ASPIRE
Powering Business Transformation™

Cisco Partner
Master Security Specialized
Master Networking Specialized
Master Collaboration Specialized
Gold Integrator

Key Foundations for a Strong Enterprise Cybersecurity

A how-to guide for IT staff and senior management in organizations to secure business data against today's evolving threat landscape.

Table of Contents

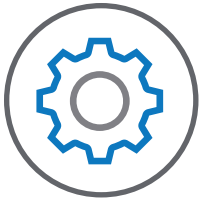
Modern, Efficient Cybersecurity

The objective of this e-book is to provide easy-to-understand and actionable guidance that will deliver dramatic improvements to your overall security posture without introducing a ton of complexity.

The foundational elements of security introduced here are applicable to organizations of any size, particularly for mid-sized businesses.

Advanced Cloud-based solutions

Minimal effort needed to implement



Easy to consume and manage

Understanding the Challenges

Today's businesses are evolving quickly. Digital transformation is key for organizations that wish to bring more value to their customers by reshaping their business models. Leveraging technology to drive agility, innovation, and optimization is at the heart of every IT strategy.

Addressing cybersecurity, privacy, and compliance remains one of the biggest challenges for executives.

- Finding, recruiting, and retaining security expertise is challenging and expensive.
- The pandemic accelerated work from home (WFH) and cloud adoption. Security is still catching up.
- Cyber Insurance coverage providers require more comprehensive security controls to be in place

Organizations need expert guidance to develop a security strategy that effectively manages risk while addressing specific business challenges. Work with professional experts to choose the right solutions, prioritize investments, and dramatically improve your security posture right away.

Effective Protection

Defend the edge

A Cloud-driven Secure Internet Gateway combines multiple security functions to protects users from Internet-based threats wherever they go.

Secure Internet Gateways unify secure web gateway, DNS-layer security, firewall, and cloud access security broker (CASB) -- in a cloud-delivered security service.

Prevents malware, ransomware, or phishing attempts from malicious or fraudulent websites

Protects roaming users and devices, no matter where they are, without the need to be connected to an office network or VPN

Enforces corporate acceptable use policy with over 60 pre-built content categories, as well as custom-defined allow and block lists

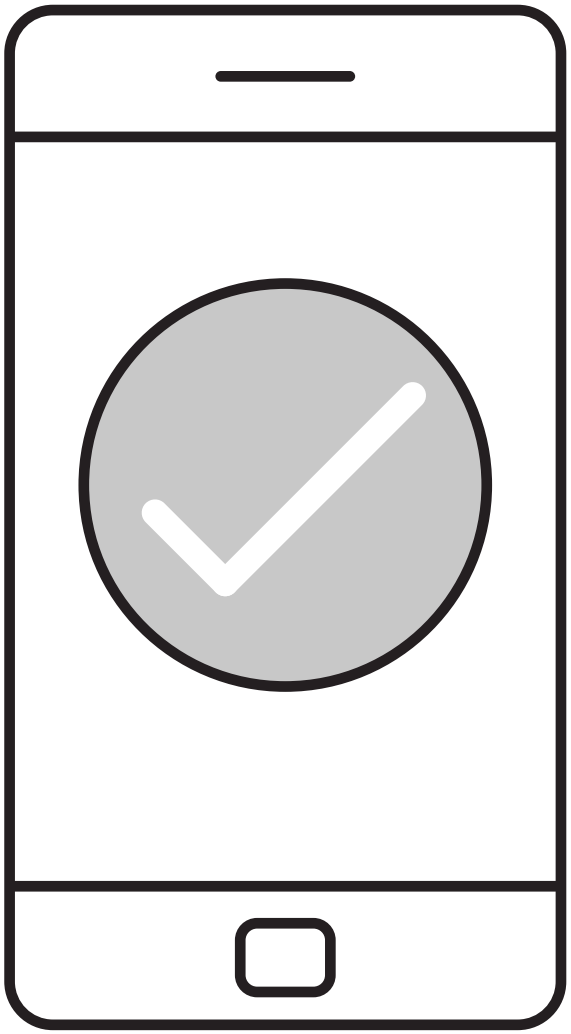
Effective Protection

Safeguard users, devices, and applications

Multi-factor authentication (MFA) and device trust are great places to start for enterprises looking to secure the workforce. Verify user identity and device security before users can access business applications.

MFA is easy to deploy and provides a seamless method to enable work from anywhere, on any device, by implementing controls to ensure secure access to applications.

MFA access security shields any application from compromised credentials and devices, and its comprehensive coverage helps you meet compliance and cyber insurance requirements with ease.



