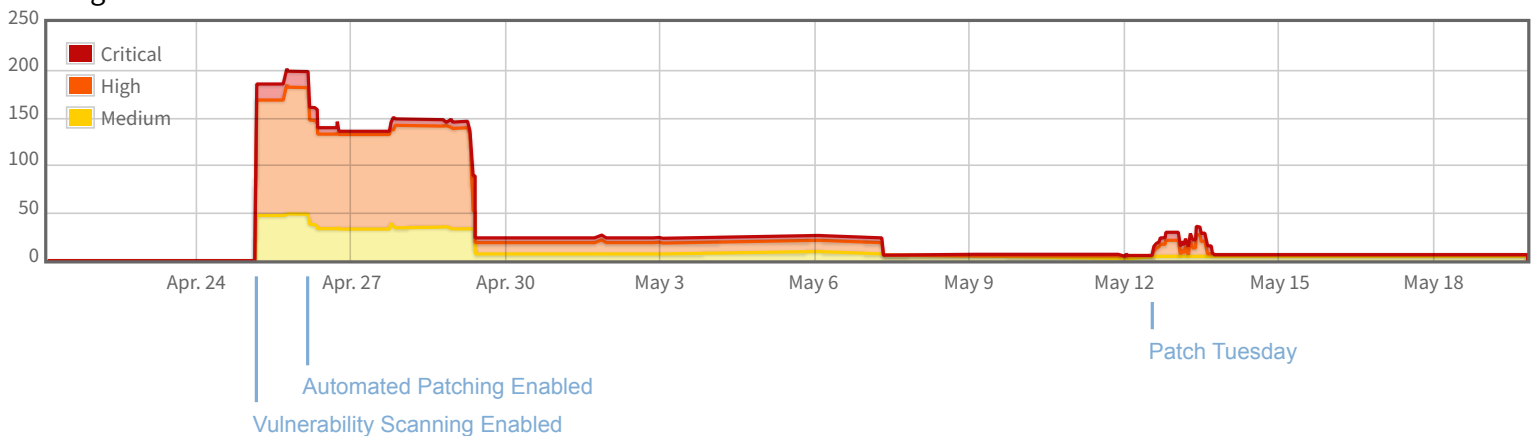# LITHIK
SECURITY MANAGER

Do you know if your network is safe?

Do you have the time to make it safe?

Would you know if you were breached?

Not many people can answer yes to all those questions. The Lithik Security Manager gives you the information you need to really understand where your risks are. Between automatically fixing about 90% of the vulnerabilities, and giving you details on how to fix the rest, your network will never have been more secure, and you'll be able to prove it. Stop operating in the dark and start experiencing the peace of mind that comes from knowing your network is safe.

Missing Patches on Windows Machines

Legend:
- Critical
- High
- Medium

Y-axis: 0, 50, 100, 150, 200, 250

X-axis: Apr. 24, Apr. 27, Apr. 30, May 3, May 6, May 9, May 12, May 15, May 18

Annotations: Automated Patching Enabled, Vulnerability Scanning Enabled, Patch Tuesday

"With the scorecard I can instantly tell how well it's working – way better than a gauge."
"Our organization is far more secure now than before the appliance was installed."

Find out more at lithik.com/lsm

Benefits

Awareness

One of the biggest obstacles to securing your network is how hard it is to actually figure out where you are most vulnerable. A Windows domain is already a tricky thing to administer. When you throw in individually managed routers, switches, firewalls, etc., even experienced auditors can miss potential threats. Maybe a vulnerability scan detects the issues, but the 1,000 page report you often end up with is hardly actionable. The LSM puts all this information in one place, and gives you the ability to instantly sort and filter the information in a way that's understandable. You want to see the vulnerabilities on an individual machine? No problem. You want to see all the Windows vulnerabilities that can't be fixed by a patch? Piece of cake. You want a report that lays it all out? Pick a format.

"The LSM is a powerful window into our systems and security."

– CIO

Security

Describing the work it takes to run a vulnerability mitigation program that's anything close to comprehensive, typically involves words like "drudgery" or "impossible". You'd like your patching software to just work, but instead it's finicky and mysteriously fails to fix certain items without any explanation. When you see the LSM try its hand, the biggest mystery you'll be left with is why you didn't get it sooner. Between improvements beyond the baseline Windows patching software and updates for popular third party software, it's not uncommon to see 90% improvement on a network that already had a patch program in place.

"It works like an ox – the scans and remediation were continuous throughout the day."

– IT Consultant

Simplicity

It's pretty popular to claim software is "Easy to use", yet include a 200 page PDF manual. We'd rather things work the way you'd expect them to, which is why our setup guide only needs to be a few pages long. Within 30 minutes of powering it on, you can have the LSM hard at work scanning for and mitigating vulnerabilities. If there's a setting that's risky, the LSM will tell you then and there. If the policies you set conflict with each other, or if one of your machines isn't being managed, it will be laid out clearly.

"I was able to quickly and effectively navigate through the GUI within 10 minutes of logging in."

– IT Consultant

"It's not necessary to be a security engineer if you have their tools packaged into a nifty appliance like this."

– IT Administrator

Feature Overview

Executive Level Summaries for Key Security Concerns
- Windows Patch Status
- Firewall Egress Filtering
- Vulnerabilities
- Device and Software Approvals

Fully Customizable Email/Text Alerts

Integrated Filtering and Sorting for All Data

Customizable Automatic Patch Management
- Supports different policies for different groups
- Create custom groups, or set according to network, domain role, or OU

Vulnerability Monitoring Powered by Your Choice:
- Nessus
- OpenVAS

Device Inventory for All Network Devices, including:
- Approval system for new devices
- Comprehensive device history
- Detailed OS and hardware information

Searchable Software Inventory, including:
- Approval system for newly installed software

Integrated Antivirus Monitoring (for selected products)

Active Directory Inventory and Changes, including:
- Approval system for new accounts and memberships
- Alerts for suspicious account activity

System Events
- Context-relevant events are displayed on each page
- Every network event is recorded in a time-stamped, categorized, downloadable log

Reporting
- On-demand PDF reports of any combination of inventoried components, events, or current metrics
- Customized monthly PDF reports can be generated automatically at the beginning of each month
- CSV and text reports also available

Firewall Monitoring Add-On
- Egress filtering configuration monitoring
- Monitor events and policy violations for selected firewalls
- VPN access logs available for selected firewalls

Monitor ❯ Manage ❯ Report

Find out more at lithik.com/lsm