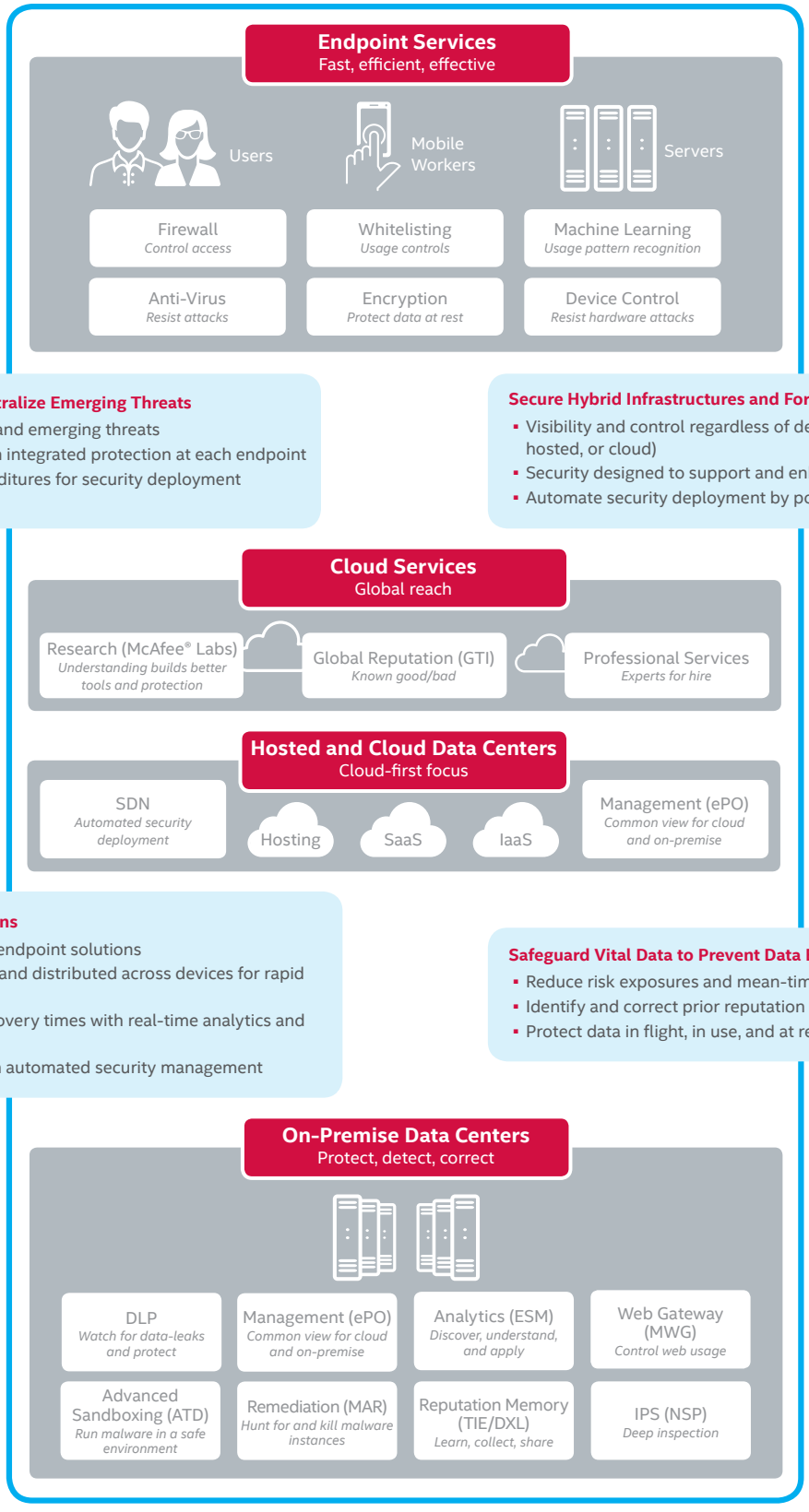
Intel Security Capabilities



Intelligent Endpoint to Neutralize Emerging Threats

- Protect against advanced and emerging threats
- Increase effectiveness with integrated protection at each endpoint
- Reduce operational expenditures for security deployment operations

Secure Hybrid Infrastructures and Fortify Critical Environments

- Visibility and control regardless of deployment (on-premise, hosted, or cloud)
- Security designed to support and enhance virtual environments
- Automate security deployment by policy

