The 6 Business and Security Benefits of Zero Trust

Zero Trust Delivers Security Plus Impressive Business Results

Businesses today operate much differently than they did just a few short years ago. Employees, devices, even applications are no longer locked away inside of the corporate perimeter. They're on the web and on the go. Providing security for a new breed of anytime, anywhere workers and cloud-based applications requires a novel approach. Organizations are increasingly turning away from solutions that secure the perimeter and then trust everything inside and are instead moving to a zero trust security model to protect sensitive resources and data.

Under the assumption that every user, request, and server is untrusted until proven otherwise, a zero trust solution dynamically and continually assesses trust every time a user or device requests access to a resource. This approach prevents attackers from exploiting weaknesses in the perimeter to gain entry, and, once inside, move laterally to access confidential applications and data.

But zero trust offers more than a line of defense. The model's security benefits deliver considerable business value: greater enterprise visibility, reduced IT complexity, less demanding security workloads, data protection, a superior user experience, and support for cloud migration. This white paper describes the six security and business benefits afforded by the enterprise's adoption of zero trust.

1. Protect Your Customers' Data — and Your Business

Once malware makes its way onto an end-user machine within the firewall, it can exfiltrate customer data to a command and control (CnC) server outside of the network. Allowing private and confidential customer data to fall into the wrong hands can have serious consequences for both your customers and your business. Impacts include:

- **DISRUPTION FOR CUSTOMERS:** Stolen personally identifiable information wreaks havoc on customers' lives. Cybercriminals may use misappropriated customer data to steal identities and/or access or open financial accounts, ruining credit scores as well as making life events such as homeownership, maintaining a driver's license, holding a job, and filing for a marriage license extremely difficult for the victim. Though benign compared to the theft of a Social Security number or home address, leaked personal details such as where the customer grew up, where they vacation, and who their friends are may be the missing links that scammers need to access the victim's accounts.

- **REPUTATIONAL DAMAGE:** Many regulations, including the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), require customer breach notifications should a data breach occur. The resulting loss of customer and stakeholder trust is exceedingly harmful for an enterprise because many people refuse to do business with a company that has been breached, particularly if it failed to protect the customers' data.

- **LOSS OF INTELLECTUAL PROPERTY:** Stolen intellectual property or strategic plans can cost your company years of effort, R&D investments, trade secrets, or copyrighted material — and potentially wipe out your competitive advantage.

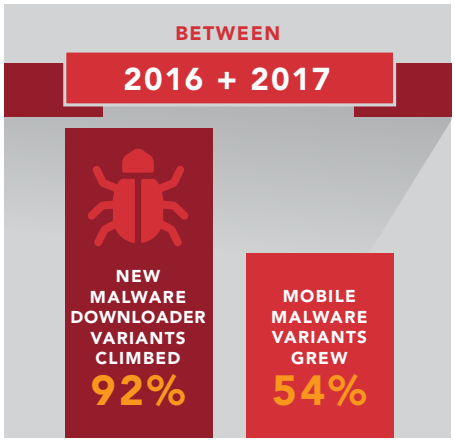
- **FINANCIAL COSTS:** In the wake of a breach, companies face all manner of direct and indirect costs. Customers' refusals to do business with a breached company will naturally result in lost revenues, but indirect expenses can be equally, if not more, financially damaging. These costs might include higher insurance premiums; customer and crisis management; incident response, investigation, and security audits; operational disruption, employee turnover, and recruiting services for hiring new CISO and/or security staff; and legal fees, settlements, and regulatory fines. Consider, for example, GDPR: As of May 25, 2018, those who do business with European Union residents but fail to comply with GDPR regulations designed to protect sensitive customer data can be fined 20 million euros or 4% of global annual revenues, whichever is higher.

Enforcing an effective zero trust solution — ensuring that only authenticated and authorized users and devices can access applications and data — will help to mitigate data exfiltration, preventing many of these negative consequences.

2. Reduce Time to Breach Detection — and Gain Visibility into Your Enterprise Traffic

One of the core tenets of zero trust is that location is not an indicator of trust — therefore, the network is assumed to be hostile. Zero trust replaces the principle of "trust but verify" with "always verify and never trust." And visibility is the foundation of verification.

