MODERN INFRASTRUCTURE AND MULTICLOUD

Defense Strategies to Prevent Cyber Attacks

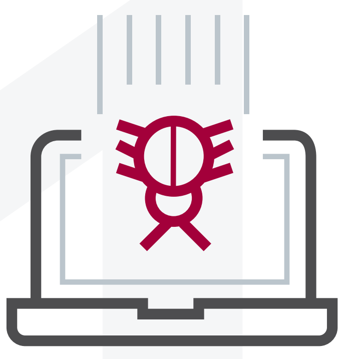
Prevent attacks from wreaking havoc on your network and build better cyber resilience through strategic defense layers.

THE ATTACK PATH

4 Critical Stages

STAGE 1

Initial Access Attempt



The Threat

- Phishing email
- Compromised credentials
- Vulnerable endpoint

The Reality

82.6% of phishing emails now use AI. Phishing hyperlinks increased 36.8%, malware attacks rose 20%, and social engineering tactics jumped 14.2%.[1]

Your Defense

Cisco XDR: Email security, endpoint detection, and behavioral analytics

Best Practices: Employee training and multi-factor authentication (MFA) implementation

STAGE 2

Shift to Lateral Movement

The Threat

- Network reconnaissance
- Privilege escalation
- Internal spreading

The Reality

Attacks from compromised accounts bypassing traditional detection increased 57.9%.[1] Attackers can achieve lateral movement in as little as 27 minutes (48 minutes on average), and 90% of organizations detected lateral movement incidents in the past year.[2, 3]

Your Defense

Cisco XDR: Network traffic analysis and anomaly detection

Best Practices: Network segmentation and zero-trust architecture

STAGE 3

Permanent Foothold and Command Control

The Threat

- Backdoor installation
- External communication establishment

The Reality

Ransomware incidents were shown to result in cybercriminals embedding backdoors and other persistence mechanisms for 21% of 2,000 senior security decision-makers in IT and business roles.[4]

Your Defense

Cisco Managed Firewall: Intrusion detection and prevention, security policy enforcement, and traffic inspection

Best Practices: Regular security audits and access reviews

STAGE 4

Data Exfiltration Attempt

The Threat

- Data collection
- Encryption
- Transfer preparation

The Reality

Data exfiltration extortion now costs an average of $4.44 million per incident, with attackers often wiping backups in 19% of ransomware cases.[5, 6]

Your Defense

Cisco XDR and Managed Firewall: Data loss prevention, encrypted traffic analysis, and security policy enforcement

Best Practices: Data classification and backup strategies

Why Advanced Managed Security Services?

Enterprises of all sizes can secure their hybrid environments with advanced protection powered by Connection's Managed XDR Services—providing human-led monitoring and continuous improvement built on Cisco's best-in-class platform.

Expert-driven Protection
Continuous threat intelligence updates combined with AI-powered detection and response

Adaptive Defense
Real-time threat landscape evolution with automated response capabilities

Comprehensive Coverage
Seamless protection from on-premises to edge to cloud with integrated security operations

Why Connection?

Modern enterprises need modern defenses.

Get a comprehensive security assessment and discover how Connection managed services apply Cisco XDR and Managed Firewall technologies to fortify your defense layers.

Elevate Your Cybersecurity Posture Now

Cybersecurity
Modern Infrastructure
Extended Detection and Response (XDR)

Contact an Expert

1.800.998.0067

Sources:

[1] KnowBe4 Phishing Threat Trends Report, 2025
[2] ReliaQuest Annual Cyber-Threat Report, 2025
[3] Illumio 2025 Global Cloud Detection and Response Report, 2025
[4] Barracuda Ransomware Insights Report, 2025
[5] IBM Cost of a Data Breach Report, 2025
[6] Barracuda Ransomware Insights Report, 2025

Connection®
we solve IT®