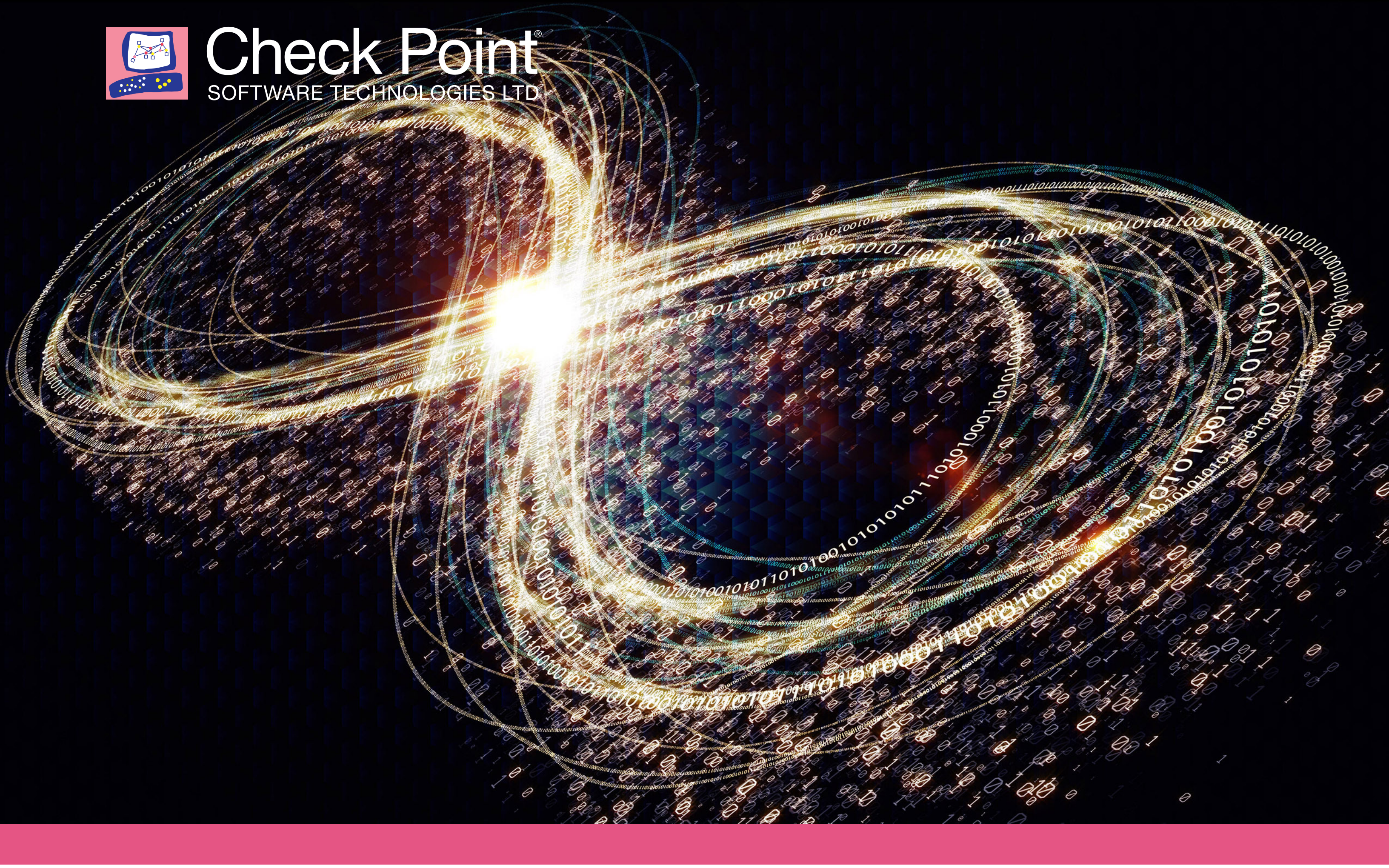
Check Point®
SOFTWARE TECHNOLOGIES LTD.



THE ULTIMATE GUIDE TO

ZERO TRUST SECURITY

Best Practices, Methodologies and Technologies
for Protecting Data in a
"Perimeter-Everywhere" World

Executive Summary

In today's digital, cloudified, distributed, and mobile work environment, there is no "inside the security perimeter," because the perimeter is everywhere. This new reality has dire implications for cybersecurity, with an attack surface that has never been greater, and with cybercriminals who have become acutely adept at exploiting this new reality.

