CLOUD4C

TRUST NONE, VERIFY EVERYONE:

SURVIVAL GUIDE FOR BUSINESSES IN UNCERTAIN TIMES

Navigating The New Normal

The global COVID19 pandemic has shaken the world. People are homebound. Schools, offices, entertainment - everything now comes home. While streets have emptied out, traffic on internet highways is at its peak, and burgeoning every second. The corona virus has set in motion, what Time concludes, 'the world's largest work from home experiment'. And, leading businesses such as Twitter, Facebook, Adobe and many others, have already deemed this experiment successful by announcing increased work from home options for most of their employees. But, there is a dark underbelly to this experiment too.

Security, the Biggest Concern In COVID Era

As millions of people access critical data from home, they open up the networks to unprecedented threats. The cybercriminals have found unique opportunity to take advantage of these uncertain times. IBM X-Force Research uncovered unprecedented rise in suspicious activities on the internet between February and May 2020. The cybercriminals are on prowl, setting up phishing domains, spoofing donation sites and even running campaigns targeting various work from home (wfh) applications. The businesses were never so vulnerable. The pandemic induced lockdown has trickled down business activities. And, necessity of work from home has laid their networks bare to mischief. Organizations are now staring at not just financial loss, but possible data breach, that can impact the trust and confidence of their customers. The consequences are much costlier and far reaching than one could imagine.

While businesses explore ways to stabilize and offset impact of this global pandemic, they must act fast and ensure complete network and data security. No, your traditional security architecture is not enough. Yes, your network is vulnerable even within the protection of firewalls. As millions of workers access applications, networks and systems from remote locations, each carry the key to penetrate your network. The traditional Virtual Private Network (VPN) access is not enough. Virtual Desktop Infrastructure (VDI) alone cannot keep access to critical systems and applications safe. These systems only verify users at the point of entry, leaving them free to roam once they are within the network servers. The atmosphere of vulnerability is all pervading, you cannot trust any gateway completely. And, hence you must fortify every access point, build layered security architecture to secure your networks and servers. In short, opt for zero trust security model- '**trust none, verify everyone**'.

The pandemic induced lockdown has trickled down business activities. And, necessity of work from home has laid their networks bare to mischief.

Time for Zero Trust – Trust None, Verify Everyone

Zero trust is a security model that, as the name suggests, trusts no one by default and demands strict access control. It does not allow umbrella access to network servers and restricts movement within strict confines of stated perimeter, that too for a limited timeframe. The model was designed over a decade ago by John Kindervag, an analyst at Forrester Research Inc. And, though it was being adopted by organizations keen to protect their network and data, the need was never more pronounced than now.

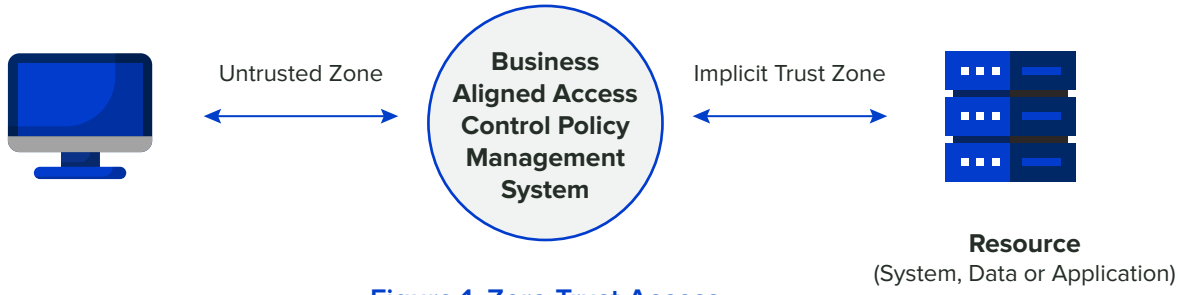


Figure 1. Zero Trust Access

Zero trust model challenges the traditional security model that protects the network perimeter with strict controls, but beyond that it gives relatively free movement access. The traditional perimeter-based security model is like installing a sophisticated lock on your main door, leaving the rooms within the house unlocked. Each of your rooms, thus is vulnerable, and dependent on the security system at the main door for their safety. Implied to business scenario, this could wreak havoc to the network and data security. Anyone with access to the network can come within the perimeter walls and the system will trust them by default, allowing them access to mission critical systems, applications and data. And, this can be the biggest risk businesses can expose themselves to, especially when large number of workforce is accessing their networks and systems remotely.

