

# MVISION Device-to-Cloud Security Suites

**Simplify security, accelerate digital transformation, and better defend against advanced attacks, no matter where and how your teams are working.**

Transformation to the cloud is no longer a choice but a business necessity. Whereas before the transition to the cloud happened gradually and with plenty of strategy and planning, the global pandemic changed all that. Suddenly organizations needed to embrace the cloud to enable a distributed workforce. Sometimes it was so fast that security was an afterthought.

Organizations now need a unified strategy to mitigate risk across all threat vectors — endpoints, network, and cloud. It just doesn't keep on top of the overwhelming present risks, but it also shifts organizations from reactive to proactive security. This better prevents future risk from becoming an impossible burden with limited IT budgets.

<b>MVISION Advanced</b> <b>Proactive Endpoint Threat Prevention</b>	<b>MVISION Premium</b> <b>Full Endpoint Security with EDR and Data Protection</b>	<b>MVISION Complete</b> <b>Comprehensive Threat and Data Protection Across Endpoints, Web, and Cloud</b>
Optimize your endpoint threat protection against the attack campaigns that are critical and keep your data and devices safe.	Building on MVISION Advanced, MVISION Premium provides comprehensive defense against sophisticated attackers (inside and out) for endpoints and data with real-time investigation and response to threats.	Further expanding security protections, MVISION Complete delivers advanced security to confidently enable a secure distributed workforce and accelerate digital transformation with unified threat and data protection across endpoints, web, and cloud, as well as easy investigations and response.
<b>MVISION Insights:</b> Industry-leading proactive endpoint threat management		
▪ McAfee Endpoint + MVISION Insights	▪ McAfee Endpoint + MVISION Insights + <b>DLP + MVISION EDR</b>	▪ McAfee Endpoint + MVISION Insights + DLP + MVISION EDR + <b>MVISION UCE</b>

## SOLUTION BRIEF

### Cloud-Delivered Security Suites for Critical Business Needs

McAfee MVISION Device-to-Cloud suites have been designed to help simplify and accelerate cloud transformation and more effectively defend against advanced attacks. With these cloud-based solutions, organizations can better enable a secure, distributed workforce and more quickly reap the advantages of cloud — enhancing agility, lowering costs, and risk.

The Device-to-Cloud suites all begin with McAfee's MVISION Insights and endpoint security. Capabilities increase as you scale through the offerings.

### Industry-Leading, Proactive Endpoint Threat Management

Comprising the foundation of all three Device-to-Cloud suites is McAfee's unique endpoint threat management solution: MVISION Insights. This industry-first solution intelligently drives endpoint security to be more proactive. It does this by prioritizing and predicting attack activity across the globe. It provides guidance using local intelligence as well as intelligence drawn from McAfee's massive sensor network of more than one billion sensors worldwide.

### Significantly speed detection and response

MSVISION Insights helps reduce blind spots and increase situational awareness by letting you know precisely how your defenses stack up before threats hit. It can proactively track and prioritize local and global threats that are predicted to hit your enterprise.

MSVISION Insights helps you:

- Identify and preempt threat campaigns.
- Prioritize risk level from a single console.
- Reduce mean time to detection and resolution.
- Dynamically strengthen security posture to get ahead of adversaries.
- Spend less time reacting during an attack.

The risk intelligence helps with prioritization, which empowers your enterprise with the insight it needs to focus on the most pressing needs first. It offers a single console for detection, remediation, and preemptive, accelerated response times for significant risk reduction. This is the only endpoint security that offers this combination of capabilities simultaneously. Its proactive, actionable Security Analytics helps you understand the strength of your security posture and address any issues to get ahead of adversaries.

The intelligence and actionable insights give you the best possible cybersecurity stance against the most likely threats and boost confidence in your defenses.

MSVISION helps better safeguard your unique environment with prescriptive guidance and automated actions to proactively defend against threats and increase your effectiveness against outside attacks.

In the MVISION Premium and MVISION Complete suites, MVISION Insights threat analysis can easily pivot to take advantage of McAfee® MVISION EDR to search on additional context, like indicators of compromise (IoCs) and reduce investigation cycles. Threats are presented

### MSVISION Insights

---

- **Prioritize** – Know if you are in the path of the most dangerous campaigns that matter to you. Your personalized dashboard will prioritize global telemetry from one billion sensors based on your industry sector and geography.
- **Predict** – Receive personalized automated assessments of your security posture risks against dangerous campaigns pinpointing potential gaps in your countermeasures.
- **Prescribe** – Be equipped to adjust compensating controls with the only prescriptive, actionable, endpoint threat management solution available today.

## SOLUTION BRIEF

to you in a manner that is understandable, and then those threats are prioritized and actionable. Guided response based on analyzed and prioritized intelligence and insight elevates even novice analysts. From the integrated console, you can quickly and easily respond by making changes to your configurations, isolating infected devices, updating policy, or pivoting to endpoint detection and response (EDR) to enrich and accelerate your investigation.

