HCL BigFix

Speeding Your Journey to Zero Trust

Conventional Defenses Are Not Enough

In the last decade or so, Information Technology (IT) has evolved to make it clear that organizations can no longer rely on conventional cybersecurity defenses. Trends including cloud migration have caused the perimeter to disappear, forcing cybersecurity teams to rethink how best to protect their organizations.

To help them, the concept of **Zero Trust** has gained steam. In 2022, 41% of surveyed organizations reported they have already deployed a Zero Trust approach, compared to 35% in the previous year.[1] A recent U.S. federal mandate to move to Zero Trust cybersecurity principles is also likely to accelerate adoption across both the public and private sectors.

UNDERSTANDING THE ZERO TRUST MANDATE

What is it?
A sweeping government-wide effort to migrate to the Zero Trust architecture, as part of Presidential Executive Order (E.O.) 14028, "Improving the Nation's Cybersecurity."

Why is it needed?
To improve network, infrastructure, and data security "to defend the vital institutions that underpin the American way of life."

Who is affected?
While the initial E.O.'s requirements are specific to government agencies, E.O. 14028 incentivizes most organizations, across many industries to follow the government's lead and expand implementation in the private sector.

Why migrate endpoints to Zero Trust?

55 new common **vulnerabilities and exposures were discovered daily** on average, throughout 2021[2]

Organizations have an average backlog of 57,555 **identified vulnerabilities**[3]

The number of cybersecurity **incidents due to vulnerability exploits** grew 33% between 2020 and 2021[4]

The Changing Endpoint Security Game

The global migration to cloud services, the rise in remote work, and bring-your-own-device (BYOD) trends have complicated IT environments, erasing what was once an identifiable network perimeter. Traditional cybersecurity methods can't keep up. Zero Trust helps close the gap left by perimeter-based defenses.

A Zero Trust approach:

- Focuses on removing inherent trust relationships in IT networks.
- Assumes no connection, device, or identity is to be trusted, regardless of location.
- Requires continuous diagnostics and monitoring — dynamically authenticating, authorizing, and validating every user, device, application, and connection before granting access to a resource.

To improve security, Zero Trust:

- Eliminates components that enable an adversary to compromise your systems.
- Helps proactively discover and remove threats, before they can enter your environment.
- Focuses on protecting resources (assets, accounts, workflows, etc.) rather than network segments.

Zero Trust Architecture (ZTA)

- Reduces organizational risk, boosts security, and improves regulatory compliance.
- Improves visibility into all of your owned and associated assets, including their integrity and security posture.
- Enforces access policies based on attributes such as behavior and environment.

63% of organizations cite a **lack of visibility into endpoints as the biggest barrier** to achieving a strong security posture[5]

Endpoints are on the Front Line

The Department of Defense first declared cyberspace a war-fighting combat zone in 2010. If cyberspace is a battlefield, endpoints are your first line of defense.

Endpoints include any devices and connections employees use to access your organization's data and resources. On the cyberspace battlefield, you should assume endpoints are compromised. However, you don't need to accept this compromise. Instead, find a way to respond and secure all devices, as quickly as possible.

ACCOMPLISHING THIS CYBERSECURITY MISSION REQUIRES TWO CAPABILITIES:

- **Improve visibility into all endpoints, whether they're owned by your organization or by others.**
- **Repair vulnerabilities quickly, on the fly, before an adversary can use them to access your data and resources.**

The importance of Zero Trust endpoint management

According to NIST Special Publication 800-207, one of the key requirements of Zero Trust Architecture (ZTA) is the ability to identify and monitor devices, including those not owned by the enterprise. As NIST explains, "The ability to manage enterprise assets is key to the successful deployment of ZTA."

Continuous Diagnostics and Mitigation for Endpoints

Achieving Zero Trust requires you to continuously evaluate device security. Continuous Diagnostics and Mitigation (CDM) is a strategic security approach implemented by the Cybersecurity and Infrastructure Security Agency (CISA) that is designed to help you monitor the current state of devices and apply fixes as needed.

Approaching Zero Trust with CDM can help you understand what's going on across every endpoint, to quickly diagnose issues, and mitigate risks.

With CDM you can:

- Collect telemetry to assess endpoint security and integrity.
- Update device configurations and settings automatically.
- Change access policies dynamically to isolate vulnerable or compromised devices.

ANSWER CRUCIAL QUESTIONS

Implementing CDM provides valuable insights into your assets, including information on configurations and vulnerabilities, to help you answer questions such as:

1. What devices, services, and applications are used in your organization?
2. Who is connecting to your resources, including internal and external users?
3. What is happening inside your network?

STAY AHEAD OF THREATS

- 55% of organizations say they can't keep up with the volume of required patching due to a lack of adequate resources[6]
- 42% of organizations have experienced a data breach because they didn't apply an available patch[7]
- It takes organizations an average of 51 days to mitigate a critical vulnerability[8]

A CDM platform resolves these challenges by identifying vulnerable, compromised, and unmanaged devices, and quickly applying a fix, whether that involves patching the device, modifying configurations, or changing access policies.

Achieving Zero Trust with HCL BigFix

HCL BigFix makes security seamless and accelerates adoption of Zero Trust and other industry-specific mandates with a one-stop solution to help you effectively monitor endpoints, identify risks, mitigate vulnerabilities, and manage configurations.

BigFix works at enterprise speed and scale to help you quickly mitigate vulnerabilities such as Log4j across your entire infrastructure — without causing a degradation to business services. With BigFix, ensuring security is not a barrier to achieving your business goals. Instead, you can:

- Minimize tool sprawl by consolidating tools that assess, monitor, and report data.
- Gain context and insights into what's happening across your organization.
- Seamlessly push controls to endpoints, operating systems, and other assets.

Report data in real-time and build a score-based trust algorithm.

Proactively monitor and measure the security posture and integrity of all owned and unmanaged devices connecting to your resources.

HCL BigFix
CAPABILITIES

Automatically apply patches and update configurations that aren't secure.

Instantly change access policies and close endpoints.

Automatically collect telemetry about the state of assets, network infrastructure, and communications to improve your security posture,

Resources

[1]IBM, Cost of a Data Breach Report 2022

[2]Trustwave, 2022 SpiderLabs Telemetry Report

[3]Ponemon Institute/IBM X-Force, "The State of Vulnerability Management in the Cloud and On-Premises," August 2020

[4]IBM Security, X-Force Threat Intelligence Index 2022

[5]Adaptiva, 2022 Managing Risks and Costs at the Edge

[6]Ponemon/IBM, The State of Vulnerability Management in the Cloud and On-Premises

[7]Ponemon/IBM, The State of Vulnerability Management in the Cloud and On-Premises

[8]Edgescan, 2021 Vulnerability Statistics Report

HCL BigFix

HCL BigFix can help you achieve the Zero Trust philosophy of "never trust, always verify," while improving your organization's security posture, protection, and regulatory compliance.

Start your journey to better cybersecurity by learning how HCL BigFix can streamline your move toward a Zero Trust Architecture.

EXPLORE HOW HCL BIGFIX CAN HELP YOU ADVANCE ZERO TRUST SECURITY IN YOUR ORGANIZATION.

Info@hclfederal.com