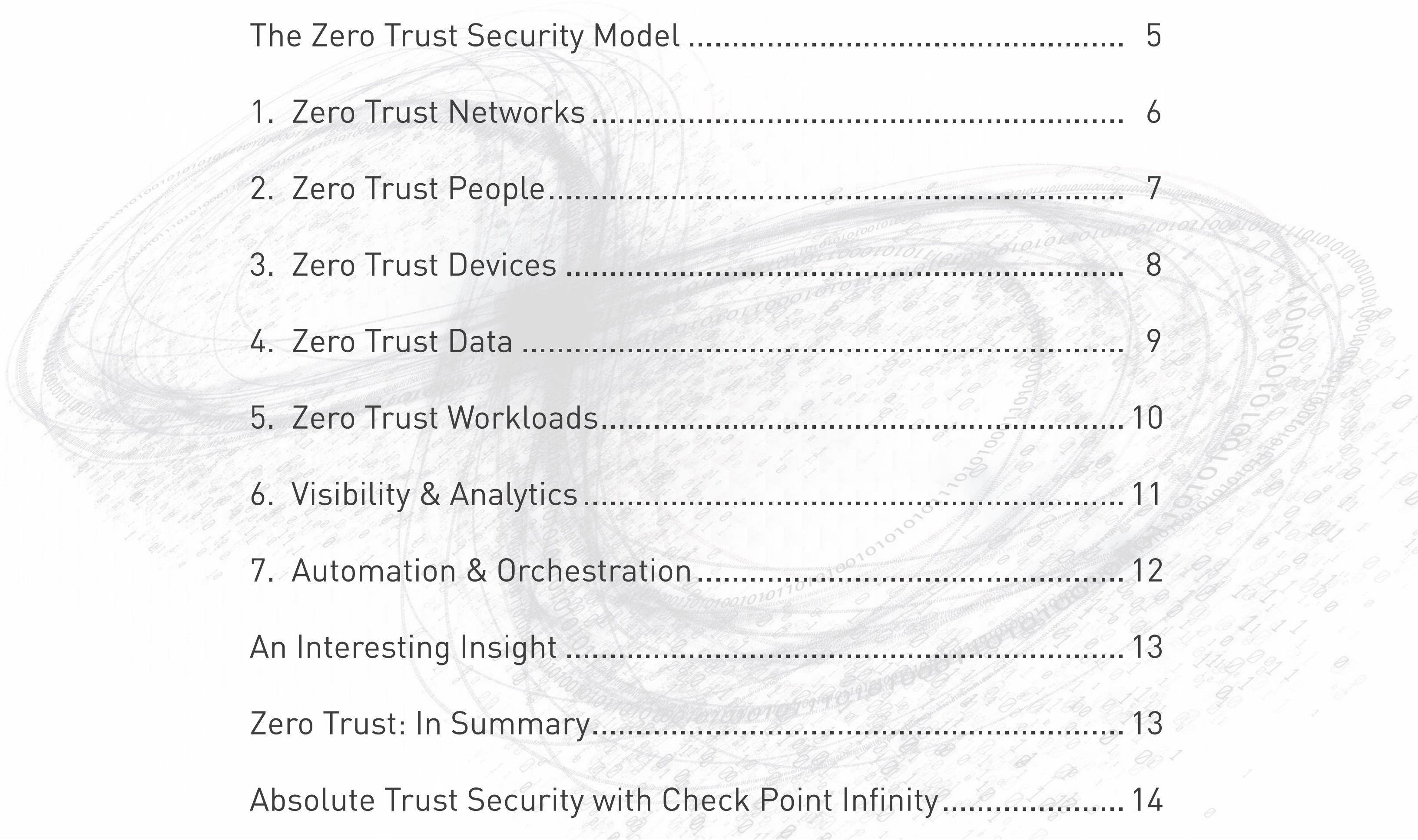
The key to overcoming the challenge of "perimeter everywhere" is Zero Trust Security, a security model that is driven by the precepts of never trusting anything outside nor inside the organization's security perimeters.

In this guide, we will cover the seven principles of the Zero Trust security model and share the best practices, methodologies, and technologies that enable its effective implementation.

Read this paper to learn how you can:

- Prevent malicious lateral movement with granular network segmentation
- Use context-aware authorization to protect against identity-thieves
- Protect all devices from threats, and isolate them if compromised
- Classify, protect and encrypt data, wherever it is
- Protect workloads with extended visibility and adaptable policies
- Quickly detect and mitigate threats with a single view into security risks
- Use rich API's to automate security tasks and incident response

TABLE OF CONTENTS



Background

AN EVER-CHANGING IT ENVIRONMENT AND THE EVOLVING THREAT LANDSCAPE

There is no doubt – the modern workplace is undergoing a revolution that brings profound implications to cybersecurity. Namely, the workspace is dynamic and roaming, the move to the cloud is accelerating, there is a broad proliferation of IoT-connected devices, and the workforce has never been more diverse – with partners, customers, and freelancers connecting more and more to the corporate network.

What this means for security is that long gone are the days of contained network infrastructure and a well-defined security perimeter, where all enterprise data rests, moves, and is consumed within the perimeter.

To complicate matters, even more, cybercriminals have never been more successful at penetrating and moving laterally within the security perimeter. Once inside, they collect valuable and sensitive data and can do so for months before being detected[1].

As an evidence, the rates of large-scale, multi-vector mega attacks are also growing, wreaking havoc on organizations and individuals worldwide:

- 1.76 billion records were leaked in January 2019 alone[2];
- Ransomware is expected to cost businesses and organizations $11.5 billion in 2019[3];
- The global cost of online crime is expected to reach $6 trillion by 2021[4].

LEGACY SECURITY APPROACHES ARE NO LONGER EFFECTIVE

Today, with cyber threats existing inside and outside the perimeter, legacy security infrastructures have become obsolete.

Legacy approaches have mainly been focused on scanning for threats only in "North-South" traffic – i.e. client-server traffic that moves in and out of the security perimeter.

Furthermore, access control has also been perimeter-based, where access to a company's data and assets had been granted to every entity (user, device, workload, or system), as based on the perimeter it is operating in, and determined in most cases by the IP address.

This "trust by default" approach has led to a dangerous and excessive trust, which is being exploited by hackers.Clearly, it's time for a new security paradigm.

