Ironcore Resources

ZERO TRUST AWARENESS: ENDPOINTS

ENDPOINTS AND ZERO TRUST

Endpoints are critical components of any Zero Trust security model. In the context of cybersecurity, an endpoint refers to any device that connects to a network, including laptops, desktops, servers, mobile phones, and IoT devices. One of the primary principles of Zero Trust is the concept of never trusting any user or device by default. In this model, every user and device must be authenticated and authorized before gaining access to any network resource.

WHY IT'S IMPORTANT

Endpoints are important in Zero Trust because they are often the weakest link in an organization's security infrastructure. Endpoints are vulnerable to a wide range of threats, including malware, phishing, and social engineering attacks. Bad actors use these methods to exploit endpoints as an entry point to an organization's network, applications, and data. By focusing on endpoint security, Zero Trust can reduce the attack surface and protect against data breaches.

60%

Almost 60% of organizations reported at least half of their users work at two or more days a week remotely.

70%

70% of organizations reported allowing access to corporate assets from personal devices.

75%

3 out of 4 organizations lack an endpoint solution that can automatically detect & stop an attack, quarantine infected endpoints, ***OR*** recover encrypted files.

ENDPOINT SECURITY

Endpoint security solutions facilitate the ability of organizations to authenticate and authorize devices, enforce access controls, protect against threats, and reduce the risk of data breaches. Security solutions like endpoint detection and response (EDR) allow organizations to detect unauthorized access and monitor the activity of endpoints. Organizations that implement robust endpoint security solutions as part of their Zero Trust strategy can significantly improve their security posture and protect against cyber threats.

In addition to authentication, endpoint security is also essential for enforcing access controls. The Zero Trust model emphasizes the principle of least privilege, which means that users and devices are granted only the access they need to perform their tasks. Application Whitelisting solutions in particular help facilitate an organization's ability to enforce access controls by ensuring endpoints are only able to run approved and vetted software or programs. This approach helps to minimize the attack surface by limiting access to only those resources that are required and approved for business operations.

www.ironcore-inc.com
zerotrust@ironcore-inc.com / 608-779-9400

CHOOSING AN EDR

Endpoints play a crucial role in the authentication process because they are the devices that are used to access the network. By utilizing endpoint security solutions such as endpoint detection and response (EDR), organizations can monitor the activity of endpoints and detect any unauthorized access attempts. However, not all EDR solutions are the same. When choosing an EDR solution here are some recommended features.

ANOMALY DETECTION

Next-Gen technologies such as machine learning, AI, and behavioral analysis can sift through mountains of endpoint-related data in real-time to quickly detect potential threats.

THREAT RESPONSE

Automated responses to potential attacks are crucial for blocking malicious activity on compromised endpoints quickly to minimize damages.

ISOLATION & CONTAINMENT

Tools that isolate and contain compromised endpoints prevent intruders from accessing your organization's network and protect sensitive data.

THREAT INTELLIGENCE

Accepting threat feeds from several providers, such as Financial Services Information Sharing and Analysis Center (FS-ISAC), helps understand threat behavior and identify attack vectors.

CONSIDERATIONS

ENDPOINTS AND REMOTE WORK

The importance of endpoints in Zero Trust is further emphasized by the increasing use of mobile devices and remote work. In today's distributed work environment, employees are using a variety of devices to access the network, including laptops, mobile phones, and tablets. This trend has made endpoint security even more critical because it is more challenging to control the security of devices that are outside the organization's network perimeter. By using endpoint security solutions, organizations can enforce security policies and controls on these devices and ensure that they are not used to compromise the organization's security.

MANAGING ENDPOINTS OVER TIME

Managing endpoints is not a one-time process, but rather an ongoing effort that requires regular review and updates. Keeping an accurate record of active endpoints, adjusting access privileges as needed, and ensuring endpoints are compliant with security patches and policies all require continued management and review. Utilizing tools that examine an endpoint's security posture before determining whether or not to grant access to the network limits an organization's risk to exploited vulnerabilities. Organizations that implement a Zero Trust security model with strong access controls can significantly improve their security posture and protect against data breaches.

SUBSCRIBE TO OUR BLOG

Scan the QR Code or visit www.ironcore-inc.com/blog to follow more educational series like this.

IRONCORE
STRONG · TRUSTED · SECURE

www.ironcore-inc.com
zerotrust@ironcore-inc.com / 608-779-9400