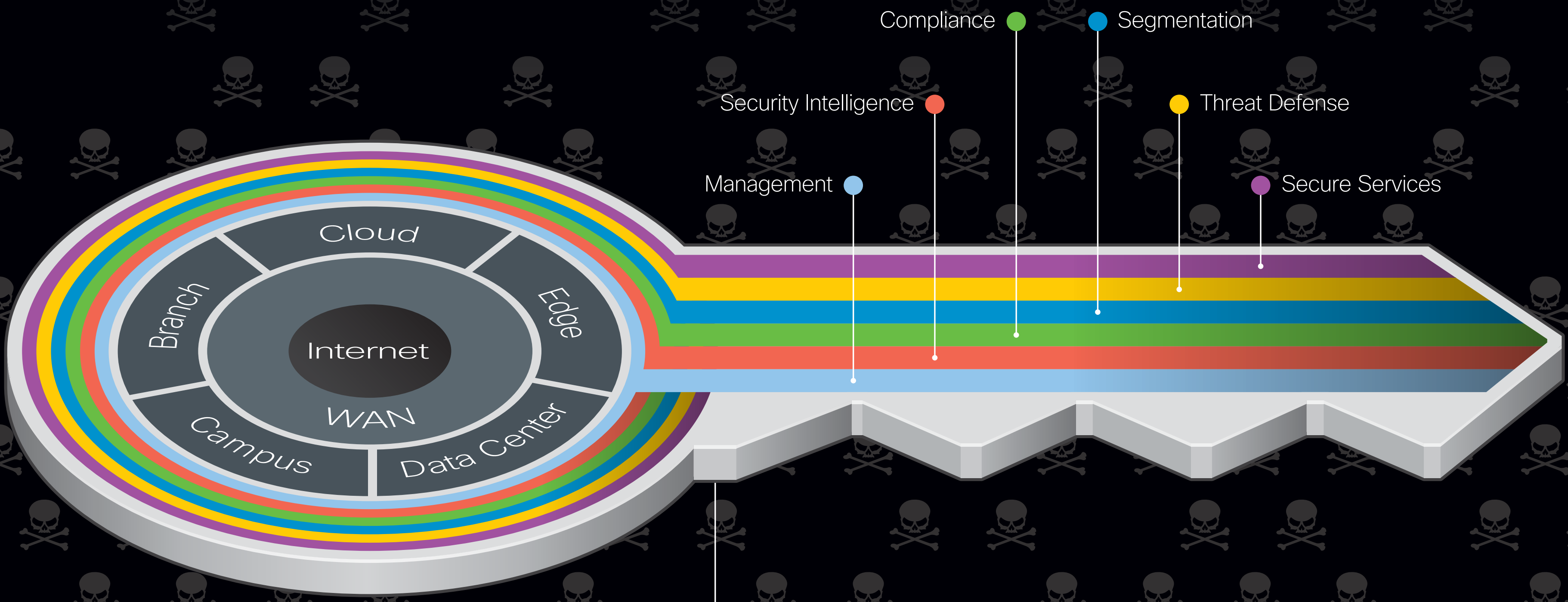
SAFE

SIMPLIFIES SECURITY

August 2015

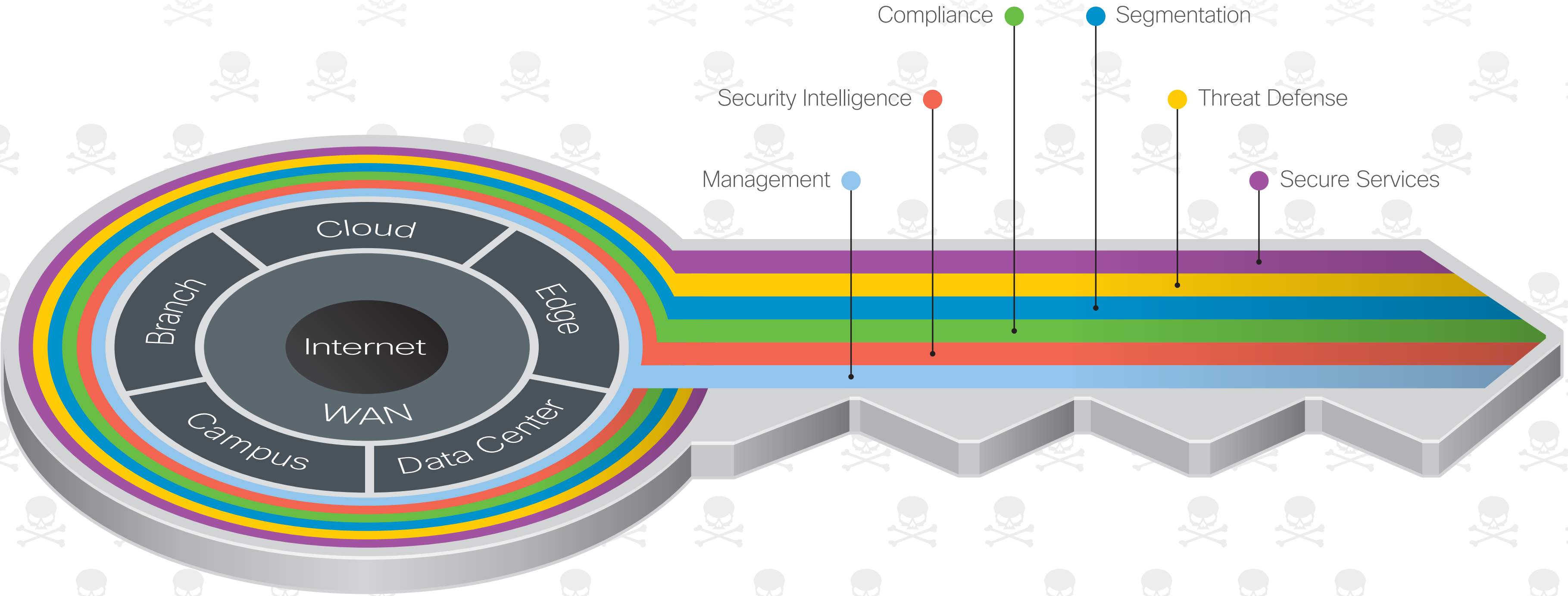


The Key to SAFE organizes the complexity of holistic security into Places in the Network (PINs) and Secure Domains. PINs are reference examples of locations found in networks, and Secure Domains are the taxonomical areas used to protect them.

Introduction

SAFE is a secure architectural framework example for business networks. SAFE simplifies complexity using a model that focuses on the areas that a company must secure. Each area is treated with holistic discussion of today's threats and the capabilities needed to secure them. Critical challenges have been deployed, tested, and validated at Cisco. These solutions provide guidance, complete with configuration steps, to ensure effective and secure deployments for our customers.

For more information, visit cisco.com/go/safe



Secure Domains

Secure Services

Provides technologies such as access control, virtual private networks, and encryption. It includes protection for insecure services e.g., applications, collaboration, and wireless.

Threat Defense

Provides visibility into the most evasive and dangerous cyber threats. It uses network traffic telemetry, reputation, and contextual information for that visibility. Enables assessment of the nature and the potential risk of the suspicious activity so that the correct next steps for cyber threats can be taken.

Segmentation

Establishes boundaries for both data and users. Traditional manual segmentation uses a combination of network addressing, VLANs, and firewalling for policy enforcement. Advanced segmentation leverages identity-aware infrastructure to enforce policies in an automated and scalable manner, greatly reducing operational challenges.

Compliance

Addresses policies, both internal and external. It shows how multiple controls can be satisfied by a single solution. Examples of external compliance include PCI, HIPAA, and Sarbanes-Oxley (SOX).