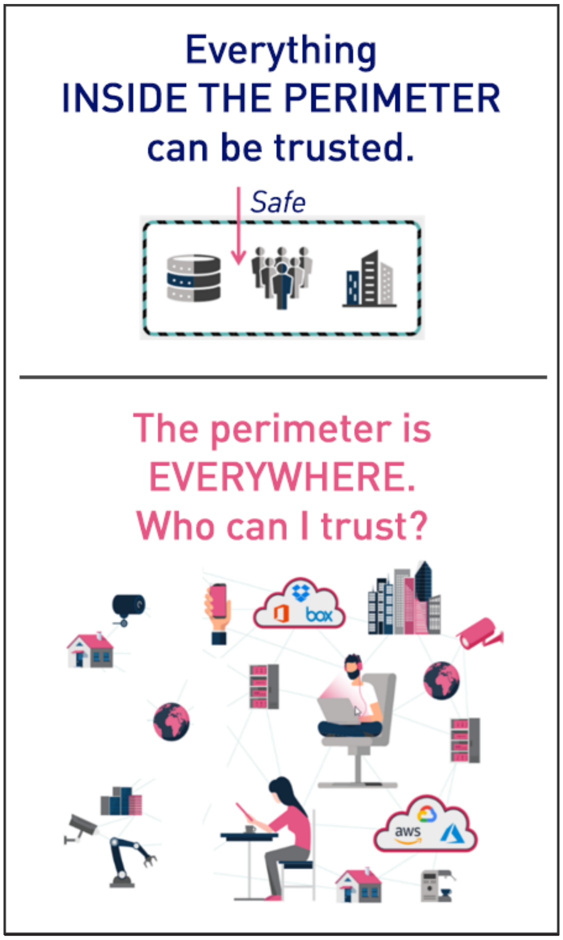


Figure 1. "Perimeter-everywhere" Environment

[1] Advanced Threats in retail companies, Ponemon Institute
[2] List of data breaches and cyber attacks in January 2019, IT governanace
[3] Ransomware damage costs predicted to hit $11.5B by 2019, CSO Magazine
[4] The Hill

The Zero Trust Security Model

THE NEW PARADIGM: NEVER TRUST. ALWAYS VERIFY.

The new security paradigm is "Zero Trust," a security model that constitutes a more data-centric and identity-aware approach that is designed to handle the new challenges of our "perimeter-everywhere" world. Zero Trust is driven by the precepts of never trusting anything inside nor outside the organization's security perimeters. Rather, before access is granted, anything and everything that is attempting to connect to an organization's systems must always be verified. With Zero Trust, the security team puts policies in place to validate every connection attempt and every device, and to intelligently limit access.

ZERO TRUST SECURITY: THE 7 PRINCIPLES

Zero Trust is more than a just concept or an approach. The Zero Trust Extended Security model, introduced by Forrester, offers seven key principles that enable the adoption of a "Default Deny" security posture, where systems are hardened and isolated until a level of trust is established.

A survey conducted by Check Point on Augst 2019 reveals that there is wide adoption of the Zero Trust approach by security professionals across multiple industries. More than half of respondents (52%) noted that the organization has begun or had completed an implementation of the Zero Trust approach, with 18% planning to start implementation during the coming year.

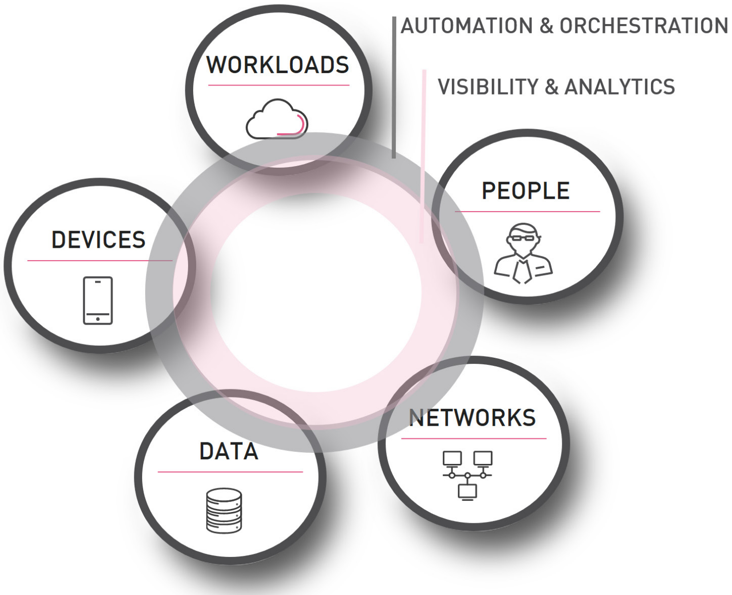
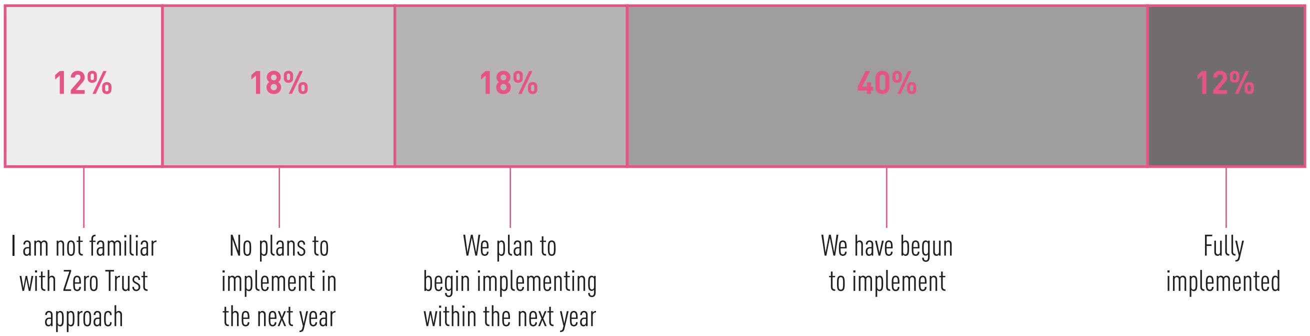


Figure 2. Zero Trust Extended Security model by Forrester

Organizations are beginning to adopt a Zero Trust approach to security.
Where does your organization stand in its adoption of this approach?



