WHITE PAPER

Enforce a Zero Trust Security Model in Today's Hostile Environment

云智慧 Cloudwise

Akamai

Executive Summary

Companies of all types are pursuing digital transformation. The goal is to improve customer value, operate with greater efficiency and agility, and increase innovation. But as companies leverage new cloud and DevOps workflows to build their digital business, security has not kept pace. The proliferation of cloud applications and an increasingly mobile workforce have fundamentally reduced the effectiveness of the network perimeter. Applications, data, users, and devices are moving outside of the enterprise's zone of control, fundamentally increasing the attack surface. As infrastructure becomes more permeable to enable new business models, cyber criminals are becoming more adroit, sophisticated, and incentivized to find ways to circumvent security measures. Traditional perimeter security was never designed for today's reality.

In the face of proliferating cyber attacks, and the associated breaches that follow, how can companies protect themselves? This white paper describes a security paradigm for today's hostile environment: zero trust. Using this model, users and devices are never trusted, and the environment is assumed to be hostile. Zero trust highlights that there should be no trust distinction between internal and external networks. With this model, all access requests and devices are always verified with full logging and behavioral analytics. Additionally, this paper will address why IT should look to embrace cloud services to move away from perimeter security.

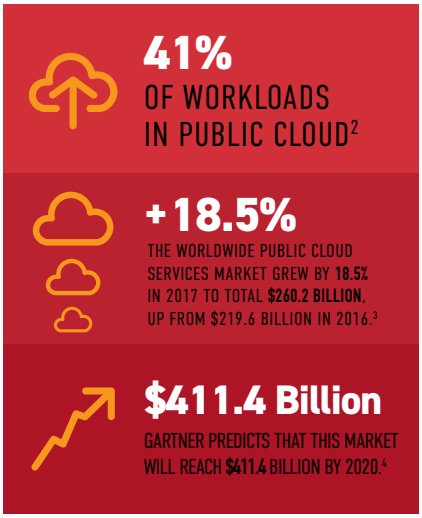
Digital Transformation Is Omnipresent

Significant digital transformation is now ubiquitous across the majority of industries. And the trend is accelerating. IDC Research predicts that global digital transformation investment will reach $2.2 trillion in 2019, an almost 60% increase from 2016.[1]

Companies are leveraging advanced cloud and network architectures to deliver new customer value while increasing operational efficiency, agility, and innovation. Digital transformation benefits consumers by allowing companies to offer digital products, better services, personalized interactions, and a superior customer experience. Employees take advantage of digital technologies to easily communicate and collaborate online, enhancing productivity and morale.

The Trusted Perimeter Is Dead

But while leveraging digital services brings many benefits, companies are seeing their attack surface grow in today's increasingly hostile threat landscape. As a result, they need to rethink the fundamentals of perimeter security and the manner in which they protect their critical applications, data, and users.



Digital transformation has a profound impact on the way companies deliver IT solutions, as well as their threat exposure. Traditionally, users have interacted with applications in a trusted manner across private local area networks (LANs), wide area networks (WANs), or virtual private networks (VPNs). Companies adopted perimeter security, such as firewalls, VPNs, and network access controls (NACs), to keep cyber criminals out of internal networks. Once inside the network, users were inherently trusted to go where they pleased.

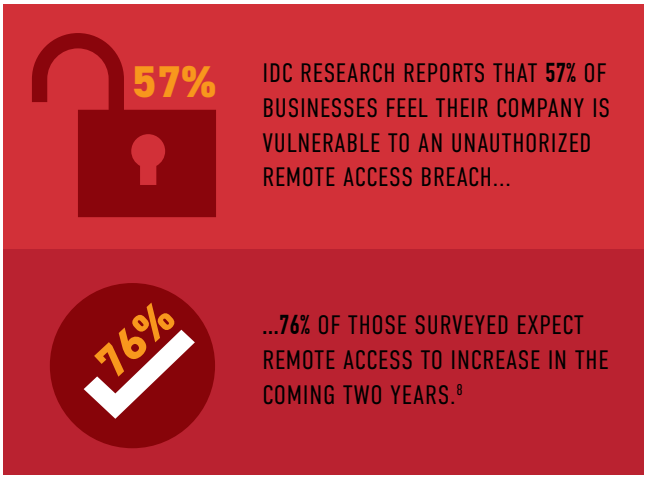
As companies undergo digital transformation, they are turning inside out. Applications increasingly reside in the cloud, outside of IT's traditional zone