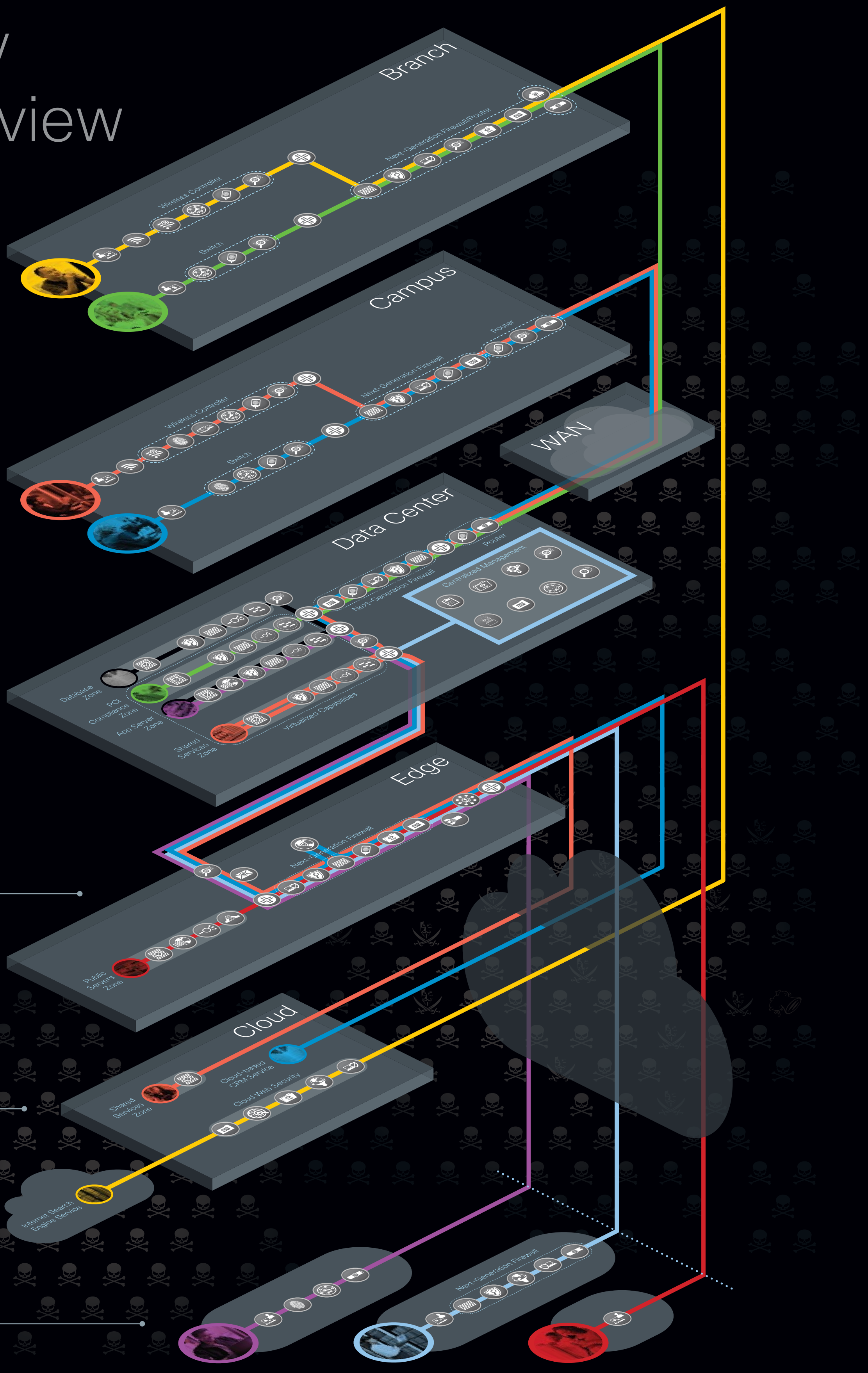
Security Intelligence

Provides global detection and aggregation of emerging malware and threats. It enables an infrastructure to enforce policy dynamically, as reputations are augmented by the context of new threats. This enables accurate and timely security protection.

Management

Management of devices and systems using centralized services is critical for consistent policy deployment, workflow change management, and the ability to keep systems patched. Management coordinates policies, objects, and alerting.

Best Practice Security Capability Flows Overview



5 | Secure Branch