1 Zero Trust Networks

PREVENT MALICIOUS LATERAL MOVEMENT WITH GRANULAR NETWORK SEGMENTATION

With the growing proliferation of East-West traffic, there is a great need to contain unauthorized and malicious *lateral* traffic and stave off the spread of an attack within the organization.

The key to addressing this need is **granular network segmentation**. Namely, the idea is to divide and rule networks by building micro-perimeters around valuable assets.

Through micro-segmentation only the absolute minimum, legitimate traffic between segments is allowed, while everything else is automatically denied.

BEST PRACTICES FOR THE ZERO TRUST NETWORK

1. **Identify** which data and assets are valuable to the organization, e.g. the customer database, source code, smart building management systems, etc.
2. **Classify** the level of sensitivity of each asset - such as 'highly restricted,' e.g. the customer database, 'restricted,' e.g. the HR portal, which is open to all employees, including the level of sensitivity of public assets, such as the corporate website.
3. **Map** data flows among all entities across your network, including:
   a. **North-bound traffic**, such as sales teams accessing Salesforce.com via managed devices on the corporate network only.
   b. **East-West traffic**, such as from a frontend web portal to backend servers.
   c. **South-bound traffic**, such as from the website backend server to Google Analytics via the internet.
4. **Group** assets with similar functionalities and sensitivity levels into the same micro-segment. For example, all R&D internal assets, such as source code and ticket management system.
5. **Deploy** a segmentation gateway, whether virtual or physical, to achieve control over each segment.
6. **Define** a "least privilege" access policy to each of these assets, for example, allowing each R&D group to access only their own team's source code.

TIP! *Find the right balance between the granularity of the segmentation and the number of perimeters or micro-segments that can effectively and efficiently be managed.*

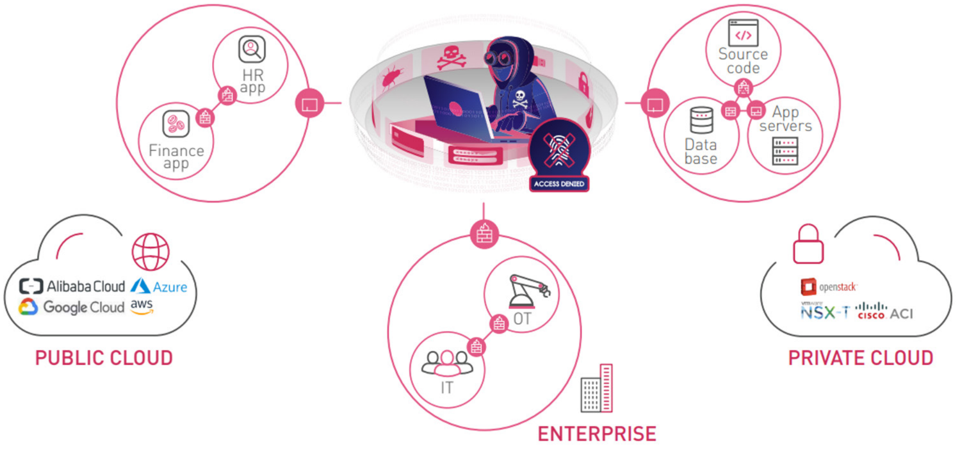


Figure 3. Zero Trust Network

2 Zero Trust People

USE CONTEXT-AWARE AUTHORIZATION TO PROTECT AGAINST IDENTITY-THIEVES

Protecting data against identity-thieves becomes all the more vital when considering the fact that more than 80% of data breaches involve stolen or weak credentials[5] (rendering the username/password approach practically irrelevant).

Zero Trust models overcome this fallibility by never granting trust by default to anyone attempting to access or process data. According to Zero Trust, every user connection attempt should be reevaluated, identities should be strictly authenticated, and access should be granted after the entire context of connection is inspected.

BEST PRACTICES FOR ZERO TRUST PEOPLE

1. **Authenticate user identities on the network level, rather than only on the application layer.** Bad actors do not use the front door, they usually seek and exploit vulnerabilities in applications, rather than trying to hack log-in pages. Authenticating users against security gateways will block hackers from getting too close to systems, and dramatically minimize the attack surface.
2. **Simplify the authentication process with single-sign-on (SSO)** by integrating authentication with the identity directory service (e.g. Microsoft AD, Cisco ISE, etc.). Users can be dismissed from double authentication (i.e. on the gateway and on the application), thereby eliminating the risk of multiple credentials and passwords.
3. **Reassure identities with multi-factor-authentication (MFA)** by adding an MFA layer that provides additional protection in the case of highly sensitive applications, or when required by context, such as when users connect from external networks or use an unfamiliar device.
4. **Set context-aware policies.** This entails narrowing down the definition of authorized connections by adding multiple conditions regarding the context of the connection attempt, such as a specific time, geo-location, connection method (VPN/WIFI), type of device, and more.
5. **Detect anomalies.** Compare each connection attempt to the baseline to detect suspicious events such as multiple unsuccessful login attempts, unrecognized devices, unusual times and locations, and more.