of control. Respondents to a RightScale survey reported that they run 41% of their workloads in the public cloud.[2] The worldwide public cloud services market grew by 18.5% in 2017 to total $260.2 billion, up from $219.6 billion in 2016.[3] Gartner predicts that this market will reach $411.4 billion by 2020.[4]

Employees no longer connect primarily from within the four walls of an office. Many employees are frequently on the road or working remotely, spread across the globe, connecting via unsecured networks. PGI's Global Telework Survey found that 79% of global knowledge workers are telecommuters.[5]

Additionally, the idea that a digital business employs only fulltime workers is outdated. Most companies depend on suppliers, vendors, contractors, and partners who require access to specific, internal applications to be productive. Not surprisingly, any third-party access increases the risk that critical corporate information could fall into the wrong hands. Additionally, the proliferation of Bring Your Own Device (BYOD) policies means that IT has less control over the devices that users employ to access corporate applications and data.

At the same time, cyber criminals are increasingly finding their way through the firewall. Some enter with trusted user credentials, others via malicious links or attachments. Symantec Research found that the email malware rate has increased significantly from 1 in 220 emails sent containing malware in 2015 to 1 in 131 emails in 2016.[6] And once attackers have breached a network, they are not detected for a global average of 146 days.[7] IDC Research reports that 57% of businesses feel their company is vulnerable to an unauthorized remote access breach, and 76% of those surveyed expect remote access to increase in the coming two years.[8] The losses from unauthorized remote access are high. On average, businesses expect to cede $6.5 million to this cause.[9]



Traditional Perimeter Security Is Inadequate

With corporate applications, data, devices, and users moving outside the perimeter, and cyber threats moving inside, traditional perimeter security is no longer sufficient.

Companies have long protected corporate networks using perimeter stacks, or DMZs, that include appliances for access control (VPN appliances, identity providers, single sign on/multi-factor authentication, client-server), security (web application firewalls, data loss prevention, next-gen firewalls, secure web gateways), and application delivery and performance (load balancing and optimization). But these perimeter architectures were never designed to optimize the experience for users that are accessing applications from a variety of locations. Additionally, they weren't designed for Software as a Service (SaaS) or applications hosted in the cloud. To overcome this, IT departments often have to repeat these stacks for redundancy and high availability across multiple regions and data centers as necessary, increasing cost and complexity.

As applications move to the cloud, companies no longer have the same control — traditional network security based on packets, ports, and protocols doesn't work when companies don't manage the full application environment and network.

Companies will continue to run both on-premises and cloud applications for the foreseeable future. They will need to maintain a patchwork of access control and security solutions that may not play well together, and will have no central place to manage and control these technologies. Fragmented systems lead to increased risk and reduced visibility.

To top it all off, the premise underlying perimeter security — that walls work — has become obsolete. Criminals often gain entry onto corporate networks by using legitimate usernames and passwords or installing malware that finds

weaknesses in existing security solutions. A recent report revealed that 91% of cyber attacks start with a phishing technique designed to steal authentic user credentials.[10] Perimeter solutions do nothing to safeguard corporate data and applications from attacks that originate inside the perimeter.

The New Age of Zero Trust

With traditional perimeter security taking its last breaths, how should organizations protect applications, data, and their workforce from ever-increasing, high-profile cyber security threats? The answer is to implement a zero trust security model that changes the common mantra of "trust but verify" to "never trust, always verify."