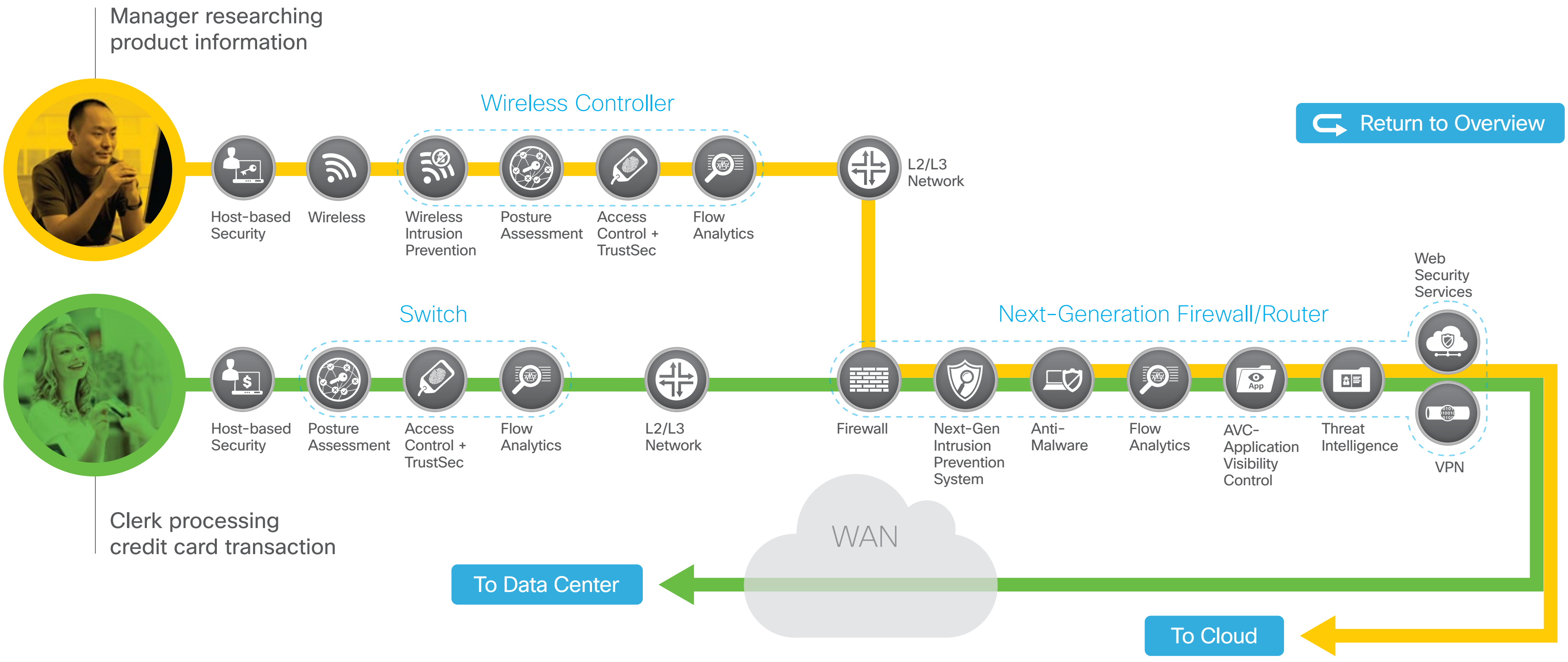
6 | Secure Campus

7 | Secure Data Center

8 | Secure Edge

9 | Secure Cloud

10 | External Zones



Secure Branch

Key Security Challenge

Branches are typically less secure than their campus and data center counterparts. Economics often dictate that it is cost prohibitive to duplicate all the security controls typically found at larger locations when scaling to hundreds of branches. However, this makes them prime targets and more susceptible to a breach. In response, it is important to include vital security capabilities while ensuring cost effective designs in the branch.

