opticca security

Cybersecurity Solutions: Building better cyber resilience

As technology advances, so do the capabilities of cybercriminals, making it essential to adopt proactive measures to safeguard against potential threats.

Cyber resilience is your ability to anticipate, withstand, recover from, and adapt to adverse conditions of cyber attacks. Going beyond traditional cybersecurity measures that primarily focus on prevention and defence, **cyber resilience** emphasizes your ability to quickly detect and respond to cyber incidents, minimizing their impact and ensuring continuity of operations.

Reduce risks, preserve trust, contain disruption, and make your business **cyber resilient** to today's and tomorrow's cyber threats with our portfolio of end-to-end security solutions, delivering a resilient security foundation with 360-degree visibility across your business. Focus on what matters most, driving your business forward.

Web Application Firewall (WAF)

A WAF helps protect your web applications by inspecting and filtering traffic between each web application and the internet. It works best as part of a suite of tools that support a comprehensive application security program. A WAF can be instrumental in preventing fraud and data theft for companies operating web-based products or services involving customer interactions. WAFs can help defend web applications against attacks like cross-site request forgery (CSRF), cross-site scripting (XSS), file inclusion, and SQL injection.

Next-Generation Web Application Firewall (NGFW)

An NGFW combines the best features of a traditional network firewall and a web application firewall with VPN support and packet filtering basics, plus deep packet inspection, antivirus inspection, website filtering and other features that focus on your network security. It typically acts as a firewall blocking incoming requests by inspecting the network layer packets, but it integrates additional inspection capabilities to handle more advanced scenarios and block more sophisticated threats that stem from coordinated attack vectors.

Zero Trust Security (ZTS)

ZTS implies that no one is trusted by default from inside or outside your network, and verification is required from everyone trying to access your network's resources. User identities and privileges, as well as device identities and security, are continuously monitored and validated. ZTS reduces the impact of user credential theft and phishing attacks by requiring multiple authentication factors and eliminates threats that bypass traditional perimeter-oriented protections.

Cloud Security & Compliance (CSPM)

Cloud security and compliance comprises safeguarding sensitive data, adhering to regulations, maintaining customer trust, and ensuring business continuity. You can minimize the risk of dangerous breaches by implementing strong security measures like encryption and access controls, automated compliance monitoring, security assessments, and meeting compliance regulations.

Distributed Denial-of-Service Security (DDoS)

DDoS security leverages preventive and detective controls in tandem, reducing potential security threats before they happen and identifying those that get through soon after they emerge so you can remediate them before too much damage occurs.

Secure Access Service Edge Security (SASE)

SASE combines networking and security functions into a single cloud-based service. It integrates various security services, including firewall-as-a-service, secure web gateways, and zero-trust network access to address potential vulnerabilities. SASE ensures consistent security across all your users and applications, regardless of their location, mitigating security risks and safeguarding your critical data.

Container Security (CS)

Container hardening is the process of using container scanning tools to detect and address possible vulnerabilities to minimize the risk of attack. Robust container security reduces the risk of deploying a container that carries a security flaw or malicious code into your production environment.

Content Delivery Network Security (CDN)

CDNs analyze and absorb unusual traffic spikes and take the load off your origin server. When a website visitor wants to access a particular web page, it's optimally mapped and sent to the nearest CDN server. This server will then respond to the request by delivering a cached or copied version of your web page to the visitor's device.

Cybersecurity Asset Management (CSAM)

CSAM is identifying, on a continuous, real-time basis, all devices, resources and services within your IT estate and the potential security risks or gaps that affect each one. Robust cybersecurity asset management delivers the visibility needed to build a comprehensive security strategy that mitigates threats quickly and proactively.

Ensure cybersecurity excellence

Build a more efficient and robust cyber security ecosystem with Opticca Security, your consultative partner. With established relationships with leading cyber security vendors like Cloudflare, ShiftLeft, Snyk, and Sonatype, we can deliver solutions that pair best-in-class technology with your strategic objectives.

As you navigate the security challenges of finding and stopping threats, we're here to help – now and as your needs evolve.

Let's begin with a conversation.