ERICOM CYBERSECURITY INSIGHT SERIES

Zero Trust: Reshaping the Security Landscape

Never trust, always verify… especially when browsing the web

Zero Trust Security

Not placing your faith in anyone or anything is the new enterprise security paradigm. In the past, internal traffic was generally considered trustworthy while external traffic was usually untrusted. With the proliferation of insider threats and highly sophisticated malware, this notion is not only long outdated, but downright dangerous.

> *Organizations must not trust anyone or anything, inside or outside their network*

The Zero Trust concept transforms the way security strategy is conceived, planned and executed. No security barrier is considered safe enough on its own. No enterprise can be viewed as a fortress, protected by its own perimeter defenses. No traffic is automatically "okay". Point-blank, organizations must stop trusting anything or anyone, inside or outside their network.

Micro-segmentation and Authentication

In the years since the Zero Trust concept was formulated, an explosion of new micro-segmentation and authentication solutions has begun to bring it from theory to practice. The idea is to enforce security policies by enabling organizations to control what communication should -- or should not -- be allowed between various points on the network.

> *Rigorously control which communication should -- or should not -- be allowed between points on the network*

Activities are broken down to the smallest processes, each of which can be individually secured. Under the Zero Trust paradigm, machines, networks and IP addresses are all segmented and access to each component, and between components, is restricted according to rigorously applied security policies and authentication.

Micro-segmentation is quite demanding. Within a truly micro-segmented network, an IT team must manage large amounts of data processes across people, networks, devices and workloads. One small misconfiguration can set organizations back a day's worth of productivity. Moreover, nuanced access and authentication processes can create a poor user experience that further hinders productivity.

More significantly, while micro-segmentation and related solutions go a long way toward securing networks and data from everyone and everything, gaps still remain in truly locking down all traffic both within the network and from the outside.

The Web Cannot be Micro-segmented

One of the main areas of risk not covered by micro-segmentation or other Zero Trust solutions is web browsing. While essential in today's business environment, browsing remains a wide-open loophole through which malware penetrates organizations. Micro-segment to your heart's content, but it won't prevent browser-based ransomware variants, cross site scripting attacks and drive-by downloads from gaining a foothold in your network. Once malware bypasses that interface, it can easily make its way on to your endpoints and then onto your network.

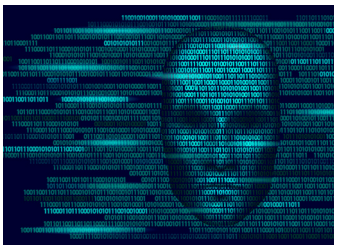
> *Browsing remains a wide-open loophole through which malware penetrates even Zero Trust organizations*

ERICOM CYBERSECURITY INSIGHT SERIES

Zero Trust advocates often cite whitelisting trusted sites and denying access to all others as the solution. But limiting access to all but known-to-be-needed sites kills productivity. This limited access creates hurdles for IT staff and end-users alike, as users are forced to request, and wait, for access and IT staff must use their scarce time handling access requests.

Moreover, even if organizations could whitelist every site their employees need, they would still be vulnerable to malware that infiltrates via legitimate sites. There is no way to know with certainty what's taking place behind the scenes on any given website, even one that has been whitelisted.

> *There is no way to know what's taking place behind the scenes on any website*



There is always the chance that the site may have been recently infected — so although it's technically "trusted", it may still deliver malware to visitors. Even proven methods like URL filtering, anti-phishing lists, web gateways and other types of filtering and screening solutions cannot instantly, hermetically block threats that originate from the web. Thus, the current Zero Trust model leaves room for browser-borne malware to infiltrate networks.

Remote Browser Isolation is Zero Trust for the Web

For complete security, the Zero Trust concept must be extended to browsing, too. Remote Browser Isolation takes as a given that nothing from the web can be trusted. Every website, each piece of content and all downloads are treated with the same extreme suspicion. While users can interact transparently with whatever sites they need, those sites are in fact airgapped away in a virtual browser, in a disposable isolated container, located remotely in the DMZ or cloud.

> *Remote browser isolation airgaps sites away from endpoints, while enabling users to browse naturally*

On their endpoint browsers, user receive a clean media stream that is free of executable code and browser-based threats. When a tab is closed, the container and all its contents are destroyed. Nothing untrusted can make its way onto endpoints and normal workflow continues uninterrupted. Remote browser isolation neutralizes the web as a threat to your organization.

While trusting "no one and nothing" is a smart way forward in today's evolving, highly complex threat landscape, there's little point in adopting it only part way. By applying Zero Trust Security to the most prevalent threat vector, Remote Browser Isolation, is the key to truly securing today's organizations.

> *Remote browser isolation neutralizes the web as a threat to your organization*

www.ericom.com

Americas:
T +1 (201)767-2210
E-mail: info@ericom.com

UK & Western Europe:
T +44 (0)1905 777970
E-mail: ukinfo@ericom.com

Worldwide:
T +972-2-591-1700
E-mail: info@ericom.com

Follow us