Top Threats Mitigated

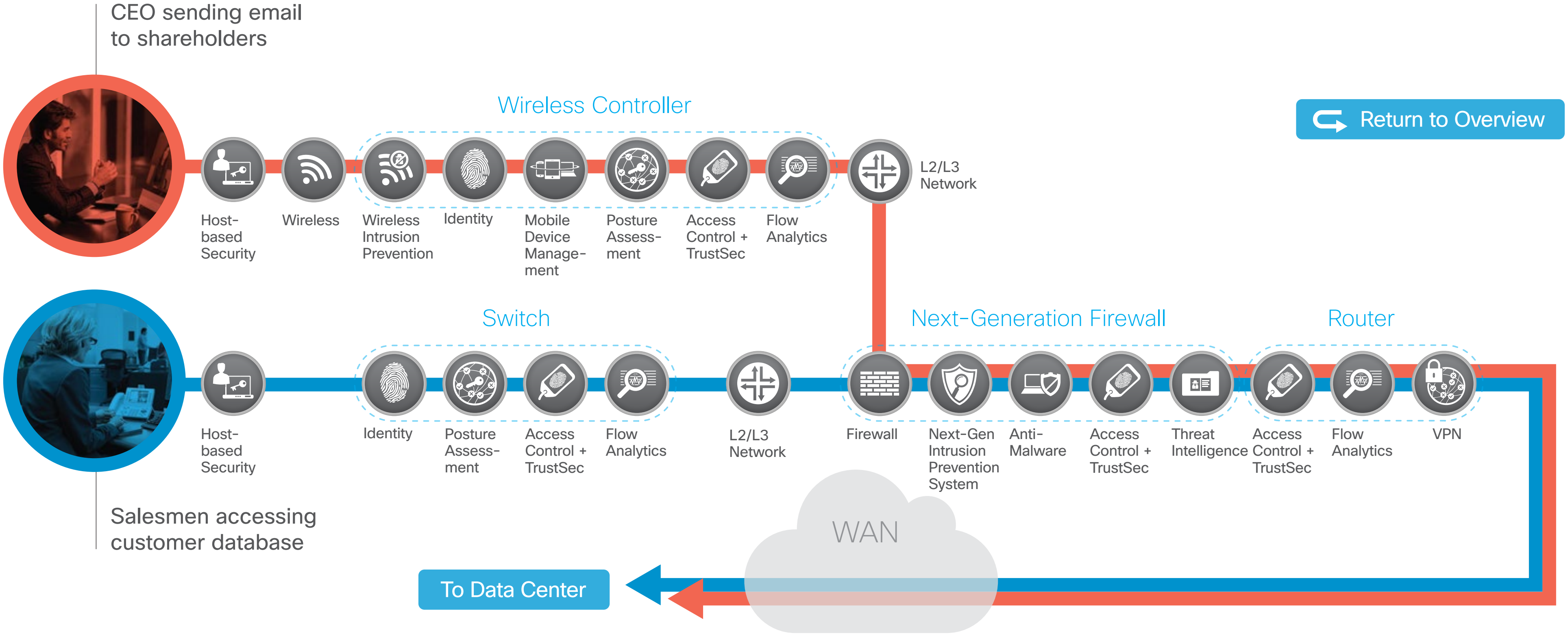
- Endpoint malware (e.g., POS malware)
- Unauthorized/malicious client activity
- Wireless infrastructure exploits (e.g., rogue AP, MitM)
- Exploitation of trust

Capability	Product
	Cloud Web Security, Meraki MX, FirePOWER URL
	Adaptive Security Appliance, Integrated Services Router, Meraki MX
	Cisco Collective Security Intelligence, Cisco Talos Security Intelligence
	Integrated Services Router, Adaptive Security Appliance, Wireless LAN Controller, Catalyst Switch

Capability	Product
	Cisco Advanced Malware Protection for Networks
	Wireless Controller/Catalyst Switch, Centralized Identity Services Engine
	Cisco FirePOWER Services on Adaptive Security Appliance, UCS-E, or FirePOWER Appliance
	Adaptive Security Appliance, Integrated Services Router, Meraki MX

Capability	Product
	AnyConnect Agent, Centralized Identity Services Engine
	Cisco Advanced Malware Protection for Endpoint, AnyConnect, Anti-Virus (partner)
	Centralized Mobility Services Engine, Centralized Wireless LAN Controller, Meraki
App	FirePOWER Services Module or Appliance, Meraki MX