Optimize Security Operations

- Integrated perimeter and endpoint solutions
- Reputations are collected and distributed across devices for rapid application
- Reduce discovery and recovery times with real-time analytics and remediation
- Augment limited staff with automated security management

Safeguard Vital Data to Prevent Data Breaches

- Reduce risk exposures and mean-time to remediation
- Identify and correct prior reputation decisions automatically
- Protect data in flight, in use, and at rest

intel Security

Intel Security Products and Services

Endpoint Protection

The McAfee Endpoint Security 10 architecture brings together multiple protection modules within a single framework, enabling them to communicate and work together to deliver stronger protection. Additionally these services can make use of external services such as analytics, sandboxing, and remediation automation to both share and benefit from the sharing of new threat information.

Endpoint protection includes:

- **AV Threat Prevention** – scan for malware and signs of attack
- **Firewall** – Statefully inspect traffic
- **Web Control** – Site ratings and categorization
- **Threat Intelligence Exchange** – Reputation-based controls over what software is trusted and by whom with corporate-wide whitelisting/blacklisting based on usage policies
- **Encryption** – Protection of data at rest
- **Device Control** – Resists attacks through portable hardware
- **Common Administration** – A single management console for all servers and clients, regardless of purpose (client or server), location (on-premise or hosted), or deployment (company owned or cloud sourced)

Supporting Services

- **Global Reputation** – McAfee Global Threat Intelligence (GTI) is a cloud service that discovers, collects, and distributes reputations globally.
- **Research** – McAfee Labs is a leading global source for threat research, threat intelligence, and cybersecurity thought leadership, and delivers threat intelligence in real-time to supplement local protections.

Professional Services

- Collection and Distribution of Global Threat Intelligence
- **Research** – Understanding threats and their perpetrators enabling the building of better protection
- **Professional Services** – Offers comprehensive services from incident response and risk assessment to customized deployments and training.

Data Center Protection (On-Premise, Hosted, and Cloud)

This model helps organizations become more effective at blocking threats, identifying compromises, and implementing remediation as well as countermeasure improvements more quickly.

Data center protection includes:

- **IPS** – McAfee Network Security Platform (NSP) is the industry leading intrusion prevention system, providing both signature and signature-less technologies that defend against zero-day threats. Intelligent workflows and the ability to leverage a Security Connected architecture enables shared learning and the ability to respond to threats in real time.
- **Web Gateway** – McAfee Web Gateway (MWG) controls web usage by analyzing all web traffic, even if it's encrypted. It intercepts attacks before they can challenge endpoints, including threats stealthfully packaged in an attempt to avoid detection.
- **Reputation Memory** – McAfee Threat Intelligence Exchange (TIE) serves as a firm's institutional memory of attacks and their contexts. Builds, collects, and shares reputation information across the entire enterprise. Reduces time to malware detection, protection, and remediation from days and weeks to minutes and milliseconds.
- **Remediation** – McAfee Active Response (MAR) enables the automated and continuous hunting for signs of compromise. It ensures consistent policy enforcement out to the network boundary.
- **Analytics** – McAfee Enterprise Security Manager (ESM) is an industry leading SIEM solution that brings event, threat, and risk data together to provide strong security intelligence, rapid incident response, seamless log management, and compliance reporting.
- **DLP** - McAfee DLP solutions safeguard intellectual property and ensure compliance by protecting sensitive data wherever it lives; on premises, in the cloud, or at the endpoints. Simplified policy management enables proactive data loss prevention while simplifying deployment and use.
- **Advanced Sandboxing** – McAfee Advanced Threat Defense (ATD) is the industry's most effective sandboxing solution, offering both dynamic (execution) and static (malware decompilation) support for superior detection results.
- **Management** – McAfee Enterprise Policy Orchestrator® (ePO) provides an extensible, scalable, centralized management environment for the entire McAfee security portfolio. One screen, deployed on-premises or in the cloud, to connect, manage, and automate security.
- **SDN** – Intel's Security Controller enables software-defined security connects orchestrators and security solutions for managing dynamic environments with automated security provisioning, policy management, protection, and remediation.

novanis™ IT SOLUTIONS

To learn more or to arrange a Novanis consultation:

Walter Meek
217 698 0999 x501
Walter.Meek@Novanis.com

intel Security

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com