CrowdStrike Store

AUTOMOX

CROWDSTRIKE

Data Sheet

AUTOMOX: ENDPOINT HARDENING

Reducing the attack surface with cross-platform, globally accessible cyber hygiene at scale

CHALLENGE

Corporate environments are evolving to face growing cyber threats by adopting cloud-native products like the CrowdStrike Falcon® platform to scale their endpoint security perimeter beyond the office walls. However, the security teams that manage and enforce the cyber hygiene of these endpoints — including patch management, local policy enforcement and vulnerability mitigation — continue to rely on legacy technology and on-premises deployment infrastructure, with scaling limitations due to connectivity needs.

As corporate networks continue to become more technologically diverse, with multiple operation systems and a large inventory of third-party software, existing patch management and cyber hygiene solutions are unable to keep up, leaving vulnerabilities unpatched for an average of 102 days. As organizations continue to grow and evolve, many businesses have been forced to adopt multiple tools that require extensive training, dedicated on-site resources and multiple dashboards to try to keep up with the basics of endpoint hardening.

By not actively addressing vulnerabilities, gaps are being left in the basic security perimeter — and CrowdStrike Falcon must work harder to keep the endpoints secure.

KEY BENEFITS

Reduce time to remediation of discovered and reported endpoint vulnerabilities from CrowdStrike® Falcon Spotlight™

Remediate discovered vulnerabilities before weaponization

Patch and configure Windows, macOS, Linux and third-party software at scale through cloud-native controls

Create, automate and enforce custom policies leveraging Bash and PowerShell

SOLUTION

As a cloud-native patch management solution, Automox naturally complements CrowdStrike's cloud-native endpoint security solution.

Cloud-native and globally available, Automox endpoint hardening enforces operating system (OS) and third-party patch management, security configurations, and custom scripting across all managed devices from a single, intuitive console. Automox enables IT teams to scale with the growth and needs of an organization by providing automated toolsets, from patch management to configuration enforcement. IT teams also gain in-depth visibility of on-premises, remote and virtual endpoints, no matter their location — all without the need for a virtual private network (VPN) or on-premises management servers.

Using the information provided through CrowdStrike Falcon Spotlight, joint customers manage their investigation of threats and vulnerabilities from the Falcon platform, and using Automox can quickly resolve vulnerabilities for all of their managed endpoints. Automox and CrowdStrike help minimize the manual effort behind patch management and risk mitigation through automation, all while ensuring managed endpoints are protected against the most advanced threats. Providing full coverage of automated endpoint hardening and advanced endpoint protection raises joint customers' security confidence.

With the two solutions in place, an organization can prioritize remediation at scale with Automox, ensuring that the CrowdStrike Falcon solution is focused on critical threats.

"We needed a solution that was cloud-based, served our multi-OS environment and gave us the right mix of automation and control needed to configure and customize for a variety of end users. Automox just worked."