Return to Overview



Secure Campus

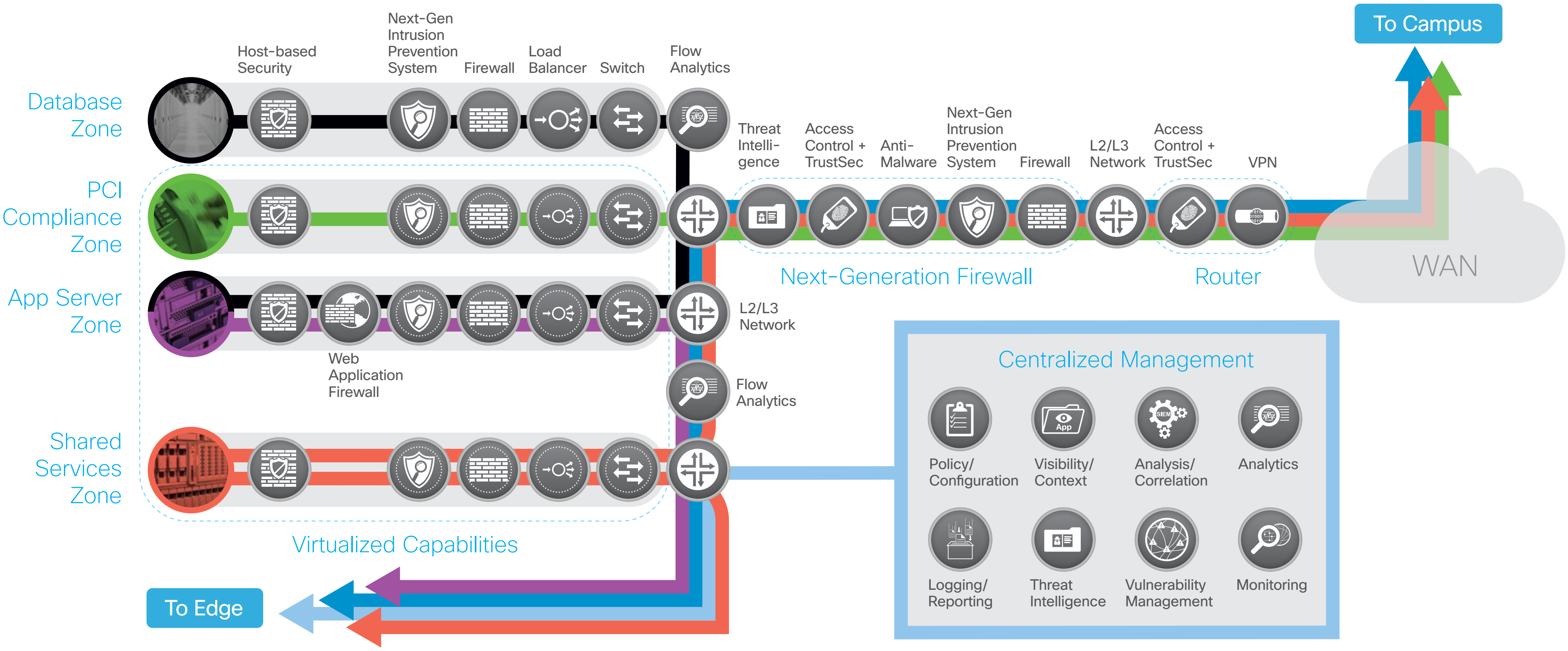
Key Security Challenge

Campuses contain large user populations with a variety of device types and traditionally little internal security controls. Due to the large number of security zones (subnets and VLANs), secure segmentation is difficult. Because of the lack of security control, visibility, and guest/ partner access, campuses are prime targets for attack.

Top Threats Mitigated

- Phishing
- Web-based exploits
- Unauthorized network access
- Malware propagation
- BYOD – Larger attack surface/increased risk of data loss
- Botnet infestation

Capability	Product	Capability	Product	Capability	Product
	Cloud Web Security, Centralized Web Security Appliance		Cisco Advanced Malware Protection for Networks		AnyConnect Agent, Identity Services Engine
	Adaptive Security Appliance, Integrated Services Router, Meraki MX		Wireless Controller/ Catalyst Switch, Identity Services Engine		Cisco Advanced Malware Protection for Endpoint, AnyConnect, Anti-Virus (partner)
	Cisco Collective Security Intelligence, Cisco Talos Security Intelligence		Cisco FirePOWER Services on Adaptive Security Appliance, UCS-E, or FirePOWER Appliance		Mobility Services Engine, Wireless LAN Controller
	Integrated Services Router, Wireless LAN Controller, Catalyst Switch		Adaptive Security Appliance, Aggregation Services Router, Meraki MX		Identity Services Engine, Meraki Mobile Device Management



Return to Overview

Secure Data Center

Key Security Challenge

Data centers contain the majority of information assets and intellectual property. These are the primary goal of all targeted attacks, and thus require the highest level of effort to secure. Data centers contain hundreds to thousands of both physical and virtual servers, segmented by application type, data classification zone, and other methods. Creating and managing proper security rules to control access to (north/south) and between (east/west) resources can be exceptionally difficult.