Preview of MVISION Insights: [www.mcafee.com/enterprise/en-us/lp/insights-preview](http://www.mcafee.com/enterprise/en-us/lp/insights-preview)

### Proactive, Cloud-Native Endpoint Threat Protection

Coupled with MVISION Insights and providing the basis for all suites, McAfee® Endpoint Security (ENS) provides advanced endpoint protection. It enables customers to respond to and manage the threat defense lifecycle and provides a collaborative, extensible framework to reduce the complexity of conventional multivendor endpoint security environments.

It offers visibility into advanced threats to help speed detection and remediation response times when faced with suspicious applications, downloads, websites, and files. If needed, Rollback Remediation can automatically return your endpoints to a healthy state. It helps find and remove redundancies caused by multiple point products or defenses, while a common endpoint architecture integrates several layers of protection to allow threat insights to be shared for faster convictions and analysis.

McAfee ENS was built for real-time communication between threat defenses. It shares global threat intelligence and real-time local event intelligence between endpoints to further aid in rapid detection and response. Management is kept simple through a true centralized console, and easy-to-read dashboards and reports. With McAfee Endpoint Security, you can ensure system uptime for users, find more opportunities for automation, and simplify complex workflows.

McAfee Management of Native Encryption safeguards data on devices by managing the native encryption functionality offered by Apple FileVault on macOS, and Microsoft BitLocker on Windows, directly from McAfee ePO. McAfee Device Control offers content-aware data protection for USBs and other external storage devices.

McAfee Endpoint Security's orchestrated analysis of and response to threats enables it to automatically protect your environment from zero-day threats like ransomware and advanced malware attacks, and to stop network infection simultaneously. This provides you with the robust endpoint security solution that today's advanced threats require.

### Full Endpoint Security with EDR and Data Protection

Scaling in protection and coverage, the McAfee Premium suite provides additional functionality including more advanced data loss prevention (DLP) capabilities and MVISION Endpoint Detection and Response (EDR), a key component of an integrated security ecosystem. MVISION EDR is a simple, powerful threat detection and response solution that helps reduce mean time to detect

#### McAfee Endpoint + MVISION Insights

- Increase proactive attack surface management.
- Provide ransomware and advanced malware defense.
- Safeguard data and devices.

## SOLUTION BRIEF

and respond, as well as increase operational efficiency. It makes detecting and responding to threats easy and fast.

AI-guided investigation automatically gathers, summarizes, and visualizes evidence from multiple sources and iterates as the investigation evolves. With in-depth understanding of the threat and single-click response capabilities, MVISION EDR enables you to quickly and confidently respond to threats. AI-guided investigations help maximize the skills of existing staff by walking analysts through the questions they should ask and providing answers in near real-time. This makes it easier for analysts of any experience level to quickly and more effectively prioritize and triage threats, and to minimize potential disruption. Cloud-based deployment and analytics enable skilled security analysts to focus on strategic defense instead of tool maintenance.

### **Safeguard sensitive data with more advanced data protection**

To help protect sensitive data from day-to-day end-user actions, McAfee DLP Endpoint and Device Control deliver increased visibility and control to stop data loss caused by risky employee behaviors. It can help prevent sensitive or confidential information from being shared via email, leaking onto the internet, shared via social media, or added to removable devices. It can also prevent unauthorized printing, copying, pasting, or screen captures.

### **Comprehensive Threat and Data Protection Across Endpoints, Web and Cloud**

Further expanding capabilities offered in our MVISION Device-to-Cloud offering, the MVISION Complete suite adds capabilities that provide comprehensive data and threat protection across endpoints, network, and web.

McAfee Unified Cloud Edge (MVISION UCE) converges three award-winning technologies into a single, next-gen solution:

- Cloud access security broker (CASB): Direct API and reverse proxy-based visibility and control for cloud services,
- Secure web gateway (SWG): Proxy-based visibility and control over web traffic and unsanctioned cloud services, and
- Data loss prevention (DLP): Agent- and network- based visibility and control over sensitive data.

These technologies work together as a next-gen SWG solution to protect data from device-to-cloud and to prevent web- and cloud-based breach attempts that are often invisible to a corporate network. MVISION UCE reduces the cost and complexity of modern cybersecurity and extends a hyper-scale service edge with a more mature, resilient, and higher performance threat and data protection infrastructure. It creates a secure environment for the adoption of cloud services and for access to the cloud from any device for ultimate workforce productivity.

### **MSIVISION Premium**

- Minimize SOC analyst fatigue with high-fidelity detections.
- Simplify incident investigation and response with AI-guided investigations.
- Safeguard sensitive data with advanced data loss prevention.

**McAfee Endpoint + MVISION Insights + DLP + MVISION EDR**

## SOLUTION BRIEF

MVISION UCE in the MVISION Complete suite provides:

- Zero-day malware protection from any cloud service,
- Sanctioned and unsanctioned application protection with Integrated CASB,
- 99.999%<sup>1</sup> service availability to protect a distributed workforce,
- Neutralize ransomware and protect against advanced web-based attacks with remote browser isolation,
- Blazing fast, low-latency always-on security with a hyper-scale service edge,
- Advanced, multi-vector data loss prevention, and
- Visibility and control of inbound and outbound encrypted traffic to better protect against advanced threats and protect data.