Originally championed by Forrester Research, a zero trust security model assumes that there is no "inside" and that everyone and every device is equally untrusted. It treats all applications as if they face the Internet and considers the entire network to be compromised and hostile. Core components of zero trust include:

- Ensure that all resources are accessed securely, regardless of location or hosting model
- Adopt a "least privilege" strategy and strictly enforce access control to limit the risks associated with excessive user privileges
- Inspect and log all traffic for suspicious activity to improve security detection and response

Long Live the Cloud

As users, devices, data, and applications continue to evolve, the capabilities that enforce the zero trust approach should exist in the cloud and use the Internet as its core network. Rather than using firewalls that block IPs/ports, cloud-based security should focus on the application layer and higher level protocols. Utilizing cloud-based security controls should empower companies to close off their firewalls and hide internal applications from the Internet. Authentication and authorization services then control access from managed and unmanaged devices to every application, whether they're on-premises, running on an Infrastructure as a Service (IaaS) platform such as Amazon Web Services, or are SaaS applications.

The cloud-based security controls should verify all outbound DNS requests coming from company devices — including laptops and Internet of Things (IoT) devices — to ensure that they are not headed for malicious or unacceptable sites. The solution should also monitor and analyze traffic behavior for signs of suspicious activities, such as communication with a command and control (CnC) server or data exfiltration, and alert IT to any issues immediately.

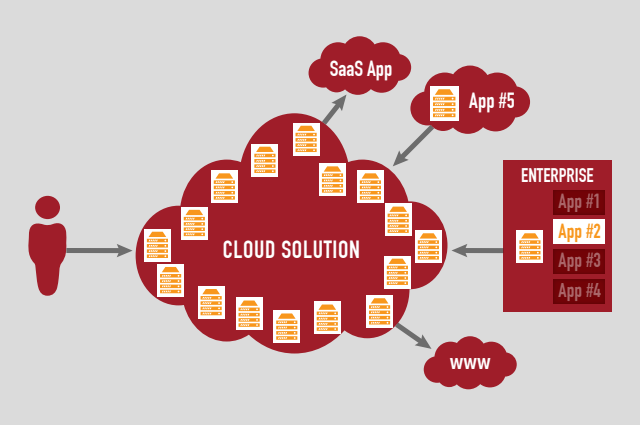
Implementing zero trust via the cloud solves most challenges with outdated perimeter network security. It ensures that authenticated users are authorized access only to permitted applications. It also prevents infected endpoints from accessing malicious or unacceptable websites, or from connecting to malicious CnC infrastructure that can take control of users' machines and exfiltrate data. Furthermore, it can block malware from moving laterally across the network.

Enabling Zero Trust with the Cloud

Businesses can reduce their attack surface by employing a cloud service to enforce a zero trust security model while enjoying the agility, scale, and cost advantages of the Internet.

Protected Access

Companies undergoing digital transformation need to provide employees, suppliers, consultants, and other partners with fast, easy, and safe access to applications that are behind the firewall from any device, anywhere in the world. Traditional access technologies typically use a variety of hardware and software appliances to give network access to any user with the proper credentials. However, studies have shown that most breaches result from valid user credentials that are either stolen or improperly used. A zero trust security model assumes that all users are compromised and should not be trusted.



Using the cloud as an extension of your infrastructure enables zero trust access by providing entry to only the applications that users need rather than to the entire network. This principle of least privilege extends to all devices and applications anywhere in the world.

With cloud-based security, direct access to applications is disallowed since all applications are hidden from the Internet and public exposure. The cloud lies not only in the authentication and authorization path, but also directly in the user's data path, and is the only entry point for users to gain access to critical enterprise resources. The cloud service provides a secure, mutually authenticated TLS connection from within the corporate network or IaaS and delivers the application to the user. Secure proxies apply strong authentication and security controls. These capabilities isolate internal networks and IaaS applications from the Internet and move the attack surface to the edge.