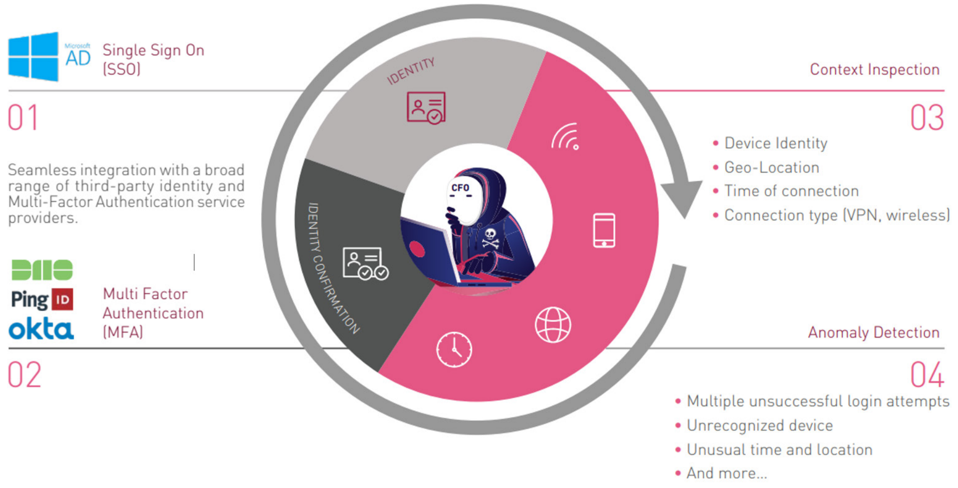

Microsoft AD
Single Sign On (SSO)
01
Seamless integration with a broad range of third-party identity and Multi-Factor Authentication service providers.
DUO
Ping ID
okta
Multi Factor Authentication (MFA)
02
IDENTITY
IDENTITY CONFIRMATION
CFO
Context Inspection
03
• Device Identity
• Geo-Location
• Time of connection
• Connection type (VPN, wireless)
Anomaly Detection
04
• Multiple unsuccessful login attempts
• Unrecognized device
• Unusual time and location
• And more...

Figure 4. Four Steps to Zero Trust People

[5] 2017 Verizon DBIR

3 Zero Trust Devices

PROTECT ALL DEVICES FROM THREATS, AND ISOLATE THEM IF COMPROMISED

The targets of hackers have become many and varied, moving beyond networks and workstations, and now also including the multitude of mobile devices (most of which are personally owned), IoT-enabled devices, and operational technology (OT),

In the case of IoT and OT devices, the vulnerability is particularly strong. They are typically connected to corporate networks and run on unpatched software. Moreover, they are often misconfigured or communicate via unsecured protocols.

These devices are inherently vulnerable and also remain poorly or completely unprotected by traditional solutions.

Accordingly, the Zero Trust model calls for protecting all devices on the network and isolating them if compromised.

BEST PRACTICES FOR ZERO TRUST DEVICES

1. **Segment IoT/OT networks.** Take a practical approach to minimize the attack surface through network segmentation. Traffic to and from devices should be highly restricted, allowing only the minimal communication required for proper functioning. Since traditional firewall and NAC solutions lack the visibility and context to detect and block out-of-scope activity, a dedicated IoT/OT security solution should be implemented.
2. **Protect workstations and mobile devices on untrusted networks.** Enforce the installation of on-device security protection for all employee devices (including BYOD), to prevent zero-day malware, malicious app installations, phishing attacks, bot attacks, and more (since the protection of an MDM mobile app will not suffice).
3. **Block infected or vulnerable devices from corporate assets.** Put in place a context-aware access policy, which restricts access to corporate assets based on the device's security posture. For example, deny access from malware-Infected devices or jailbroken/rooted mobile devices; restrict access only to endpoints with full disk encryption; and more.

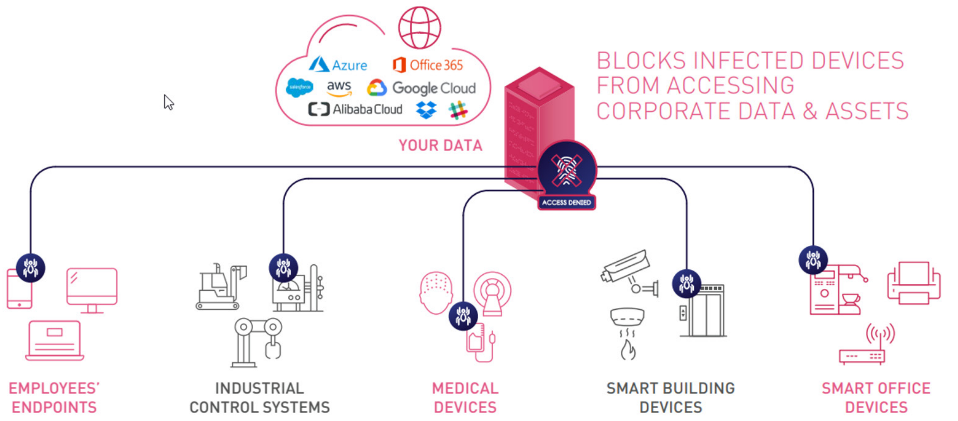


Figure 5. Zero Trust Devices, including workstations, mobile devices, IoT and OT devices

4 Zero Trust Data

CLASSIFY, PROTECT AND ENCRYPT DATA, WHEREVER IT IS

The networks of today are complex, and the journey that critical business data takes can be risky. Protecting data is challenging since it is continuously shared between workstations, mobile devices, application servers, databases, SaaS applications, and across corporate and public networks.