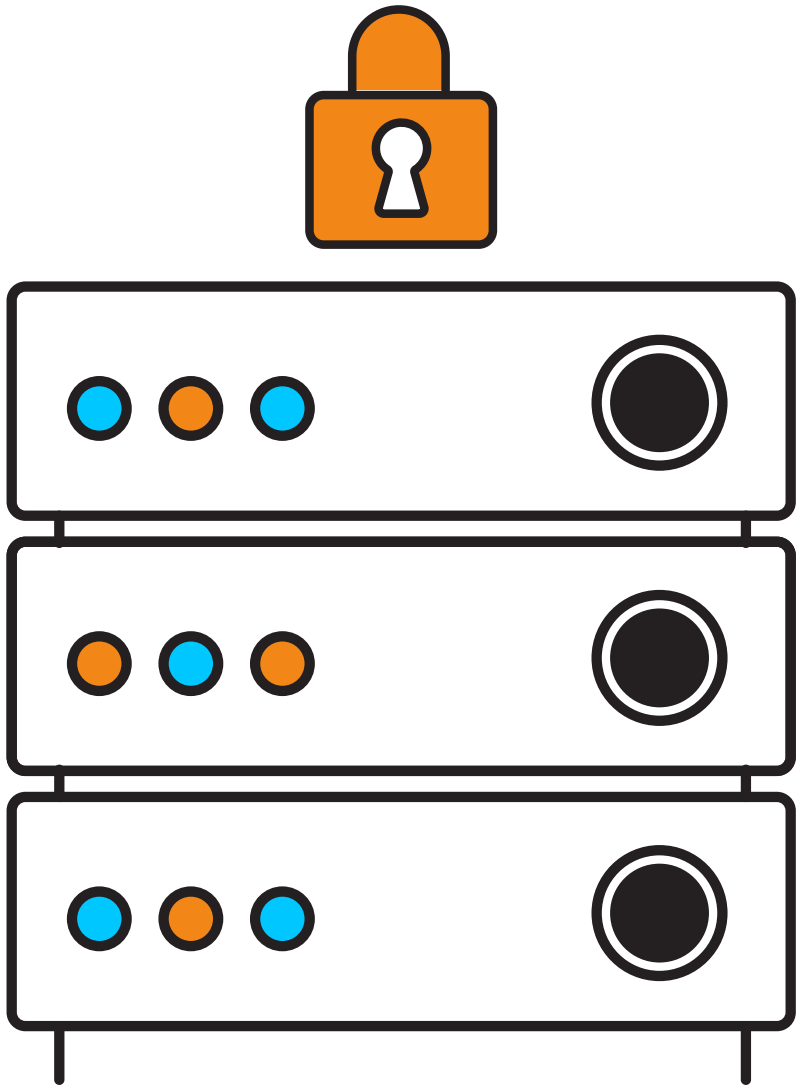
Effective Protection

Securing your endpoints

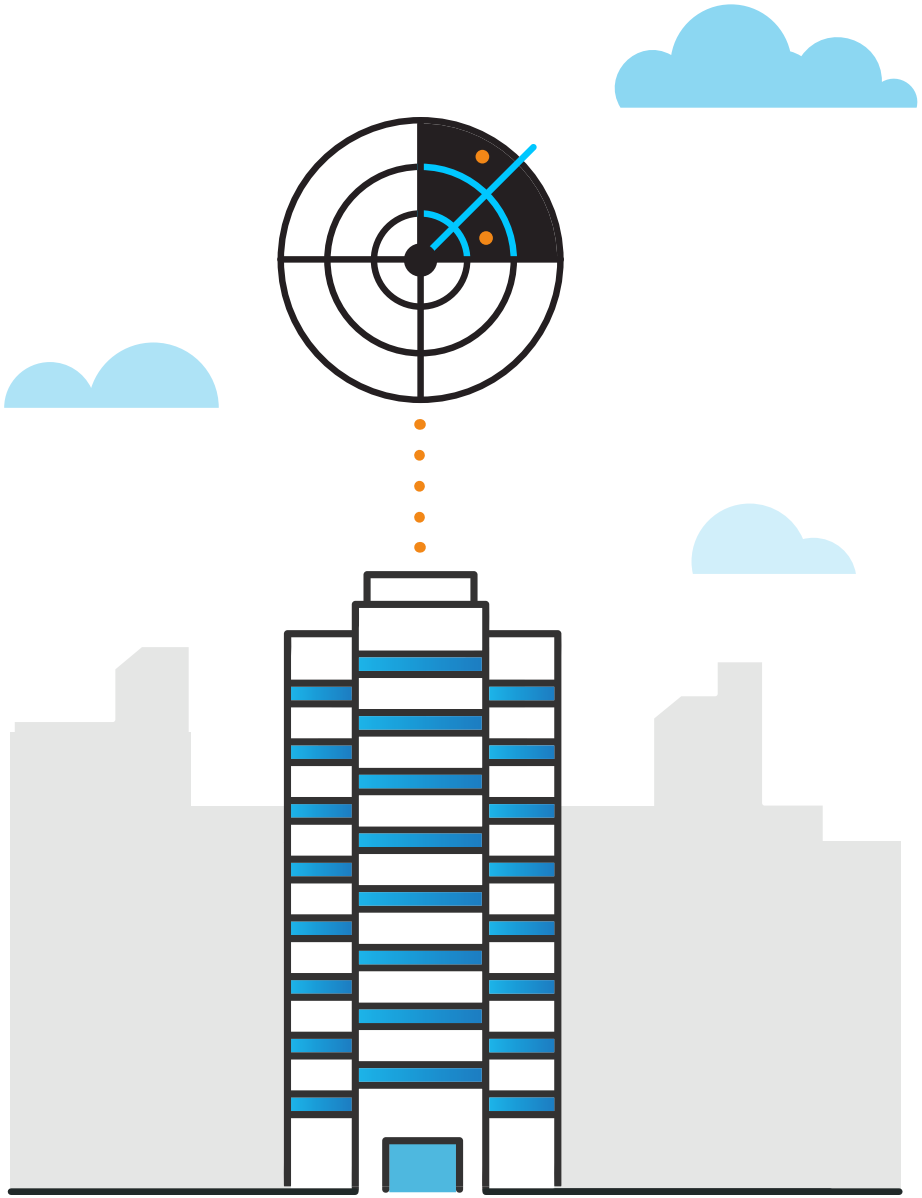
In the rapidly evolving world of malware, threats are becoming harder and harder to detect. Legacy antivirus subscriptions are no longer enough to protect your valuable data.