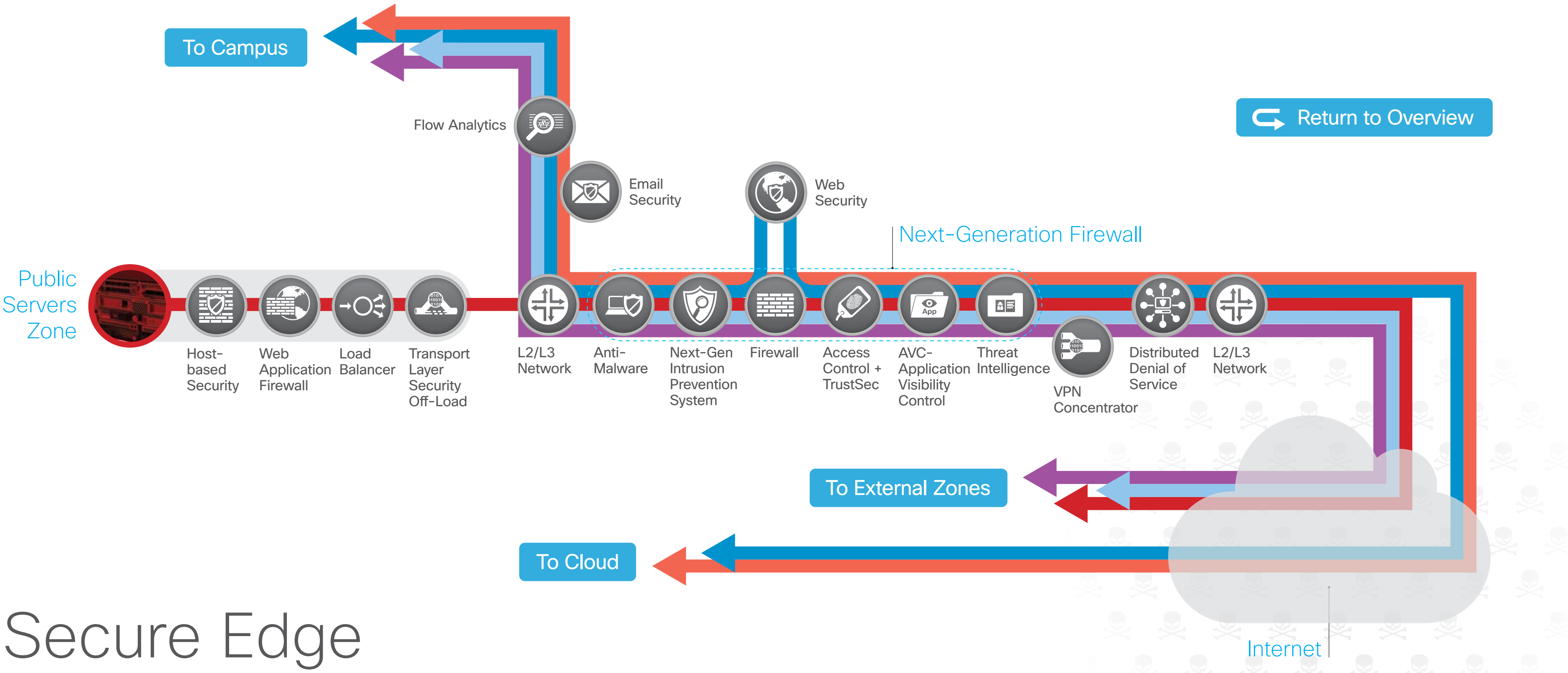
Top Threats Mitigated

- Data exfiltration (data loss)
- Malware propagation
- Unauthorized network access (e.g., application compromise, data loss, privilege escalation, reconnaissance)
- Botnet infestation (e.g., scrumping)

Capability	Product
●	Adaptive Security Appliance, Virtual Security Gateway, Firepower 9300 Appliance
●	FirePOWER Services Module, Appliance, Virtual, Firepower 9300 Appliance
●	Cisco Collective Security Intelligence, Cisco Talos Security Intelligence
●	Netflow Generation Appliance, Lancope FlowSensor, Adaptive Security Appliance

Capability	Product
●	Adaptive Security Appliance, Aggregation Services Router
●	Adaptive Security Appliance, Aggregation Services Router, Firepower Appliance
●	Cisco Advanced Malware Protection for Networks
●	Nexus/Catalyst Switch

Capability	Product
●	Web Application Firewall Technology Partner
●	Load Balancer Technology Partner
●	Cisco Advanced Malware Protection for Endpoint, AnyConnect, Anti-Virus (partner)



Secure Edge

Key Security Challenge

The Internet Edge is the highest risk PIN because it is the primary ingress point for public traffic and the primary egress point to the Internet. Simultaneously, it is the critical resource that businesses need in today's Internet-based economy.