Authentication

To give users secure access to applications and high-value data, cloud-based security should integrate with existing authentication services (e.g., Okta or Microsoft Active Directory) or provide its own authentication solutions with advanced security features, such as two-factor or multi-factor authentication. Requiring authentication for both the device and the user further enhances security because an attacker must steal at least two identities to gain access to resources, significantly improving on traditional approaches.

The cloud should further enhance security by authenticating users outside of the user's infrastructure without requiring additional hardware or software.

Authorization

By adopting a least privilege access strategy and strictly enforcing access controls, organizations reduce the pathways available for cyber criminals and malware to gain unauthorized access. A cloud solution can help by explicitly providing application-specific access rather than applying blanket privileges. Organizations can define security policies across all users, devices, applications, and data.

Layered Security Defenses

While a zero trust network tightly controls access to all network resources, applications are also subject to distributed denial of service (DDoS), structured query language injection (SQLi), application-layer attacks, and more. Cloud-based security should offer additional layers of defense that can help protect against these attacks. DDoS protection safeguards against attacks that flood targeted apps or sites with superfluous requests in an attempt to overload systems and compromise legitimate users' access to the application. Application-layer security guards against attacks, such as SQLi, that manipulate, corrupt, or delete data. These solutions also protect against the often-seen technique of using DDoS as a diversionary tactic; criminals will promulgate a DDoS attack at the same time they're attacking the application layer with SQLi or cross-site scripting (XSS).

Proxy-based Inspection of All Traffic

While access controls secure known applications, many employees and partners use Internet-based applications, such as Google or Trello. While these applications can be a boon to workforce productivity, websites can also host nefarious malware or unacceptable content such as hate speech or pornography. Additionally, phishing attacks — which leverage links to malicious domains — are on the rise and are a source of malware attacks. While most companies have layers of protection in place, DNS-based data exfiltration remains a major security gap for most companies.

Instead of resolving all DNS requests blindly, businesses need to employ cloud-based security controls to effectively apply real-time intelligence and provide proactive protection against ever-evolving threats. Cloud-based security services should be able to act as a recursive DNS server, check the domain names against a robust and frequently updated list of known malicious domains, apply its intelligence, and administer policies that prevent requests from proceeding to malicious domains or domains with unacceptable content. Because this validation occurs before the IP connection is made, threats can be stopped earlier in the security kill chain.

Zero trust becomes exponentially more important as companies increasingly employ IoT devices. For example, IT may be unaware that a connected TV in a conference room is making requests to malicious domains on the Internet — an action potentially indicative of compromise.

Live Threat Intelligence

"Always verify" implies the need to continually monitor and inspect traffic for activity. Zero trust assumes that even traffic originating on the LAN is suspicious and should therefore be analyzed and logged as if it came from the Internet. Behavioral analytics identify suspicious traffic patterns, such as those that indicate communication with a CnC server or data exfiltration.

Conclusion

By enabling zero trust with a cloud-based architecture, companies can adjust cyber security to today's new IT realities. Whether applications and data reside in the data center or in the cloud, companies can provide users located anywhere, using any device, with secure, simple, and performant access. They can prevent users from accessing external applications containing malware that might compromise the network or that contain unacceptable content. And they can continually monitor traffic for suspicious behavior. As a result, companies can fully leverage the latest technologies to enable digital transformation — with the peace of mind that comes from knowing that high-value data and applications will remain secure.

Sources

1. https://www.idc.com/getdoc.jsp?containerId=prUS41888916
2. www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey
3. https://www.gartner.com/newsroom/id/3815165
4. https://www.gartner.com/newsroom/id/3815165
5. https://www.ondeck.com/blog/your-complete-guide-to-the-remote-workforce-in-2017
6. https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_
7. https://www.fireeye.com/company/press-releases/2016/fireeye-releases-first-mandiant-mtrends-emea-report.html
8. https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
9. https://www.computerworld.com/article/3222829/security/state-of-remote-access-security.html
10. https://www.darkreading.com/endpoint/91--of-cyber attacks-start-with-a-phishing-email/d/d-id/1327704?