Challenges in Adopting Zero Trust Security Model

As we discussed earlier, the zero-trust approach has been around for a decade, but not many organizations warmed up to it. Apart from the fact that the businesses believed their end point security approach was adequate, the complexity and cost involved in moving to layered security, hindered large scale adoption.

It is comparatively easier to design a zero-trust architecture for a greenfield implementation than to retrofit it in existing environment. Providing least privilege with 'Need to Know' principle is the key to implement zero-trust model. But many organizations are challenged to identify sensitive data spread across multiple distributed systems, and define only 'required access' parameters accordingly. In many cases, the IT teams struggle to understand flow of sensitive data within systems and applications, in a complex environment. This increases the complexity in designing micro-segments for different streams. Further, continued monitoring for such a complex system becomes an uphill task.

The legacy systems, not geared to support least privilege and 'need to know' architecture, also come in the way. Verifying users and devices at every point, before granting access is not easy, if the environment is running on legacy systems. At times, when systems speak to each other in a peer to peer network with least verification, the threats become larger. The classification of data into sensitive and less sensitive, and then building a strong access control design is effort, time and cost intensive.

Implementing Zero Trust Security Architecture

That the organizations need a zero-trust security model, thus, brooks no argument. The question however is, how does one go about it? To answer this, we need to understand Zero Trust Security Model in some detail.

Zero Trust Model has two main components – traffic within network, and end user access. Interestingly, most organizations focus exclusively on end user access control that amounts to about 20% of threat, leaving their internal traffic exposed to mischief, that could be as high as 80%. The businesses can build a robust zero trust architecture, securing their networks, applications and services with proactive access management and micro-segmentation of networks, to implement layered security gateways.

The guiding principle to design zero trust security architecture is to secure 3 Ws – Workforce, Workload and Workplace. This translates to only authorized users and secure devices getting access to specific zones, securing all connections within applications as well as, users and device connections across networks. The access parameters are business defined and are deployed through 3 Ps – a robust Policy Engine (PE) that decides on access permissions based on data access policies, Policy Administrator (PA) that manages the communication path and, Policy Enforcement Point (PEP) that monitors and acts against unauthorized access.