Jonathan Sibray
Senior IT Director at University of Colorado Law School

BUSINESS VALUE

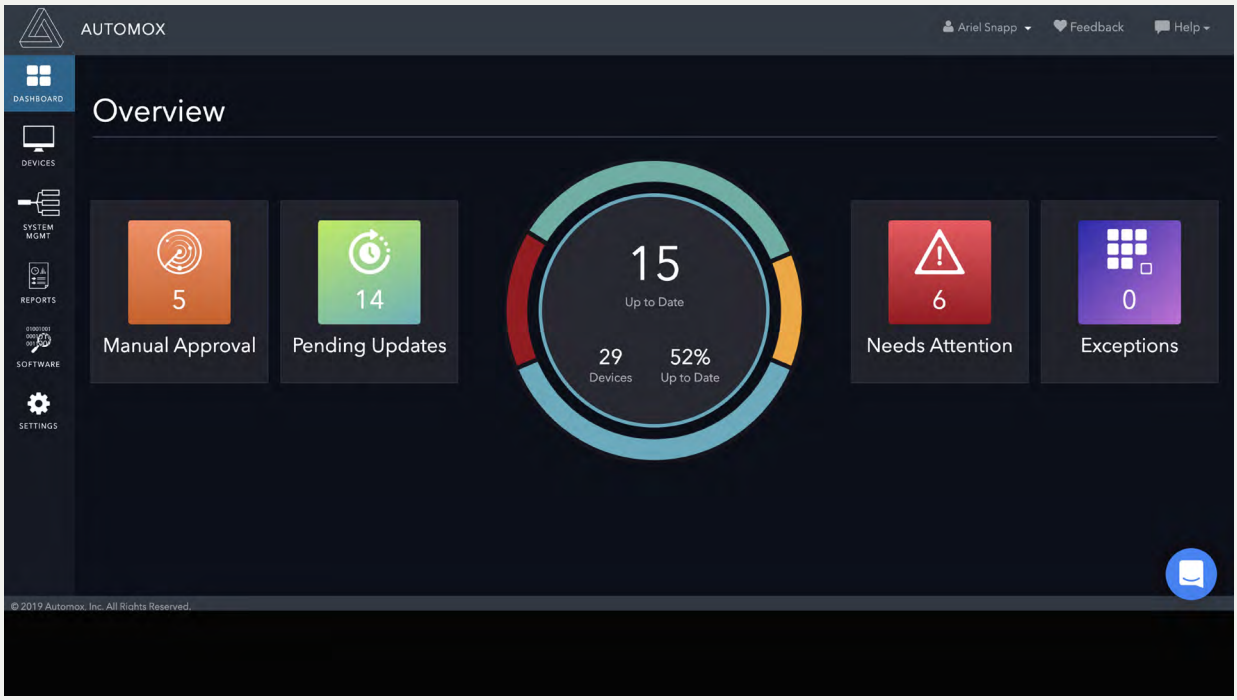
Use Case	Solution	Benefits
Legacy patching solutions are cumbersome and offer a terrible user experience for administrators and end users.	Automox's automating patching and endpoint hardening reduces the burden on IT and security operations center (SOC) analysts, freeing up valuable cycles to address other security threats.	Once you deploy the Automox lightweight agent using the installer and installation script, or your preferred package management tool, you have immediate access to the hardware and software inventory on the connected endpoints.
Traditional on-premises patch management solutions are not designed to scale beyond the office walls, leaving remote endpoints unpatched and unsupported.	Automox is globally accessible and does not require a VPN, meaning there is no functional difference between being on-premises or remote. Patching and endpoint hardening happen regardless of physical location.	IT and SecOps can quickly gain control and share visibility of on-premises, remote and virtual endpoints without the need to deploy costly infrastructure. A single, intuitive console with consistent workflows for Windows, macOS and Linux streamlines learning curves and speeds time to remediation.
Legacy solutions often require extensive labor hours, resulting in high operational costs.	Automating patching and endpoint hardening reduces the tasks for IT and SOC staff, lowering operational costs.	Cloud-based deployment and automation workflows leverage the advantage of the scalability and global availability of a software-as-a-service (SaaS) solution.

AUTOMOX

KEY CAPABILITIES

- Automates policies and groups to allow you to harden endpoints faster than adversaries can exploit vulnerabilities
- Provides visibility into the status of endpoints across on-premises, remote and virtual environments
- Allows you to customize policies for OS and third-party application updates or patches to eliminate threat vectors, and set up groups to include/exclude what needs to be patched
- Enables you to quickly resolve issues with all managed endpoints using the vulnerability information provided through Falcon Spotlight, regardless of location and with no need for a VPN

AUTOMOX CONSOLE



ABOUT AUTOMOX

Facing growing threats and a rapidly expanding attack surface, understaffed and alert-fatigued organizations need more efficient ways to eliminate their exposure to vulnerabilities. Automox is a modern cyber hygiene platform that closes aperture of attack by more than 80% with just half the effort of traditional solutions.

Cloud-based and globally available, Automox enforces OS and third-party patch management, security configurations, and custom scripting across Windows, Mac and Linux from a single intuitive console. IT and SecOps can quickly gain control and share visibility of on-premises, remote and virtual endpoints without the need to deploy costly infrastructure.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Start Free Trial
of Next-Gen AV

Learn more **www.crowdstrike.com**