Taking a Zero Trust approach to data security is a must, and requires the combination of data encryption, classification, and protection wherever the data may be – whether at rest, in transit, or in use.

> **50%** of security professionals percieve data encryption, classification and protection as the most challenging security principles to implement in their organization.
>
> *— Based on Check Point Survey*

BEST PRACTICES FOR ZERO TRUST DATA

1. **Data Encryption:** encrypting data, wherever it resides, being used or is transferred, and rendered useless if stolen.
   - Enforce full disk and portable media encryption of all the information on endpoint hard drives, including user data, operating system files, and temporary and erased files.
   - Provide secure access for remote users integrating access control, authentication, and encryption (for example, IPsec VPN, authentication proxies, mobile secure container application, among others).
2. **Data Loss Prevention (DLP)**

   Enable employees to classify and protect sensitive files with inherent protection that follows them wherever they travel or however they are being shared (on public or internal networks). Use a tool that enables defining different usage permissions (e.g., view, edit, or share) for specific users regarding files and documents.

   Deploy a DLP solution for gateways and SaaS applications, so sensitive data movements can be tracked and controlled, to ensure that data does not leave the corporate network, whether via email, web browsing, or file-sharing services.
   - Identify which data on the network is sensitive and should be protected, whether due to corporate policy or different regulations (e.g., GDPR, HIPPA, and CPI).
   - Pre-define a label for every data type, for example, social security numbers, bank accounts numbers, and source code).
   - Use labels to set granular DLP policies that are content-aware. This will enable accurate identification and handling of sensitive data and reduce the number of false positives.

TIP! *To raise employee's awareness of data use policies, and release security bottlenecks it is recommended to set self-remediation DLP policies, notifying users on improper data handling in real-time, with options to send, discard or review the issue.*

5 Zero Trust Workloads

PROTECT WORKLOADS WITH EXTENDED VISIBILITY AND ADAPTABLE POLICIES

Securing workloads, particularly those that are running on the public cloud, is essential since these cloud assets (e.g., containers, functions, and VM's) are vulnerable and serve as an attractive target to malicious actors.

The cloud is a very dynamic environment, with IP addresses changing all the time, making it nearly impossible to ensure effective IP-based controls. Moreover, since cloud-based assets are provisioned and decommissioned dynamically at a very fast pace, traditional security controls are incapable of identifying them and adapting security policies accordingly.

The key to overcoming these challenges is to gain full visibility into ever-changing public and private cloud assets. It is also critical to be able to assess the security posture of these assets at all time, to quickly detect misconfigurations and security gaps, and to actively enforce policies

BEST PRACTICES FOR ZERO TRUST WORKLOADS

1. Define cloud assets intended for protection, for example – finance applications.
2. IDentify all the workloads that relate to this cloud asset and group them with the same label, for example – all VM's that belong to financial applications should be labeled as "Financial App."
3. Define internal segmentation as based on "least privilege," for example – financial applications should communicate with the customer database.
4. Use the "Financial app" label to configure an access control policy to enforce this segmentation.

A ZERO TRUST WORKLOAD SECURITY CHECK LIST

- ✓ *Seamless integration with private and public cloud environments and their native controls, including AWS, GCP, Microsoft Azure, Oracle Cloud, IBM Cloud, Alibaba Cloud, NSX, Cisco ACI, OpenStack, and more.*
- ✓ *A cloud visualization tool for constructing a real-time topology of cloud assets, including security groups, instances, firewalls, and more;*
- ✓ *Asset-driven policy management, enabling you to group cloud assets into dynamic objects (e.g. applications, security groups, etc.), and to configure policies based thereon.*
- ✓ *Threat prevention for north-south traffic on the gateway (e.g., IPS, WAF).*

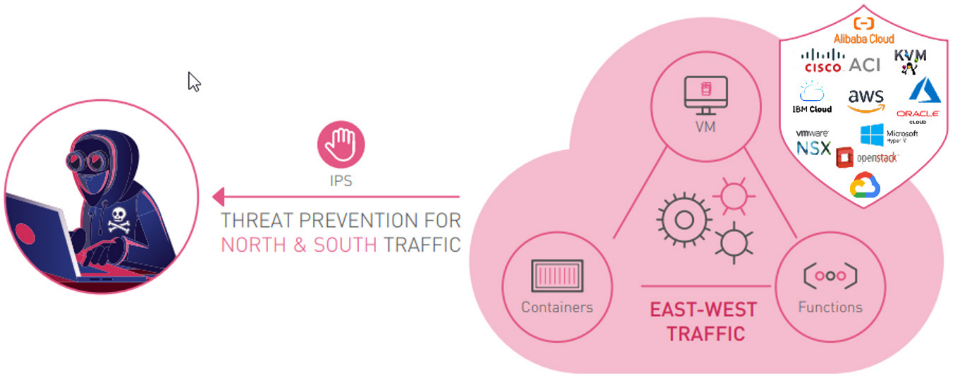


Figure 5. Zero Trust Workloads, particularly those who are running in public cloud

6 Visibility & Analytics

QUICKLY DETECT AND MITIGATE THREATS WITH A SINGLE VIEW INTO SECURITY RISKS

> "You can't combat a threat you can't see or understand."
>
> *— Forrester*

Many breaches can go undetected for months. In fact, it typically takes an average of 66 days to identify and contain a breach, according to Ponemon Institute's "2017 Cost of Data Breach Study."