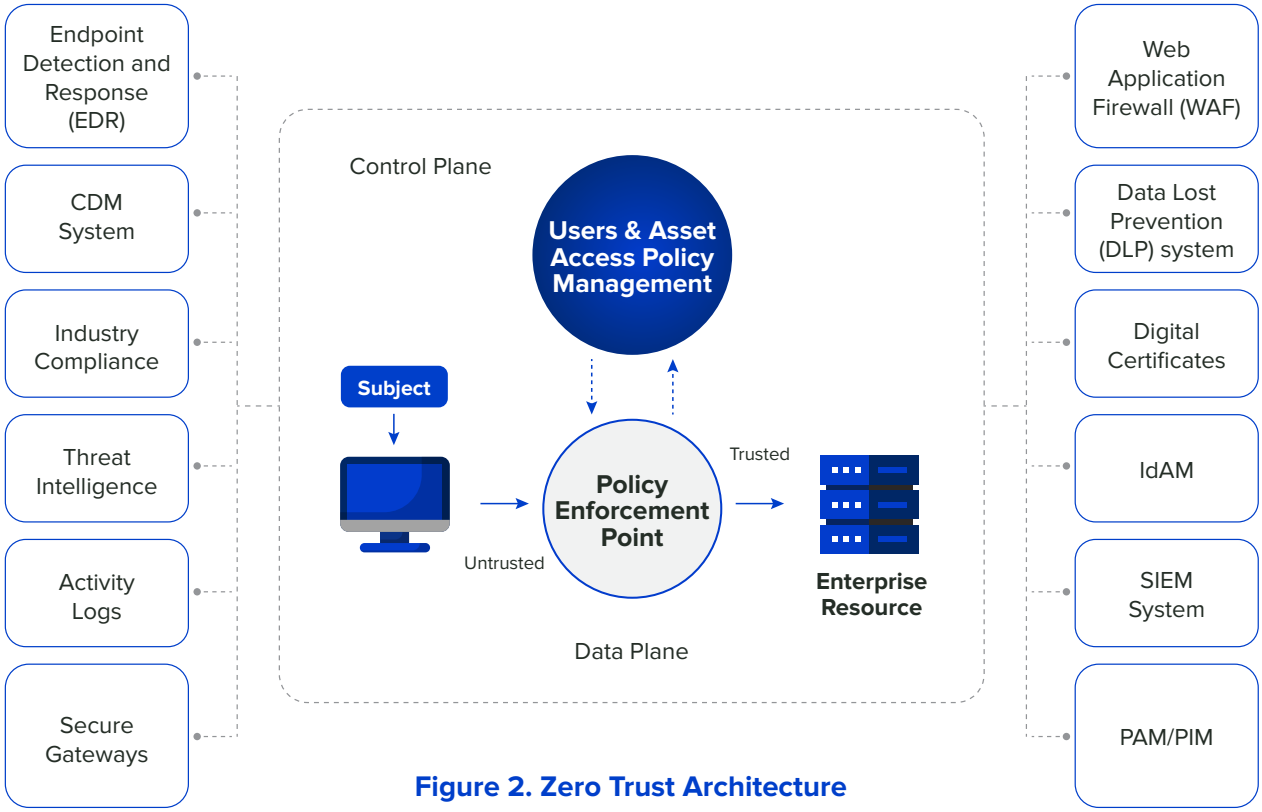


Figure 2. Zero Trust Architecture

Software Defined Networks (SDN), the Baseline for Zero Trust Security

The first step to implement zero trust security model is put in place Software Defined Network (SDN) environment. Leveraging SDN tools, network and engineering teams implement micro-segmentations to be vigilant of virtual environments. The software defined networks monitor each micro-segment and pre-empt threats to data, workloads and applications. The systems are isolated from each other to contain any malicious activity within a periphery. These create additional filters for assets, securing them against any mischief.

SDN environment is based on the extensive understanding of any movement within the firewalls and network, allowing the organizations to define controls based on their needs. The basic principle of SDN architecture is to ensure webservers are not interconnected and that the respective webservers speak to the required applications, maintaining the sanctity of network servers. The solution can be designed with unique policies and conditions defining the role and activities for webservers. SDNs are designed with deny-by-default architecture to check any unauthorized intrusion and forward access requests that match proactive traffic-engineered flows.

The basic principle of SDN architecture is to ensure webservers are not interconnected and that the respective webservers speak to the required applications, maintaining the sanctity of network servers.

Once the SDN environment is defined, organizations can implement zero trust network with Privileged and Identity Access Management (PAM), Endpoint Detection and Response (EDR), Web Application Firewall (WAF), Security information and Event Management (SIEM) and Host Data Loss Prevention (HDLP) processes. These can be complemented with an intuitive and agile Continuous Diagnostic and Monitoring System (CDMS) that ensures all the assets are running the on the latest updated version and all security patches are in place. At the user access level VDI and VPN with MFA/2FA can be better monitored for a completely secure environment.

Security information and Event Management (SIEM)

SIEM is the gatekeeper for the entire security landscape. The system collects feed from the heterogeneous environment – networks, servers, applications, databases, as well as the threat intelligence feeds. The collected feed is monitored and analyzed real-time using cross device correlation and alerts are triggered for violations. The organization now has a Holistic 360° view of the complete infrastructure security landscape. The constant real-time monitoring of network and systems activity logs using multi device correlation helps identify event, risk, behavior and historical log anomalies. The system upholds the sanctity and stability of the security configuration changes by flagging any deviation from the defined security policy at the very early stage, plugging pilferage and possible incidents breaches.