After all, you can't verify what you can't see. Zero trust provides security professionals visibility into exactly who is accessing the network, from where, which applications, and at what time. Security administrators and systems can monitor the activities of all users, devices, and data, whether they're internal or external. Predictive and behavioral analytics then evaluate all of this data to effectively apply security policies, enforce compliance, and reduce risk. When preventative controls fail, security teams rely on network and application visibility to quickly identify and respond to security incidents.



USERS/REQUESTS

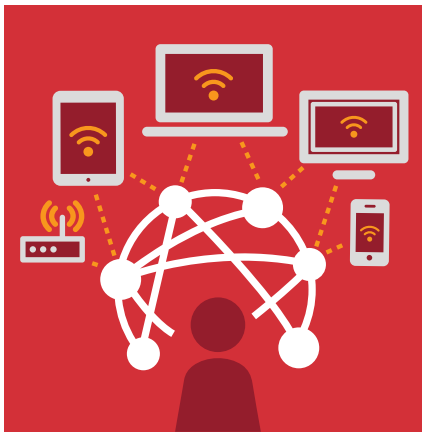
Malware attacks are increasing exponentially. Between 2016 and 2017, new malware downloader variants climbed 92% and mobile malware variants grew 54%.[1]

Most malware attacks begin when users fall for phishing schemes, visit malicious websites, or plug external drives compromised by malicious code into their devices' USB port. The malware then "calls home" to a CnC server on the Internet for further instructions. The Domain Name System (DNS) cannot determine whether the destination of a request is a malicious or safe domain; it simply resolves requests. The CnC server can then download updates to the malware or additional components onto the compromised machine, exfiltrate confidential data, or even install ransomware.

A hacker who penetrates the perimeter of a traditional enterprise security framework can often work undetected and will move laterally within the target network to infect additional hosts. This movement ensures that if one compromised system is detected, the cybercriminal continues to maintain access. These newly affected systems also begin to call home

by sending beacons to the CnC servers. This pattern continues as the hackers perform reconnaissance on the targeted systems, establishing a shadow network within the enterprise's infrastructure. Infected devices, including smart devices connected to the Internet, can also become part of a bot network of zombie devices that participate in attacks and amplify the malicious actor's reach, unbeknownst to the machine's owner.

With existing perimeter-based security systems, it's difficult to track and monitor DNS requests to external domains. Most companies don't audit this traffic due to the sheer volume of data there is to analyze. Zero trust provides visibility into user behavior in real time so that IT teams can spot calls to a CnC server and/or lateral movement quickly, and then trigger immediate intervention such as prompting multi-factor authentication.



DEVICES

A single device can make several thousand queries per day. Each user likely has multiple devices on the network. The sheer volume of requests prevents enterprises from entering all of this data into security information and event management (SIEM) systems that might be able to provide network-level visibility. And the time it would take to manually dig through data to identify which devices are making requests renders this approach obsolete. As such, it's incredibly difficult to understand what constitutes normal daily traffic and from which devices.

A zero trust solution that provides visibility into device type can very easily alert you to a problem. For example, while a laptop making thousands of recursive DNS queries a day shouldn't raise an alarm, a building's HVAC system sending superfluous requests should be investigated further.

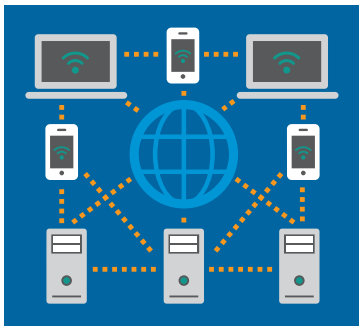
A cloud-based zero trust service that can correlate traffic on your network with traffic from other networks makes it easier to understand and identify trends that indicate irregular traffic.

DATA

As DNS traffic is unfiltered and open in traditional networks, malicious DNS queries typically go unchecked, bypassing all network-level security. As discussed above, bad actors often use DNS tunneling to exfiltrate sensitive financial records, Social Security numbers, credit card info, and other sensitive data. These data packets are encrypted, compressed, chopped, and transmitted outside of the perimeter to an external criminal server. Zero trust-based solutions inspect all traffic and use analytics to detect DNS-based data exfiltration.