### Cloud-based and Direct-to-Cloud Architecture Delivers Enterprise Scale and Resilience

McAfee's cloud-based Device-to-Cloud suites are available via subscription and have been tailored to meet our customers' most critical security needs. The solutions are backed by partner-engaged services to ensure reliable implementation so that your security team can focus on what matters — your business.

#### MVISION Complete

- Enable a distributed workforce with a 99.999%<sup>1</sup> available direct-to-web and -cloud architecture.
- Unified threat and data protection across cloud, web, and endpoints.
- Lower cost and complexity of cloud adoption.

**McAfee Endpoint + MVISION Insights + DLP + MVISION EDR + MVISION UCE**

1. 99.999% availability is based on historical information and not a guarantee of future performance.

## SOLUTION BRIEF

### MVISION Advanced

#### Proactive, Cloud-native Endpoint Threat Protection

MVISION management console (mvision.mcafee.com)

- Workspace dashboards, multi-admin, role-based controls
- Deploy up to 5 devices per user including WFH devices

Prioritized & Predictive Threat Intelligence (Insights)

- Proactive & Prescriptive Policy Improvement
- Security Risk Advisor for Endpoints with guided actions

Block malicious and target attack tactics and techniques (Next-gen AV)

- Integrated preventive controls (Static and Dynamic ML, Firewall, Exploit Prevention, Behavior Monitoring, Native OS Security Controls)
- Web controls to block suspicious websites and downloads
- Contain and restrict bad behaviors of suspicious apps
- Automatically rollback ransomware to known good state
- USB and port controls to block local threats and data exfiltration
- Manage authentication and enforce native OS data encryption

### MVISION Premium

#### Full Endpoint Security with EDR and Data Protection

MVISION management console (mvision.mcafee.com)

- Workspace dashboards, multi-admin, role-based controls
- Deploy up to 5 devices per user including WFH devices

Prioritized & Predictive Threat Intelligence (Insights)

- Proactive & Prescriptive Policy Improvement
- Security Risk Advisor for Endpoints with guided actions

Block malicious and target attack tactics and techniques (Next-gen AV)

- Integrated preventive controls (Static and Dynamic ML, Firewall, Exploit Prevention, Behavior Monitoring, Native OS Security Controls)
- Web controls to block suspicious websites and downloads
- Contain and restrict bad behaviors of suspicious apps
- Automatically rollback ransomware to known good state
- USB and port controls to block local threats and data exfiltration
- Manage authentication and enforce native OS data encryption

Endpoint threat detection, investigation, and response (EDR)

- Continuous monitoring of endpoint with 30-day event history
- Advanced threat hunting with real-time search on endpoints
- AI-Guided threat investigations and response guides
- APIs and integrations with SIEM, Threat Intelligence, SOAR, etc.

Block and control access of sensitive data at the Endpoint (DLP)

- Block sensitive data and ensure compliance (PCI, PII, and PHI)
- Monitor and address day-to-day user risky actions

### MVISION Complete

#### Comprehensive Threat & Data Protection Across Endpoints, Web, and Cloud

MVISION management console (mvision.mcafee.com)

- Workspace dashboards, multi-admin, role-based controls
- Deploy up to 5 devices per user including WFH devices

Prioritized & Predictive Threat Intelligence (Insights)

- Proactive & Prescriptive Policy Improvement
- Security Risk Advisor for Endpoints with guided actions
- Security Risk Advisor for Cloud with guided actions

Block malicious and target attack tactics and techniques (Next-gen AV)

- Integrated preventive controls (Static and Dynamic ML, Firewall, Exploit Prevention, Behavior Monitoring, Native OS Security Controls)
- Web controls to block suspicious websites and downloads
- Contain and restrict bad behaviors of suspicious apps
- Automatically rollback ransomware to known good state
- USB and port controls to block local threats and data exfiltration
- Manage authentication and enforce native OS data encryption

Endpoint threat detection, investigation, and response (EDR)

- Continuous monitoring of endpoint with 30-day event history
- Advanced threat hunting with real-time search on endpoints
- AI-Guided threat investigations and response guides
- APIs and integrations with SIEM, Threat Intelligence, SOAR, etc.

Block and control access of sensitive data at the Endpoint (DLP)

- Block sensitive data and ensure compliance (PCI, PII, and PHI)
- Monitor and address day-to-day user risky actions

Hyper Scale Secure Access Service Edge (SASE) with 99.999% availability (Cloud Secure Web Gateway, DLP and CASB)

- Real-time threat protection from web and cloud attacks (AV, Dynamic emulation, Global Threat Intelligence, Advanced Phishing Protection)
- Unified DLP across endpoint, web, and cloud
- Advanced Shadow IT Visibility & Control
- Real-time collaboration control
- User and Entity Behavior Analytics (UEBA)
- Dynamic Security for Sanctioned Apps



6220 America Center Drive  
San Jose, CA 95002  
888.847.8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. McAfee technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at [mcafee.com](http://mcafee.com). No online connected systems can be absolutely secure. Copyright © 2021 McAfee, LLC. 4633\_0920  
JANUARY 2021