According to a study conducted by IBM, it takes 206 days on an average for organizations to detect a breach, and a further 79 days to contain it. This reveals the vulnerability of our security ecosystem. These challenges can be overcome with zero trust micros-segmentation. The 'need to know' principle applied along with other security components, makes lateral movement harder for attackers. The time any mischievous act would take to breach the system is increased while detection time for such incidents is drastically reduced, as the system is quick to detect any anomalies, triggering instant alarm for violations. A robust incident management system covering the entire lifecycle - Prepare, Detect, Analyze, Contain, Eradicate, Recover and, Post Incident analysis – along with cross device correlation reduces false positives and incrementally enhances the security posture of any organization.

Secure Identity Management

Managing identity of users and devices seeking access to different zones in IT landscape is a core component in zero trust security model. This is carried out through Privileged and Insider Access Management (PAM) and Enterprise Public Key Infrastructure (PKI).

PAM is put in place to secure internal user access. The privileged and insider users pose grave risks as they can change system configuration settings, read and modify sensitive data, or grant access to other users. Their inadvertent actions can provide an open field for attackers to cause maximum damage. Privileged access accounts are generally owned by admins managing domain, application, services, emergency and business accounts. In the traditional perimeter security approach, the privileged and inside user has free movement inside network.

Zero trust architecture monitors and restricts privileged to protect the assets. Even the inside user access is highly regulated, designed on the principles of "least privilege", limited to exactly what is needed and not beyond. This involves micro-segmentation of networks along with role-based access controls (RBAC) and assets within the network. Each micro segment or zone requires separate access permission, granted for a specific time period. In the zero trust architecture, the admin will have access to only to the required server and that too for a stipulated time, leaving no room for any mischievous activity. PAM also video records user sessions for post incident monitoring.

For instance, in the event of an incident involving a specific server, the admin has to verify her credentials to enter the server environment and has free access to all the servers, allowing easy lateral movement. But in zero trust environment, even privileged and inside users are authenticated to access the required server and are not allowed any lateral movement.

Additionally, PKI is installed to generate and log certificates issued by the enterprise to resources, subjects, and applications. This ensures that the users or applications with valid certificates are entertained within the environment. Any violation or an expired certificate is detected and alerts are triggered to prevent unwanted intrusion.