To address this challenge, Zero Trust security models provide security teams improved visibility into their entire security posture, by continually monitoring, logging, correlating, and analyzing every activity across the network. This way they can quickly detect threats and mitigate losses.

BEST PRACTICES FOR GAINING VISIBILITY

1. **Establish centralized security management** with a unified view that correlates all types of events from every enforcement point, and provides full visibility into trending threats and the complete security posture.
2. **Log every activity** across the network (whether suspicious or not), including endpoints. This will provide the forensics required for incident investigation and will enable big data analysis.
3. **Use a big data analysis tool** to aggregate all security events from across every network, endpoint, and cloud in order to make the requisite correlations and identify malicious activity and security breaches.
4. **Leverage threat intelligence services** to provide comprehensive and up-to-date threat indicators that are aggregated from a large and global customer base; and ensure that this information is shared automatically among all enforcement points.

> Implementing the Threat Visibilty & Analytics principle is most challenging to **44%** of security professionals.
>
> *— Based on Check Point Survey*

7 Automation & Orchestration

USE API'S TO AUTOMATE SECURITY TASKS AND INCIDENT RESPONSE

In today's dynamic and challenging security environment, the room for error can be great. Accordingly, it is critical to eliminate reliance on time-consuming and error-prone manual work and to adopt automation and orchestration across the enterprise.

A Zero Trust security architecture must integrate with the organization's security and IT environments to enable speed and agility, and to improve incident response, policy accuracy, and task delegations.

BEST PRACTICES FOR AUTOMATION & ORCHESTRATION

1. **Reduce security admin workload:**
    - Convert repetitive security tasks into customized workflows that are executed automatically, are scheduled, and are event-driven.
    - Ensure the dynamic linking of objects in the security policy to external object stores (such as Microsoft Active Directory, or Cisco ISE), so as to free up significant staff time and decrease the risk of mistakes due to human error.
    - Delegate policy management to the relevant organization in order to reduce unnecessary communication and coordination.
2. **Automate incident detection and remediation.** Integrate security controls with the SIEM system in a way that provides deep insights on security incidents, such as event logs and threat Intelligence. Make sure the integration goes both ways, so after the SIEM performs analysis, it can trigger policy changes or provide IoC's (Indication of Compromise) for enforcement.
3. **Leverage APIs to integrate with the entire IT ecosystem.** Leverage the APIs of security solutions and products to integrate with systems such as SIEM, network management, security assessment, identity awareness, compliance testing and auditing, ticket, and workflow management, etc.

An Interesting Insight

In a survey conducted by Check Point in August 2019, security professionals were asked what are the three most challenging principles to implement in their organizations. It turns out that the answer was Zero Trust Data, Visibility and Analytics, and automation and orchestration.

Which of the following are the three most challenging principles to implement in your organization?

Please choose the top three.

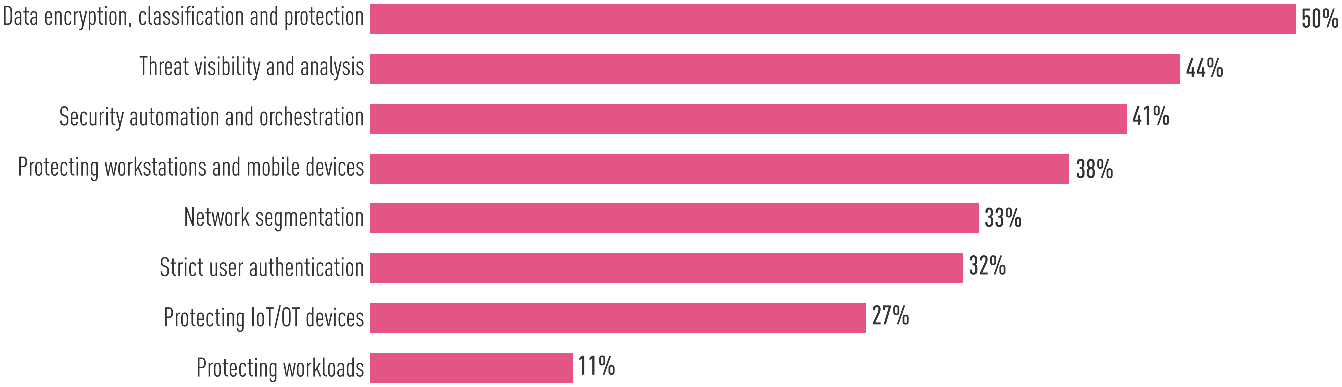


Figure 7. Survey conducted by Check Point among security professionals

Zero Trust: In Summary

As we have seen, the security environment of today is more complex than ever, with it never being more challenging to protect data, assets, and networks.

However, by following the principles of Zero Trust Security and by implementing the best practices and technologies that we have outlined so far, any organization can be supremely equipped to bolster its security posture and boost protection of its most critical data-related assets.

Absolute Zero Trust Security with Check Point Infinity

A PRACTICAL & HOLISTIC APPROACH TO ZERO TRUST SECURITY

When considering the Zero Trust strategy for cyber threat prevention, it is critical note that rebuilding the security infrastructure around this approach with disparate technologies will likely lead to complexities and inherent security gaps.

To overcome these risks, Check Point offers Absolute Zero Trust Security, a more practical and holistic approach to implementing Zero Trust, which is based on the single, consolidated cybersecurity architecture of Check Point Infinity.

