In order to implement information security in the workplace, organizations must first take steps to protect its data. For the vast majority of businesses, information is their most valuable asset. Whether we’re talking about storing customers’ credit histories or social security numbers, product drawings, patent applications, or one-of-a-kind designs, financial records, or a customer list with secret information, all of the above are examples of data that must be protected. An attack on your data could lead to incidents of identity theft, private information leaks, and significant financial damages.

As a result, to reduce the danger of data loss or leakage, every organization should adopt information security in the workplace.
How to protect Workplace

1. Multiple Layers of Security to Protect Workplace

Traditional security methods fail if an attacker can get around the weakest link, such as through spreading malware or exploiting application flaws. Layering network and endpoint security together is more successful because if an attacker gets around one measure, they’ll meet with another, making it increasingly harder for them to succeed.

The goal of network security is to prevent as many attacks as possible from reaching an endpoint via the network, whether they are malware, phishing attempts, or exploits. The goal of Workplace security is to neutralize an attacker’s capacity to do damage if an attack hits the endpoint via a USB drive or other non-network means, the communication is encrypted, or the user is online or off-network.

Integrating endpoint and network security is even more effective when these disciplines are combined for a Zero Trust architecture.

2. Network Security and Integration

Endpoint security and network security are woven together in a single, comprehensive security architecture with Zero Trust to the Endpoint.

The endpoint's intelligence can be provided into the firewall, and vice versa.

On the firewall, policies can be set up so that whenever an endpoint suffers an event, it can be quarantined until it can be fully scanned and cleansed.

Incorporating user and traffic data from firewalls into network security management solution also provides context for what’s going on across the network.

This allows you to design security policy to reflect such activities appropriately and to be applied on the endpoint.

The Pandemic exposes VPN flaws

Many organizations’ VPNs struggled to cope with the massive increase in usage as remote work increased during the pandemic. Aside from being tailored to an on-premises environment, VPNs may not always guard against sophisticated threats.

Despite the fact that it is still a popular strategy, we believe it will fail when attackers get access to the internal network after compromising individual users. Threat actors have recently gained access to systems using the credentials of employees in a number of cases. “To solve such problems, a zero-trust model can be used, in which authorization can be passed each time a user tries to access a specific resource.”

Remote work increases demand for zero-trust security

While many businesses have been migrating toward a zero-trust security approach, the COVID-19 epidemic has hastened this process tenfold.

Infosec experts say businesses are migrating from VPNs to zero-trust networks (ZTN) 2 years after lockdowns. Because it makes no assumption that the person signing in with a username and password is who they claim to be, a zero-trust model is useful for safeguarding remote employees’ devices. Instead, a ZTN checks each access request using additional data signals such as geolocation and user behavior, making access easier to govern and manage, especially when several users are operating from various places.

Perhaps as an example, in a company which has 5,000 employees spread throughout a half-dozen locations, we must now accept that we have 5,000 offices, and making that change from a management and security standpoint is a major undertaking. It’s like throwing 40 years of IT out the window and starting over from the beginning and that’s where we are.

As other example a multinational insurance company with around 500 remote workers on any given day went from 5000 to 50,000 in a matter of hours. And of the 50,000, over 20,000 did not have PCs, so 20,000 bring-your-own devices, for which we have no choice but to shift to a zero-trust paradigm quickly.
3. Managing a variety of End Points

Endpoints such as servers, workstations, desktops, laptops, tablets, and mobile devices must all be controlled in every organization. Endpoint protection need be integrated with a firewall in order for security policy to follow endpoints wherever they go in order to strengthen security posture and adopt Zero Trust. For scalability and to relocate the line of exposure away from important applications, multi-factor authentication, or MFA, can be enforced on a next-generation firewall. This integration must not degrade system performance, as users may be unaware that security is running in the background and attempt to disable or close security programs.

Making the Transition to Zero Trust

While security experts believe that a Zero Trust Network (ZTN) is safer for today’s changing workplace, it is not appropriate for every company. Many major cloud providers have identity and access management (IAM) offerings that allow customers to deploy continuous authentication systems for privileged users. As an example, some, such as medium-sized enterprises, are already 100 percent in the cloud and have been prior to the pandemic; However, the larger and older the company is, the more likely it need to have items that will not die on the network. If its a midmarket company, it might get rid of your VPN right now. Ultimately, it comes down to the use case.

Coforge S.A.F.E – Workplace Security Services

Coforge SAFE offering for workplace security helps in delivering optimized security with right enablement. The SAFE platform entails protecting end-user devices from unauthorized access, protecting the endpoints from malicious attacks, providing faster response to security incidents, and creating an environment of trust. SAFE framework and platform is built on the “prevention first” approach with multilayered security, faster recovery, and unified compliance and management to deliver a zero-trust architecture to our customers.

Features of S.A.F.E platform include:
- Proactive threat management
- Zero-day attack protection
- Advanced security features
- Reduction of human errors
- Minimization of attacks & data loss
- Regulatory compliance

S.A.F.E Benefits
- Secure Endpoints: Includes patching, hardening, advanced malware/virus protection, Anti APT, firewall and protection from social engineering attacks such as phishing
- Secure Access: Least Privilege based identity and access management
- Protected Data: Encryption, safer browsing, DLP & Email protection
- Advanced Endpoint Handling: Help in zero-day threat, zero trust
- Increase Usability: Policy & control support, vulnerability management, security configurations
- Detection & Response: MDR integration & regular support

For more details please check our Website

---

Zero Trust Architecture

Delivering Optimized Security With Right Enablement

- **Secured Endpoint**
  - Patching/Hardening
  - EPP/EDR/XDR
  - Firewall
  - Mobile Device Mgt
- **Secured Access**
  - Adaptive Access
  - MFA/SSO
  - Proxy
- **Secured Data**
  - Encryption
  - Data Loss Prevention
  - Mail Security
  - Compliance

Enablement

Security

- High
- Low
Coforge is a global digital services and solutions provider, that leverages emerging technologies and deep domain expertise to deliver real-world business impact for its clients. A focus on very select industries, a detailed understanding of the underlying processes of those industries and partnerships with leading platforms provides us a distinct perspective. Coforge leads with its product engineering approach and leverages Cloud, Data, Integration and Automation technologies to transform client businesses into intelligent, high growth enterprises. Coforge’s proprietary platforms power critical business processes across its core verticals. The firm has a presence in 21 countries with 25 delivery centers across nine countries.

Learn more about Coforge at: www.coforge.com