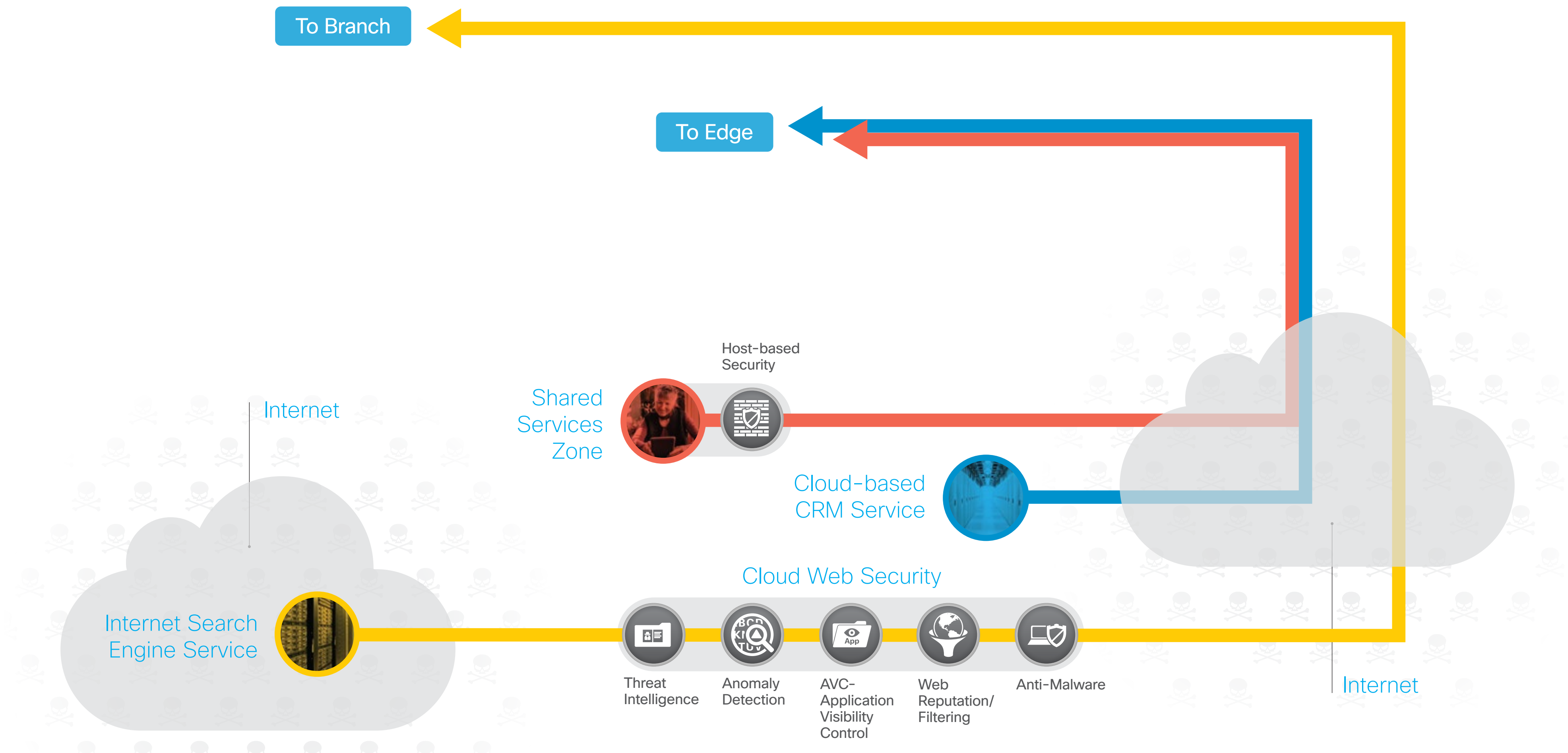
Top Threats Mitigated

- Webserver vulnerabilities
- Data loss
- DDoS
- Man-in-the-Middle

Capability	Product
	Adaptive Security Appliance, Aggregation Services Router
	Cisco Collective Security Intelligence, Cisco Talos Security Intelligence
	Adaptive Security Appliance, Aggregation Services Router, Catalyst Switch
	Adaptive Security Appliance, Firepower 9300 Appliance, Meraki MX
	FirePOWER Services Module or Appliance

Capability	Product
	Cisco Advanced Malware Protection for Networks
	Web Security Appliance, Cloud Web Security
	Email Security Appliance, Cloud Web Security
	Transport Layer Security Offload Technology Partner
	Distributed Denial of Service Technology Partner

Capability	Product
	Web Application Firewall Technology Partner
	Cisco Advanced Malware Protection for Endpoint, AnyConnect, Anti-Virus (partner)
App	FirePOWER Services Module or Appliance, Meraki MX



Return to Overview

Secure Cloud

Key Security Challenge

The majority of cloud security risk stems from loss of control, lack of trust, shared access, and shadow IT. Service Level Agreements (SLAs) are the primary tool for businesses to dictate control of security capabilities selected in cloud-offered services. Independent certification and risk assessment audits should be used to improve trust.