The Check Point solution enables organizations to fully implement all of the Zero Trust principles. Focused on threat prevention, and managed through a centralized security console, it empowers Zero Trust implementations with unparalleled efficiency for unmatched security.

COMPLETE

Accomplishes all of the Zero Trust principles

EFFICIENT

Centrally managed using a single console and a unified policy

PREVENTIVE

Focused on threat preventiion and protects from zero-day attacks

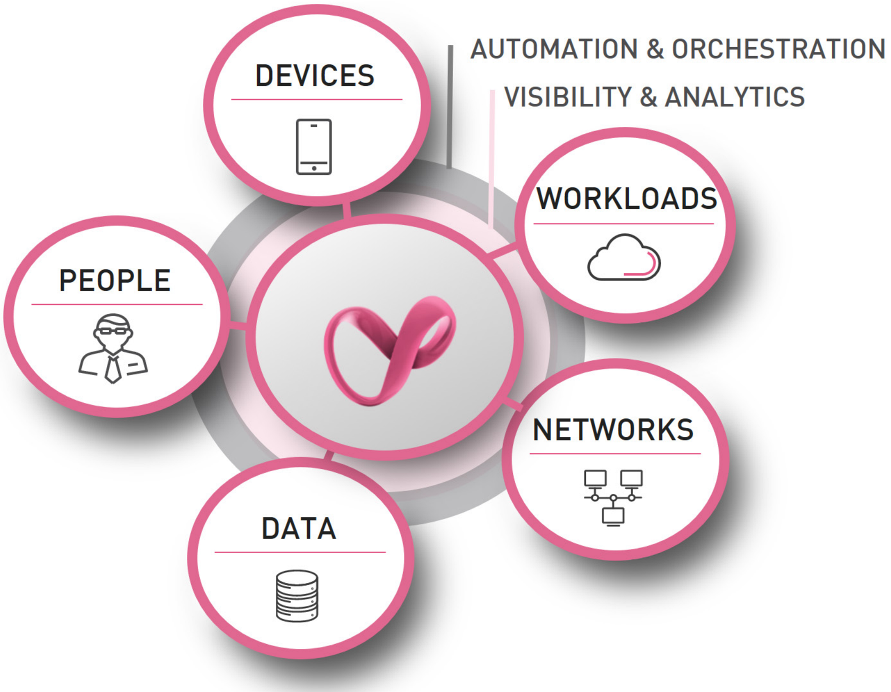


Figure 8: Absolute Zero Trust with Check Point Infinity

Click **here** to learn more about
Absolute Zero Trust Security with Check Point Infinity.

The Industry's First Zero Trust Security Workshop

START YOUR JOURNEY TO ABSOLUTE ZERO TRUST

To help organizations take a safe journey to Zero Trust implementation, Check Point offers the industry's first Zero Trust Security workshop.

The workshop was designed and is led by a team of security architects who specialize in designing and implementing Zero Trust Security models for organizations of different sizes and across multiple industries.

In this two-day workshop, we will review all aspects of your existing security infrastructure and will design a customized Zero Trust Security Strategy, along with an implementation plan for your specific business needs.

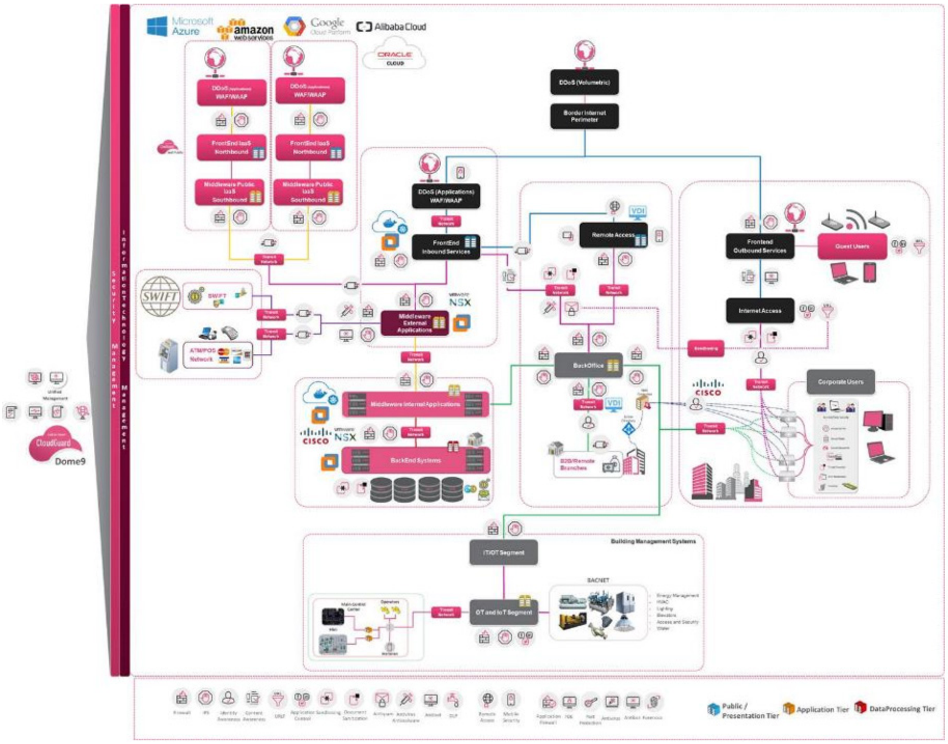


Figure 9: A Zero Trust Architecture Blueprint example designed by Check Point Security Architecture team

Click **here** to learn more about
the Check Point Zero Trust Security Workshop.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233
www.checkpoint.com