorities.

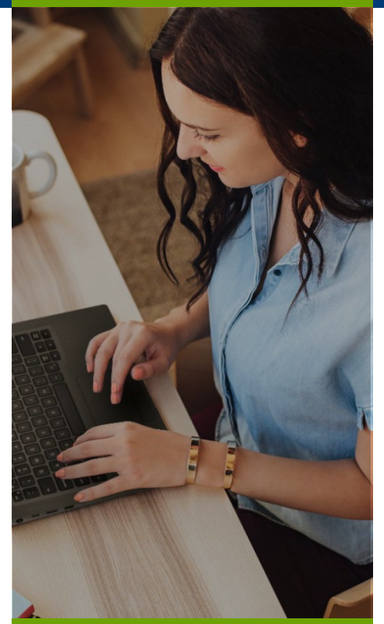
Policy engines and policy management are critical to effective Zero Trust implementations. However, no organization has an unlimited budget for security, so first, determine your business priorities. What are the most critical assets and IP you are trying to protect? Weigh that attack surface against your organization's allowable risk.

Then, review the policies and controls currently in place. Risks today originate from the cloud-based world we live in. Does your policy engine take this into consideration?

With policies in place to govern access to your most important assets, you can then expand your scope.

***LEARN MORE***

For more information, *watch this video* where Dell cyber experts discuss key security risks that organizations face today.



With more users, apps, data and devices outside a corporate network than ever before, **82%** of IT security decision makers say they've had to re-evaluate their security policies.[x]

# Three recommendations for getting Zero Trust ready

Position your organization for a successful Zero Trust transformation.

## 2 Start with secure devices.

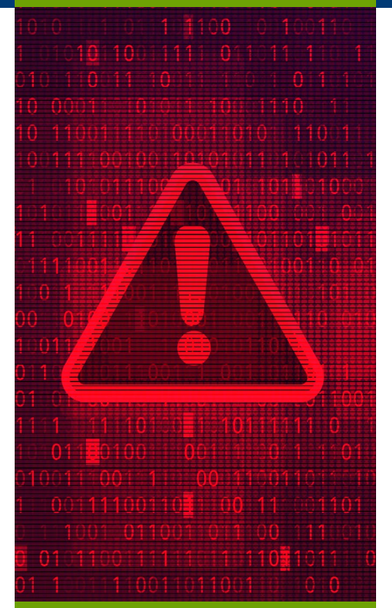
Base Zero Trust planning on a solid foundation. Strengthen your defenses with devices designed and developed with security in mind. This includes:

A. **Hardware- and firmware-based protections** that secure the endpoint stack and allow visibility (e.g., detect if a BIOS has been compromised and alert IT). Equip your organization with technologies that verify identity for every new request for access – with as minimal an impact on employee productivity as possible.

B. **Supply chain protections and integrity controls** that secure every step of the PC lifecycle. As we've seen in recent years, supply chain attacks can be devastating. For a true Zero Trust architecture, authentication, verification and monitoring starts at the supply chain. Work with vendors that 1) employ secure practices and 2) allow you to validate the integrity of your devices, from procurement to manufacturing to delivery.

***LEARN MORE***

*For more information about best practices in device security, read Dell and Intel's whitepaper, Achieving Pervasive Security Above and Below the OS.*



In **2021**, an IT management company spread a ransomware attack to at least **1,500** customers.[xi]

# Three recommendations for getting Zero Trust ready

Position your organization for a successful Zero Trust transformation.

3

## Strive for seamless integration and interoperability across your ecosystem.

To achieve an effective security posture, at a high level, three things are critical:

A. Integration of all defenses across the IT ecosystem,

B. Real-time visibility and

C. Ability to take action when needed.

In our cloud-based world, where even the smallest vulnerability left unchecked is a potential nightmare, it's important that all systems recognize potential threats *and* are set up to take necessary action.

Are your systems integrated or do they operate in siloes? Can your policy engine trigger a specific workflow when an IT admin is alerted to a corrupted BIOS on the network? In an integrated environment, automations should immediately quarantine any BIOS in question, limit any additional access and run a patching exercise.

Do you have visibility into all of your endpoints? Ideally, you have rich telemetry flowing in from every layer, from the supply chain (e.g., the loading dock) to the firmware (e.g., BIOS-level tamper alerts).

But that telemetry is only as good as your integrations. Can you action your data? It's important you have the right resources – e.g., skilled cybersecurity talent – in place to make sense of the data and program workflows that address issues.



**41% of organizations** are deploying Zero Trust[xii]

DELL Technologies

## Key takeaways

### The future of security is Zero Trust.

- Attack vectors have multiplied as we embraced the future of work.
- A breach is inevitable. Minimize the attack surface with defenses that prepare for the worst-case scenario.
- Zero Trust is a new way of thinking about security that gives organizations explicit control of the IT environment.
- Endpoint protections that activate Zero Trust principles are key to maintaining a secure, modern foundation.
- Pinpoint your most critical assets to prioritize the buildout of your Zero Trust architecture.
- Source devices from vendors that offer built-in protections and invest deeply in their supply chain controls.
- Assess security and IT interoperability. Continue to embed workflows to fortify your security posture.

## Take the next step

Security is a daunting topic for organizations of all sizes. Engage an experienced security and technology partner to help streamline your Zero Trust transformation.

Dell Trusted Workspace helps secure endpoints for a modern, Zero Trust-ready IT environment. Reduce the attack surface with a comprehensive portfolio of hardware and software protections exclusive to Dell. Our highly coordinated, defense-based approach offsets threats by combining built-in protections with ongoing vigilance. End users stay productive, and IT stays confident with security solutions built for today's cloud-based world.

Contact us: EndpointSecurity@Dell.com
Visit us: Dell.com/Endpoint-Security
Follow us: LinkedIn @DellTechnologies | Twitter @DellTech

© Copyright 2022 Dell Inc.

DELL Technologies


[i] Cybersecurity Almanac 2nd Edition. Cybersecurity Ventures, 2022 https://cybersecurityventures.com/cybersecurity-almanac-2022/

[ii] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach

[iii] American College of Cardiology, You Will Be Hacked. Plan Now: Cybersecurity in Health Care, 2021 https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care

[iv] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach

[v] ESG Complete Survey Results, Security Hygiene and Posture Management, 2022 https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management

[vi] MITRE ATT&CK https://attack.mitre.org/tactics/TA0001/

[vii] Futurum, Four Keys to Navigating the Hardware Security Journey, 2020 https://futurumresearch.com/research-reports/four-keys-to-navigating-the-hardware-security-journey/

[viii] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[ix] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[x] Absolute Endpoint Risk Report, 2021 https://www.absolute.com/go/reports/endpoint-risk-report/

[xi] TechTarget, 2021 https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks

[xii] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach



Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. This case study is for informational purposes only. Dell believes the information in this case study is accurate as of its publication date, September 2022. The information is subject to change without notice. Dell makes no warranties—express or implied—in this case study.