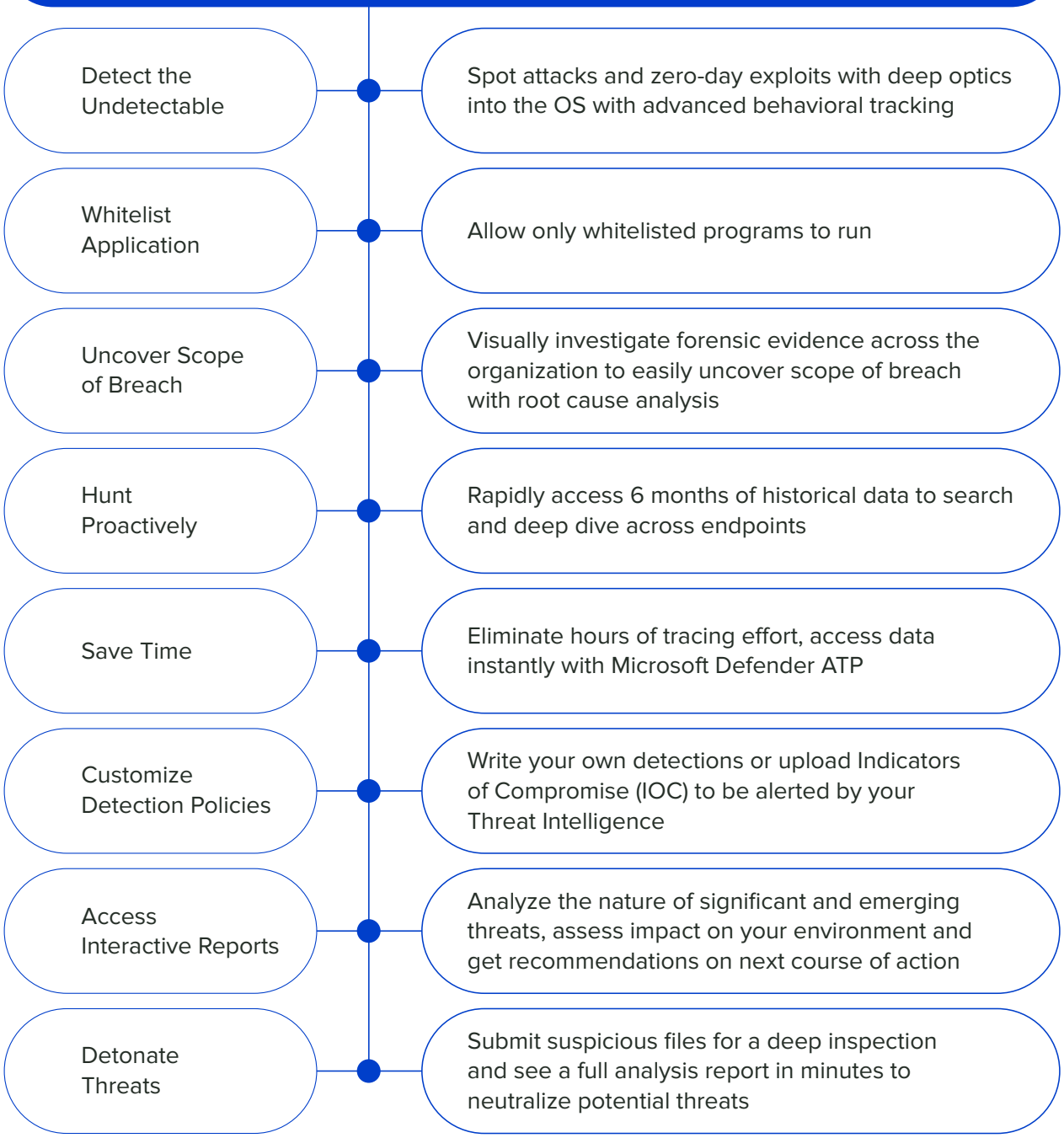
Endpoint Detection and Response (EDR)

Malware-as-a-Service has emerged as an organized threat to endpoint security. With increased work from home scenario the threats are more pronounced. There is a substantial increase in ransomware attacks with higher impunity. In fact, there has been a whooping 97% increase in ransomware attacks, costing an estimated $75 million to businesses every year. Research suggests a new organization is prone to a ransomware attack every 11 seconds, by 2021. And given the current scenario, the window can well be shrinking. These sophisticated cyberattacks are designed to sabotage digital estate of various vulnerable industries including BFSI, healthcare, retail and others and often extend to their cloud environment. The threats emanate from unpatched systems exposed to advanced persistent threats, high on velocity and stealth in nature.

The threat of malware also looms large. A malware with worm capabilities before spreads over network even before any access can be authorized. This can cause immense damage. Systems that require manual intervention are more susceptible to malware attacks. Lack of Security Orchestration, Automation and Response (SOAR) capabilities is recognized to be a major roadblock in securing the landscape. SOAR is a solution stack that automates detection and reporting of low level security threats.

The way to ensure endpoint security is to correlate vulnerabilities with endpoint detection and response (EDR) alerts to expose breach insights. This would involve micro-segmentations or micro-configuration for continuous discovery of vulnerabilities and prioritization aligned to business context while analyzing the dynamic threat landscape. Here are is an innovative approach to EDR.