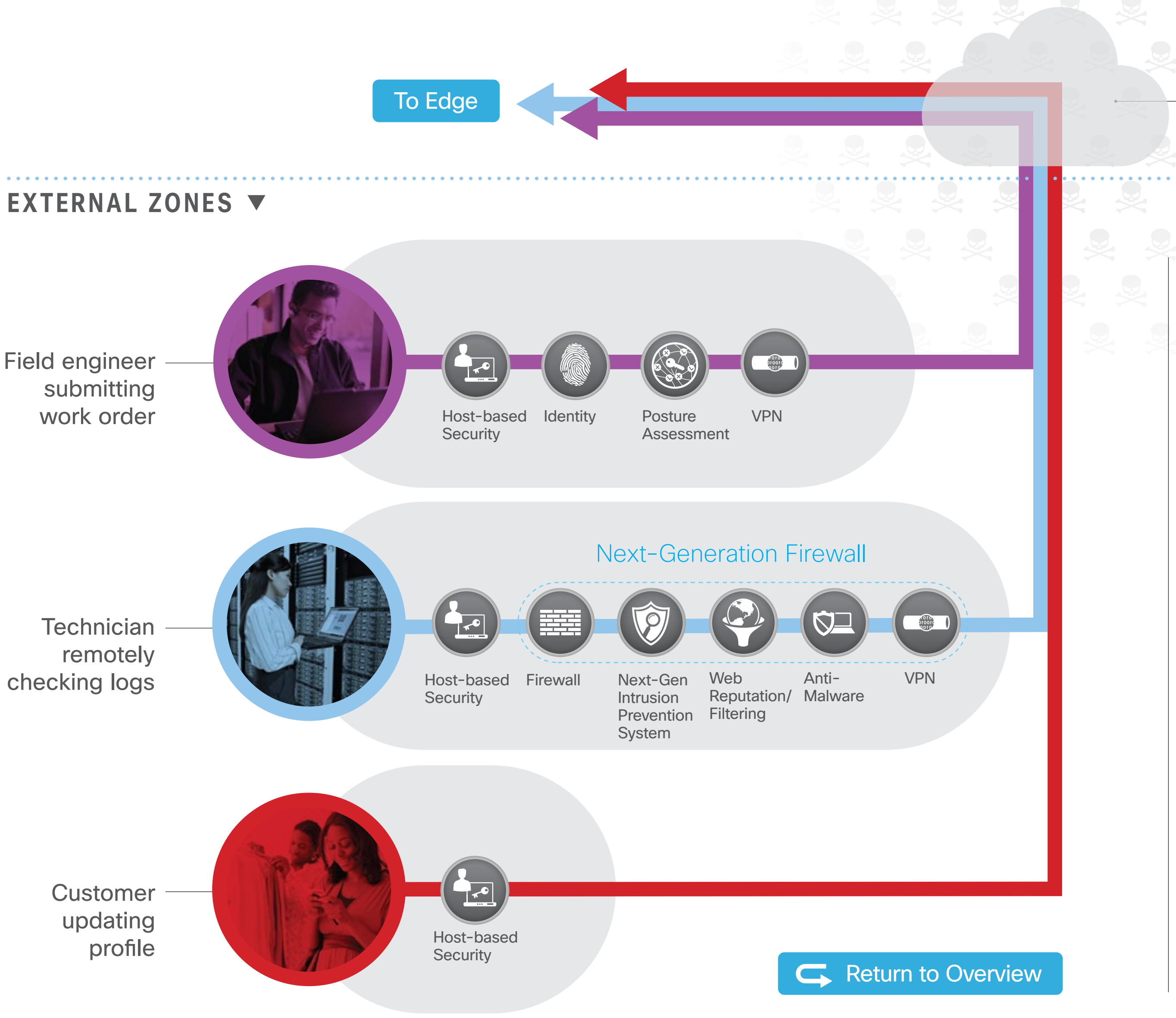
Top Threats Mitigated

- Webserver vulnerabilities
- Virus and malware
- Loss of access
- Man-in-the-Middle

Capability	Product
	Adaptive Security Appliance, Integrated Services Router, AnyConnect, Meraki MX
	Adaptive Security Appliance, Integrated Services Router, Meraki MX

Capability	Product
	Cisco FirePOWER Services on ASA and UCS-E
	Advanced Malware Protection

Capability	Product
	Cloud Web Security, Web Security Appliance, Meraki MX, Partner OpenDNS
	Cisco Advanced Malware Protection for Endpoint, Anti-Virus (partner), AnyConnect



Customers

Key Security Challenge

Securing connections to service offerings is the primary goal when establishing communications with customers outside of the corporate enterprise. A breach or loss of data creates an immediate and heightened lack of trust resulting in loss of commerce.

Remote Workers

Key Security Challenge

Securing remote access for employees connecting to the corporate enterprise from untrusted sites (such as coffee shops and hotels) is critical for maintaining data security. Identity-aware access controls, posture assessments, and encryption enforce a consistent set of policies before allowing access.

Third-Party Vendors and Partners

Key Security Challenge

Insecure access by partners and vendors can quickly compromise business operations. Implement granular access controls, anomaly detection, and SLAs to block unauthorized access and exploitation of trust.

External Zones

Businesses are Connected to Risk

Recent breaches underscore the need to consider the full ecosystem of your partners, customers, vendors, and employees. Traditional perimeter defenses are not sufficient for the attack vectors present today. Identity aware, policy enforced, and threat anomalies must accompany relationships to secure trust.

Top Threats Mitigated

- Endpoint malware
- Unauthorized/malicious client activity
- Exploitation of trust
- Man-in-the-Middle

Capability	Product
	Adaptive Security Appliance, Integrated Services Router, AnyConnect, Meraki MX
	Adaptive Security Appliance, Integrated Services Router, Meraki MX

Capability	Product
	Cisco FirePOWER Services on ASA and UCS-E
	Advanced Malware Protection

Capability	Product
	Cloud Web Security, Web Security Appliance, Meraki MX, Partner OpenDNS
	Cisco Advanced Malware Protection for Endpoint, Anti-Virus (partner), AnyConnect