3. Reduce the Complexity of the Security Stack

Implementing security with legacy technologies is very complicated and expensive. The traditional perimeter often consists of virtual or hardware appliances for access control (VPN appliances, identity providers, and single sign-on [SSO]/multi-factor authentication [MFA] hardware or software), security mechanisms (web application firewalls, data loss prevention, next-gen firewalls, secure web gateways), and application delivery and performance utilities (load balancing and application performance optimization).



To function in a global setting, these stacks must be repeated for redundancy and high availability across regions and data centers. You must purchase, install, configure, and deploy each one of these components separately for each data center in multiple localities. Administrators must then manage all of this equipment in-house, taking charge of ongoing monitoring, troubleshooting, patching, and upgrades.

Cloud-based zero trust solutions remove that complexity by shifting all of these functions to a cloud-services approach. The cloud vendor takes over all of these responsibilities while enabling your organization to move from a CapEx to an OpEx approach, as well as enabling you to scale up or down instantly as needed.

4. Solve the Security Skills Shortage

The evolving cybercrime landscape is stretching security experts to the limit. Threats are becoming more sophisticated and growing more targeted, and increasingly, tools are available to aid criminals in building, deploying, and monetizing templated attacks, such as malware-as-a-service and ransomware-as-a-service. Simultaneously, the fact that traditional security perimeters no longer provide viable protection exposes new vulnerabilities and attack surfaces that security experts must address. The answer, a tremendous influx of patched together security products, means a Byzantine stack of technologies for IT to deploy, manage, and integrate, further taxing an already stressed workforce.

These factors have driven up the demand for skilled network resources, contributing to a skills shortage. A survey released by the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) in November 2017 found that 70% of respondents believe that security skills shortages were impacting their organization. ISACA predicts that by 2019 there will be a shortage of two million cybersecurity professionals globally.

Since zero trust is implemented in the cloud, organizations that adopt this model no longer need to install a complex stack of equipment to secure each data center. They can simply use a single service in the cloud to secure all of their applications, data, users, and devices. By reducing complexity and streamlining operations, this approach allows you to do more with the security staff you have.

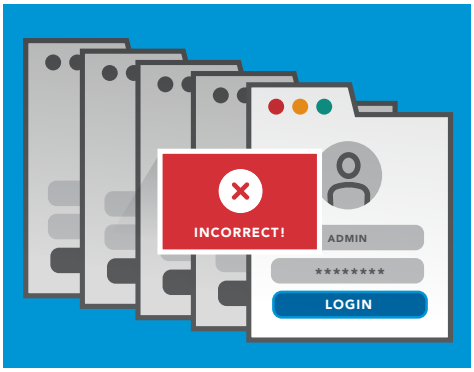
Better authentication and authorization processes for people and devices (seamless SSO and MFA) also minimize help desk requests around forgotten passwords and/or locked devices, as well as application access issues, further reducing personnel requirements. Improved network visibility that simplifies the identification of real threats means fewer false positive threat alerts that eat up the already strained time and resources of security teams.

So, in addition to reducing the number of security professionals required to monitor, manage, update, secure, and refine security controls, you can also retask resources, assigning business-critical efforts and proactive planning to more senior members of IT, ultimately reducing costs.

5. Deliver Both Security and an Excellent End-User Experience

In the past, organizations have had to make tradeoffs between strong security and a good, productive user experience.

Highly secure passwords are typically complicated and difficult to remember. They reduce productivity as users spend time reentering multiple, lengthy passwords — not to mention troubleshooting password problems with IT. When users attempt to remember complex passwords by writing them down, or use easy-to-remember passwords, they compromise security.



Zero trust solutions offer secure access, productivity, and ease of use. Simple, convenient MFA provides stronger security without the need to recall labyrinthine passwords. SSO further enhances the user experience and improves employee productivity by allowing users to log in to all of the applications which they require and have access to, without needing to reauthenticate each time or getting sidetracked by syncing issues.

Solutions that require authentication for both the device and the user further enhance security because they require authentication using something the user knows (e.g., login and password) and something the user owns (e.g., device and security key).