Innovative Endpoint Detection and Response (EDR)



Web Application Firewall (WAF)

The Web Application Firewall is mostly under threat when users connect and access data from untrusted devices. Needless to say, the threat has increased manifold in COVID19 era. The threats to WAF include injection of malicious code for weak input fields, misconfigurations when applications are not adequately hardened and vulnerabilities in patching. Often web applications are attacked on stolen credentials or with brute force.

Most organizations have limited in-house resources to maintain web application and keep monitoring release of patching, vulnerabilities and end of life operating system. An evolved and system to manage and configure WAF as per industry best practices require distinct skill sets.

The solution design has to be self-learning in order to analyse the patterns and differentiate between legitimate and suspicious patterns. The best approach to WAF is to form a vulnerability management team that stimulates OWASP TOP 10 based attacks to understand critical vulnerabilities and signatures to monitor application behaviour.

Post stimulation and review of assessment report specific true positive signatures can be enabled to auto protect. If issues persist with prevent mode alternative compensative controls can be deployed. These attacks must be monitored with a competent SIEM solution, preconfigured with correlation rules to detect OWASP top 10 based attacks.

Host Data Loss Prevention (DLP)

HDLP is the process of monitoring and blocking intentional and unintentional exfiltration of data by employees or third parties through host systems. Research suggests that 2 out of every 10 organization is at the risk of accidental data leaks by staff, and the threat has only grown in the current circumstances. Employees working from unsecured remote locations can pose a threat to company data by sharing it over personal email or open shared drives. They may mistakenly delete or overwrite sensitive data causing reputation loss to the organization. Employees with access to customer information, financial data, intellectual property, transaction data or protected health information can expose the organization to potential high risk.

An intuitive information security design aligned to host data loss prevention strategy must be in place to protect sensitive data. There must be policies and processes to control users' capability to transfer sensitive data through different communication tools including email. Further, data transfer to employee's personal cloud drives like Google Drive and Dropbox or through SSH, FTP and RDP outside the organization's purview can be arrested with continuous monitoring of user desktop. There can be restrictions in usage of certain websites to prevent them from leaving cookies or indulge in phishing exercises to compromise host data.

Protecting End User Access

Abuse of VPN accounts and concurrent session of the same user from different locations makes monitoring difficult. Organizations maintaining a bird eye view on complete remote location user activities gain the upper hand. Continuous tracking and managing assets on the cloud with required back up and change log equips them to protect their applications from misuse. The systems and assets can be protected with a robust monitoring and tracking system that identifies blacklisted IPs and assigns reputation score to the user home network by validating IP reputation with threat intelligence feeds.

Time to Act is Now

Moving to zero-trust model is often considered a complex and long drawn, put off for another day. But that day has arrived now. The businesses cannot afford to put off redesigning their security architecture anymore. The stakes are too high. In a way, it is an existential battle and no business can afford to be on the wrong side of it. Can businesses manage the complexities and secure their networks and systems with zero-trust architecture? Of course, they can. The technology has matured and the complexity in implementation is gradually being simplified by expert security architects. The availability of required talent has also substantially increased in past few years. This has helped organizations get over the roadblock to secure their complete IT environment.

The businesses are advised to adopt a phased approach and take incremental steps. They can begin at OS level and progress towards application and service level migration to zero trust architecture.

While the pandemic has made work from home a norm, most organizations do not have enough checks and balances in place to protect their environment. Sample this, research reveals that 86% of executives claim data breaches are more likely to occur with remote workers, only 35% are prepared to keep their information secure off-site. And this was before COVID 19 era. Organizations cannot afford to leave their IT environment vulnerable with the traditional perimeter security model. The cost of not implementing zero trust environment is much higher, both in financial terms and in terms of loss of reputation. In the new normal world, data is sacrosanct. Maintaining data sovereignty and fortifying systems against any breach has to be the top most priority for every organization. A fully functional zero trust environment can be designed and implemented in 6-8 weeks' time, depending on the complexity and breadth of the network. This is not time to be on the fence and weighing options. This is the time to act. Act now.