Security Business Outcomes

How to Protect Business to Support Digital Transformation

Greg Griessel
Consulting Systems Engineer - Cybersecurity
greggr@cisco.com
Security Enables Digitization
Digital Disruption, Massive Scale

50B Devices Connected by 2020

$19T Opportunity

Active Adversaries

Attack surface
Threat Actors
Attack Sophistication

Security Industry

Rapidly expanding number of security companies
Not interoperable
Not open

Security Challenges

Changing Business Models

Dynamic Threat Landscape

Complexity and Fragmentation
Goal for Effective Security
The Security Effectiveness Gap
If It’s Digital

Security Must Evolve
Architectural Approach: Integrated

- Mobile Users
- Branch Offices
- Corporate Networks
- Roaming Laptops
- Endpoint Cloud
- Network
- Complexity
- Capability
Premiere Portfolio in the Industry

*Best of Breed and Integrated Architecture*

- UTM
- Network Analytics
- Cloud Access Security
- Secure Internet Gateway
- Policy and Access
- Web
- Email
- Advanced Malware
- NGFW/NGIPS
Security Enables Digitization

Protect your Business During Digital Transformation

- Stop threats at the edge
- Control who gets onto your network
- Find and contain problems fast
- Protect users wherever they work
- Simplify network segmentation
Security Enables Digitization
Protect your Business During Digital Transformation

NGFW + Risk Assessment
If your network is down, you are not “up”. And it’s no longer someone else’s problem; network devices now come with security offerings that support your business goals securely.

The fight against threats is not lost, but it’s harder than ever. Apply threat-centric visibility and control to your NGFW for truly effective protection at the perimeter.
Security Enables Digitization
Protect your Business During Digital Transformation

Umbrella + Architecture Review

Apply consistent controls and polices for securing your mobile users as they move among many locations. Extend your NGFW protection beyond the perimeter with cloud-delivered security enabled at the DNS layer to protect users from malware, phishing and other malicious connections. Protect all users regardless of location or device, whether they are in the office, in a branch or mobile on their device, and whether they are employees or guest WiFi users.
It’s 1am and an employee accesses your corporate network remotely via their laptop. Minutes later, that same employee appears via public wifi and VPN on their tablet device, only suddenly they’re on the other side of the planet. And the employee appears to be your CFO trying to access board-level files. Is this something you want to allow? Does your current NAC solution enable you to stop the wrong people from accessing your network?
Stealthwatch + TrustSec + Segmentation Services

Security begins with the network. Build a network to support your entire business that you can segment simply to ensure the correct controls are in place. Protect one part of your network from problems that occur in another, using Software Defined Segmentation rather than deploying new hardware.

Then add visibility into the network to create the right policies; turn your network into a sensor and enforcer with a combination of solutions that control access, enforce policy and examine behavior to detect anomalies and update policies or change access rights.
AMP + Active Threat Analytics

Threats will find a way past the best defenses, and then the race is on. Reduce the time it takes to find bad stuff on your network from days to hours. Traditional endpoint methods of signature detection are slow, and threats move fast. Find, stop and remove malicious content before it does any more damage with effective tools that are simple to use.
Security Enables Digitization

**OUTCOMES**
- **Stop threats at the edge**: NGFW
- **Protect users wherever they work**: Umbrella
- **Control who gets onto your network**: ISE
- **Simplify network segmentation**: Stealthwatch + TrustSec
- **Find and contain problems fast**: AMP

**PRODUCTS**
- NGFW
- Umbrella
- ISE
- Stealthwatch + TrustSec
- AMP

**SERVICES**
- Risk Assessment
- Architecture Review
- Architecture Review
- Segmentation Services
- Active Threat Analytics

**SUMMARY**
- Apply threat-centric visibility and control to your NGFW for truly effective protection at the perimeter.
- Protect all users regardless of location or device, and whether they are employees or guests.
- Stop the wrong people from accessing your network.
- Gain visibility into behavior from within the network. Stop threats from spreading within your organization.
- Find, stop and remove malicious content with effective tools that are simple to use.
Effective Security

Simple

Open

Automated