Endpoint Detection and Response (EDR) solutions have cloud-delivered endpoint protection and advanced detection and response across multidomain control points. The single-agent solution stops threats and blocks malware, then rapidly detects, contains, and remediates advanced threats that evade front-line defenses.

EDR is a vital element of any security strategy to defend against threats to laptops, workstations, and servers.



Effective Protection



Unified threat detection across on-prem and cloud environments

Companies of all sizes face the challenge of securing their public cloud environments and on-premises infrastructure.

Network traffic analysis (NTA) extends your visibility to detect threats across your cloud and on-premises environments. NTA uses a behavior-modeling approach that detects a threat based on how it acts on the network.

Because it is a SaaS-based network and cloud security solution, there is no specialized hardware to purchase or software agents to deploy. The platform analyzes a wide variety of network telemetry to identify abnormal behavior or signs of malicious activity. You can quickly respond before a security incident becomes a devastating breach.

Effective Protection

The SecOps team you wish you had

Most midsize enterprises lack 24x7 in-house security operations to administer threat monitoring & detection effectively. Implementing appropriate layers of security tools is critical but only part of the equation. To realize the full value of your security investment, you must have a consistent way to identify and respond to threats to ensure small cybersecurity problems don't become big ones.

Managed Detection & Response (MDR) services provide 24x7 threat monitoring, detection, and response capabilities across cloud, network, and endpoints.

Subscribing to an MDR service like Aspire, for example, gives the organization access to an expert team of security analysts and incident responders. They act as an extension of your IT organization to detect, analyze, investigate, and remediate threats quickly.

You deserve 'an exceptional security operations team that won't break the bank.

Effective Protection

Better security awareness

Regardless of an organization's size, users are most commonly the weak link in network security. Your employees are increasingly exposed to sophisticated phishing and ransomware attacks. Having a security awareness program in place is more critical than ever.

Awareness training combined with well-thought-out simulated phishing attacks effectively helps to promote defensive security practices.

Robust training programs and platforms provide built-in training, testing, and assessment modules to better manage the urgent IT security problems of social engineering, spear-phishing, and ransomware attacks. They also enable your organization to stay compliant with industry regulations like PCI, HIPAA, SOX, FFIEC, and GLBA.

Mobilize your end users as a last line of defense!

Security Self-assessment

Take this brief self-assessment to identify gaps in your security strategy.

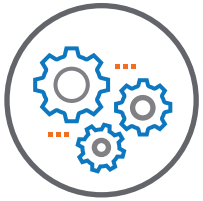
Which of the following foundational elements of network security has your organization implemented?

Cloud Edge

Multi-Factor Authentication

Endpoint Detection and Response (EDR)

Network Traffic Analytics



Managed Detection & Response (MDR)

Security Awareness Training

Let Aspire Technology Partners help secure your business. Our team of security solution architects can assist you in choosing the right tools to fit your specific needs.

Learn More

To learn more about how Aspire MDR can enable your organization towards a stronger security posture, visit our website. Contact one of our experts at CyberSecurity@aspiretransforms.com.

ASPIRE
Powering Business Transformation™

AspireTransforms.com | 732-847-9600