Cloud-based zero trust solutions also optimize application performance and deliver a seamless user experience across different device types and network conditions. These solutions adapt in real time to changes in content, user behavior, and connectivity through adaptive and cellular acceleration. Adaptive acceleration solutions leverage machine learning technology to automatically optimize performance based on real user behavior. Cellular acceleration solutions reduce latency by using fast, efficient, and modern web protocols, as well as by optimizing protocols and routing intelligently based on global Internet conditions.

6. Facilitate the Move to the Cloud

Organizations are increasingly seeking to modernize their applications and infrastructure by moving to software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) platforms. But when enterprises make this move, they cannot use familiar perimeter security solutions. Traditional appliance-based firewalls and gateways were never designed with the cloud in mind. As a result, organizations have been unable to adequately secure cloud applications — hindering their ability to migrate to the cloud.

The lack of cloud-based security and access controls has also meant that security teams have been very conservative (even paranoid) about giving partners, suppliers, customers, even employees access to new cloud services because it meant providing access to the entire network. Conversely, the inability to customize access can also mean providing too much access, with blanket permissions for all members of the ecosystem; giving the same level of access to the AC vendor as is provided to the lead developer poses serious security concerns.

Cloud-based zero trust solutions represent a new security paradigm specifically designed to secure applications in the cloud and in your data center. These solutions assume that there is no perimeter and that the environment is hostile. This cloud-based zero trust architecture provides a single point of control and authentication to give end users SSO capabilities across all of their on-premise and cloud applications. Everything looks the same to the end user. Organizations moving to the cloud now have efficient and effective security for their cloud-based solutions.

At the same time, because a zero trust environment follows least access principles, it allows IT to offer each user with access to specific applications and data. Security managers no longer fear offering access to customers, partners, and suppliers because it can be tailored and tightly controlled.

Conclusion

With zero trust cybersecurity solutions, organizations can not only obtain the security they need to protect their resources and data in today's distributed organization, they can also realize substantial business benefits. In addition to improving visibility across the enterprise and reducing time to breach detection, enterprises can also reduce the complexity of their security stack, minimize the impact of the security skills shortage, and protect customer data to avoid reputational damage and significant financial losses. Simultaneously, businesses can improve the user experience and facilitate migration to the cloud through the adoption of a zero trust security architecture.

To learn more about how a zero trust model can benefit your business, improve perimeterless enterprise operations, and bolster your organization's security posture, visit akamai.com/zerotrust.

AKAMAI'S VISION OF ZERO TRUST

Zero trust solutions meet the cybersecurity demands of the modern, perimeterless enterprise by assuming that every user, request, and server is untrusted until proven otherwise. This framework dynamically and continually assesses trust every time access to a resource is requested. Akamai's zero trust model incorporates the following key concepts:

CLOUD-BASED IMPLEMENTATION: The security stack that enforces the zero trust approach should be a cloud-based service and use the Internet as its core network. This architecture provides users with fast, easy, and safe access to applications from any device, anywhere in the world, and grants organizations the agility, scale, and cost advantages of an Internet service.

APPLICATION/USER LEVEL PROTECTION: The service should hide all applications from the Internet and public exposure. Instead, cloud-based access proxies should lie directly between the user and the application, acting as the only entry point for users to gain access to critical enterprise resources.

STRONG AUTHENTICATION: Because user names and passwords are easy to steal, a zero trust approach employs multi-factor authentication (MFA) to authenticate each user and authorizes both the device and the user for additional security.

LEAST PRIVILEGE: The zero trust solution should follow the principles of least privilege, giving users the minimum access necessary to do their jobs. It should explicitly permit each user with privileged access to each application by enforcing granular, role-based access control rather than by providing blanket privileges.

ALWAYS VERIFY: The solution must continually monitor and inspect all traffic (including DNS traffic originating from inside of the perimeter) for subversive activities. Behavioral analytics should identify suspicious traffic patterns in the audited activity.

LAYERED SECURITY DEFENSES: Because enterprise applications are also subject to application-layer attacks such as SQL injection, cloud-based access proxies should offer additional layers of application security controls.

SOURCES

1) https://img03.en25.com/Web/Symantec/%7Bf8ca1fb2-b73c-46d0-ae9e-17456c45df87%7D_ISTR23-FINAL.pdf?aid=elq_
2) http://www.issa.org/?page=2017_issaesg_surv
3) https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg