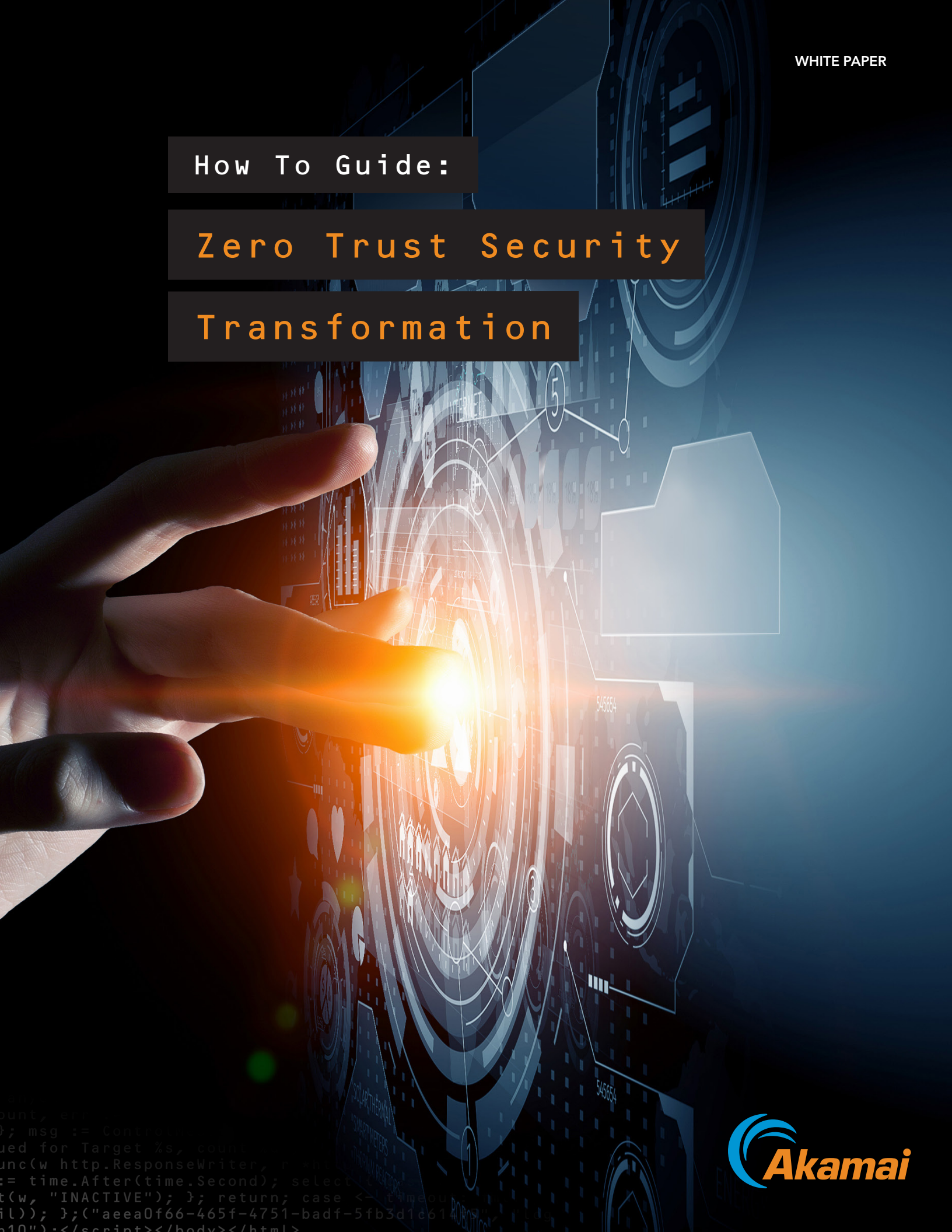
WHITE PAPER

How To Guide:

Zero Trust Security Transformation



Akamai

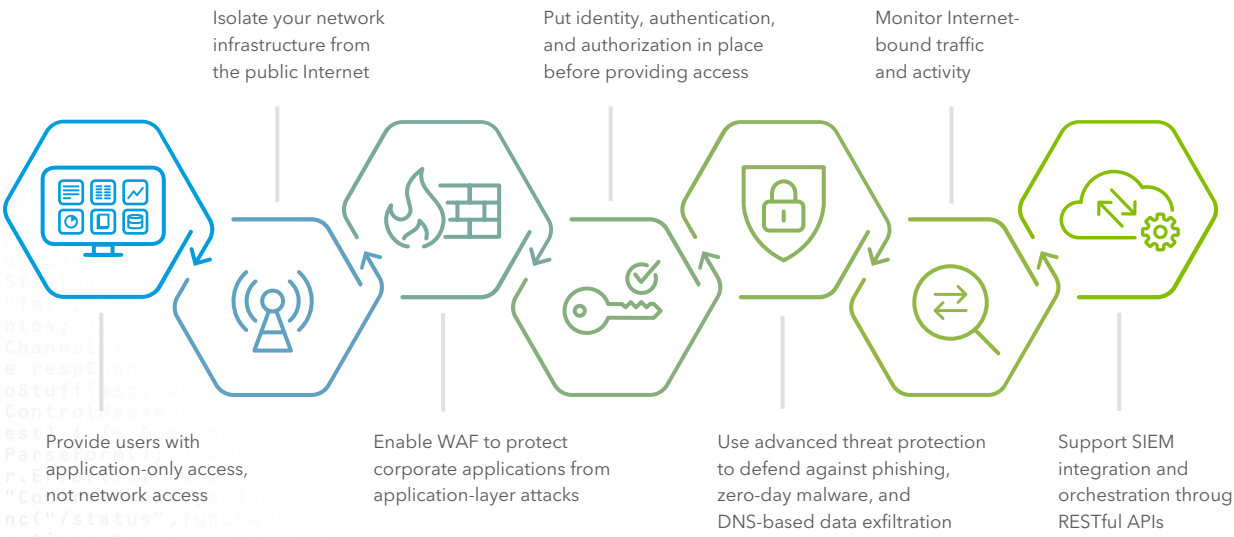
Executive Summary

The notion of a network perimeter — where everyone outside the enterprise's zone of control is malicious and everyone inside is honest and well-intentioned — can't be relied on in today's business landscape. Wide adoption of SaaS applications, migration to cloud-based architectures, a growing number of remote users, and an influx of BYOD devices have rendered perimeter-based security irrelevant. Furthermore, a perimeter-centric defense requires appliance and security policy management and frequent software upgrades, causing operational complexity and taxing already overwhelmed IT teams. As the attack surface expands, and strapped IT resources struggle to govern ever-more-convoluted network architecture, cybercriminals are increasingly proficient, sophisticated, and incentivized to evade security measures. A strategic security framework that addresses these distinct challenges is needed.

What Is Zero Trust Security and Why Is It Important?

A Zero Trust model replaces perimeter-centric security architecture. It ensures that security and access decisions are dynamically enforced based on identity, device, and user context. A Zero Trust security framework also dictates that only authenticated and authorized users and devices can access applications and data. At the same time, it protects those applications and users from advanced threats on the Internet.

To progress on your Zero Trust journey, safeguarding users, applications — and the future of your business — we suggest you:



Provide Users With Application-Only Access, Not Network Access

Legacy remote access technologies such as virtual private networks (VPNs) are not capable of meeting the growing demands of today's perimeter-less digital businesses. The traditional VPN poses a threat to enterprise security because it inherently puts a hole in the firewall, thus providing unfettered network access. Once an attacker is inside, he or she is free to move laterally to access and exploit any system or application within the network. Not only do traditional VPNs expose the business to security risks, but they are complex solutions that require significant IT resources for hardware and software management and are costly to maintain and scale.

Network segmentation, sometimes seen as a countermeasure to sweeping access, has proven to be expensive, difficult to implement, and cumbersome to manage. And it ultimately does not reduce risk; "permit any" access still allows for lateral movement within the network. While it compartmentalizes east-west traffic within a subnet, it can't stop horizontal spread within the same subnet.

To protect your business and enable Zero Trust, grant users access to only those applications they need for their role. Base this access on entitlement, user identity, device posture, authentication, and authorization. These best practices will reduce lateral attacks, limiting network exposure. Eliminating traditional VPNs will improve user experience, increase workforce productivity, and reduce helpdesk tickets. And moving away from a reliance on firewalls, hardware, and software means lower IT maintenance costs. Additionally, application-only permissions improve governance, providing visibility and insight into who is accessing applications, where data is going, and how it is being accessed.

Grant users access only to those applications they need — and base that access on entitlement, user identity, device posture, authentication, and authorization.

Isolate Your Network Infrastructure From the Public Internet

Exposing internal applications and access infrastructure to the Internet makes them vulnerable to DDoS, SQL injection, and other application-layer attacks. Cybercriminals are becoming craftier. They use ever-evolving techniques to scan enterprise network configurations to discover vulnerable applications and valuable data. As such, enterprises must isolate application and access architecture from the public Internet so it cannot be targeted by malicious actors using open listening ports. If cybercriminals can't find the network or determine which applications and services the target device is running, they can't attack it.

Enable WAF to Protect Corporate Applications

Modern cyberattacks are hypertargeted. Malicious actors leverage social engineering – emails, social media, instant messaging, SMS, and more – to prey on individuals using highly relevant and personalized bait. Cybercriminals seek out specific users with desirable seniority, skill sets, and access levels, then launch application attacks targeted at those users' permissions.

If a user's machine becomes compromised, it is often employed as a zombie device and, unbeknown to its owner, executes attacks on corporate applications that are allegedly safe behind the firewall. While most organizations use a web application firewall (WAF) to protect their external-facing applications from such attacks, many haven't extended this protection to corporate applications inside the network. WAF can protect internal applications and the data behind them from application-layer and injection attacks, like SQL injection, malicious file execution, cross-site request forgery (CSRF), and cross-site scripting.

Cybercriminals will target a device, turn it into a zombie machine, and use it to attack applications that are thought to be safe behind a firewall.

Put Identity, Authentication, and Authorization in Place Before Providing Access

Digital systems grant access to anyone who enters the correct password, without verifying the identity of the person. Weak credentials and password reuse significantly increase an enterprise's attack surface and risk. In today's threat landscape, relying on single-factor authentication, like username and password, is no longer enough. Multi-factor authentication (MFA) provides an extra level of verification and security; it ensures that only validated users gain access to business-critical applications.

Multi-factor authentication is a must. Weak credentials, along with the reuse of usernames and passwords across applications, significantly increase an enterprise's attack surface.

Once the user is authenticated and authorized through MFA, single sign-on (SSO) enables users to log in to all applications with one set of credentials. This improves productivity; there's no need to reconfirm identity for each application and no syncing issues across applications. Making continuous access decisions on a multitude of signals — including MFA and SSO across IaaS, on-premises, and SaaS applications — affords the business greater protection while also providing convenience for end users.

Use Advanced Threat Protection to Defend Against Phishing, Zero-Day Malware, and DNS-Based Data Exfiltration

Despite wide corporate adoption of layered security, malicious actors continue to gain access to enterprises by exploiting security weaknesses. Even with firewalls, secure web gateways, sandboxes, intrusion prevention systems, and endpoint anti-virus deployed, businesses are exposed and falling victim to phishing, zero-day malware, and DNS-based data exfiltration. So what are enterprises missing?

DNS is an often-overlooked vector. And cybercriminals have developed malware that is specifically tailored to exploit this security gap, evading existing security layers to infiltrate the network and exfiltrate data. Adding a layer of security that leverages the DNS protocol is critical; by utilizing this initial query stage as a security control point, a DNS security solution can detect and stop cyberattacks early in the kill chain, proactively protecting the enterprise.

Enterprises should leverage the DNS protocol as a security control point to help detect and stop cyberattacks early in the kill chain.

Monitor Internet-Bound Traffic and Activity

Enterprises must assume that the environment is hostile. This is the core tenet of Zero Trust. As such, organizations need to commit to auditing and confirming all activity, not blindly allow it. To do so, businesses require visibility into what is happening on their networks, with ample traffic and intelligence to make relevant comparisons.

Enterprises must monitor and verify all DNS requests from devices both on and off the corporate network – whether originating from laptops, mobile phones, desktops, tablets, guest Wi-Fi, or IoT devices – to ensure that queries are not headed for malicious or unacceptable sites. Organizations also require the ability to examine traffic behavior for signs of suspicious activities, such as communication with a command and control server or data exfiltration – and alert IT immediately of any issues. A view into global traffic volume and threat trends make it easier for IT to flag irregular or dangerous patterns.

Support Integration with Security Information and Event Management (SIEM) and Orchestration Through RESTful APIs

Enterprises may have hundreds, or even thousands, of applications. These require configuration via API to rapidly deploy applications in bulk while also setting policy controls for access. This is critical functionality for any large-scale application environment seeking to rapidly migrate from traditional VPN access to application-specific access. Adoption of APIs continues to increase as enterprises embrace DevSecOps and look for monitoring and configuration tasks available via RESTful API. They also need plugins to incorporate threat and event data into SIEM for further investigation and correlation. A scalable system also must integrate with workflow automation platforms and threat remediation by signaling into third-party endpoint detection and response solutions.

Conclusion

Digital transformation is a reality and enterprises must embrace a Zero Trust security model to successfully evolve the business, enabling innovation and agility, without compromising security. Advanced threat protection, application acceleration, MFA, and SSO across all applications – SaaS, on-premises, and IaaS – are some of the key benefits of operating in a Zero Trust environment. And a Zero Trust security model enables orchestration through API, as well as integration with SIEM and workflow automation platforms, providing visibility into users and applications while facilitating large-scale deployments in a fraction of the time.

Akamai can help guide your network and security evolution. Complete a seven-question Zero Trust Assessment to understand your business's level of readiness for a Zero Trust security framework. You'll receive customized next steps for network transformation. Or, for resources to kick-start your transition, visit akamai.com/3waystozerotrust.