

Brochure

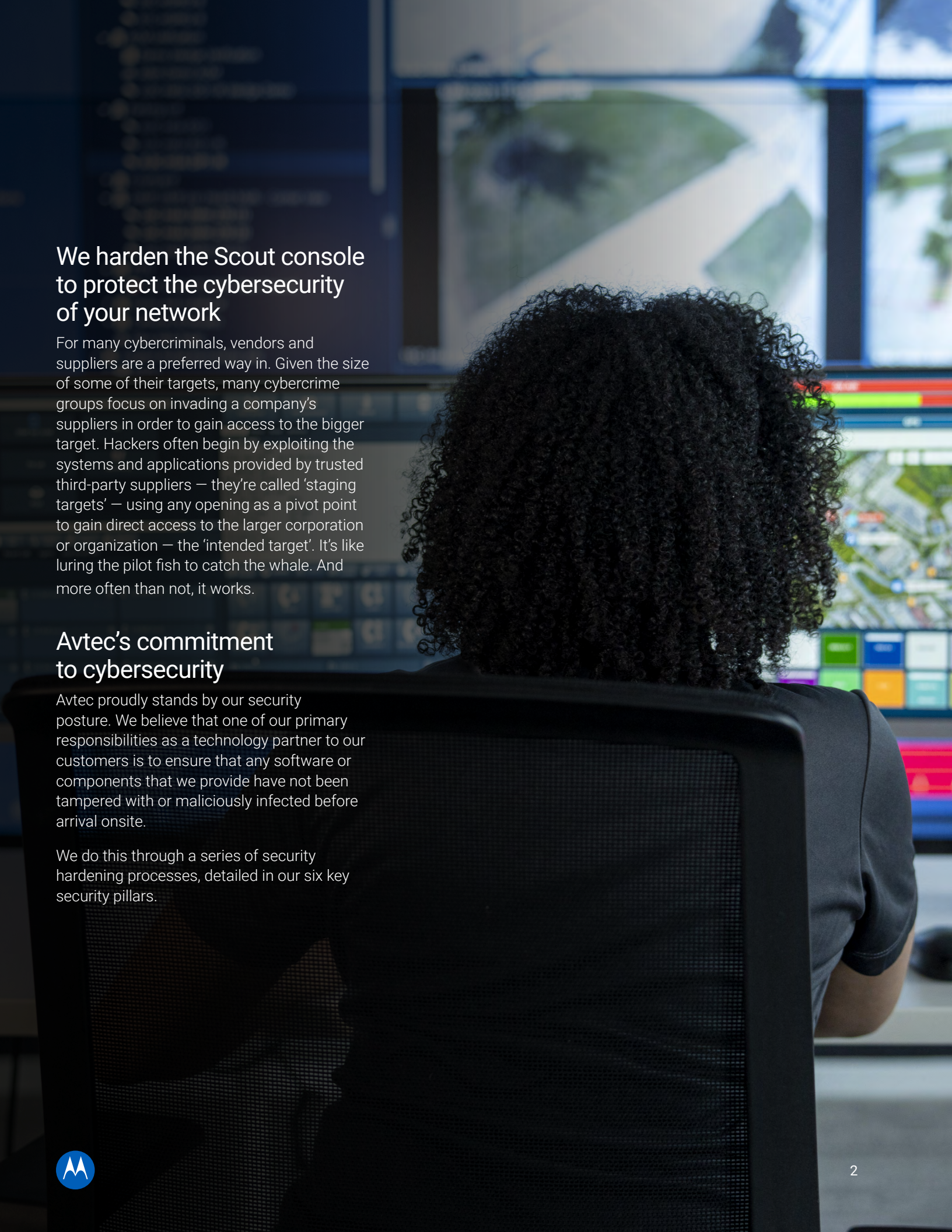
Avtec Scout

# Commitment to cybersecurity



**MOTOROLA** SOLUTIONS





## We harden the Scout console to protect the cybersecurity of your network

For many cybercriminals, vendors and suppliers are a preferred way in. Given the size of some of their targets, many cybercrime groups focus on invading a company's suppliers in order to gain access to the bigger target. Hackers often begin by exploiting the systems and applications provided by trusted third-party suppliers — they're called 'staging targets' — using any opening as a pivot point to gain direct access to the larger corporation or organization — the 'intended target'. It's like luring the pilot fish to catch the whale. And more often than not, it works.

## Avtec's commitment to cybersecurity

Avtec proudly stands by our security posture. We believe that one of our primary responsibilities as a technology partner to our customers is to ensure that any software or components that we provide have not been tampered with or maliciously infected before arrival onsite.

We do this through a series of security hardening processes, detailed in our six key security pillars.





# Our 6 key security pillars

1. Patch management
2. STIG updates
3. Security documentation
4. Internal QA testing
5. Code signing
6. Third-party security audits

## Patch management

Patch management is the process of receiving, evaluating and then applying vendor patches to systems and applications during operational activities. Patches are issued by the vendor to repair identified deficiencies.

### Avtec's patch management process

Three times per year, we qualify and include the latest critical and important Microsoft Security Patches for the main operating systems:

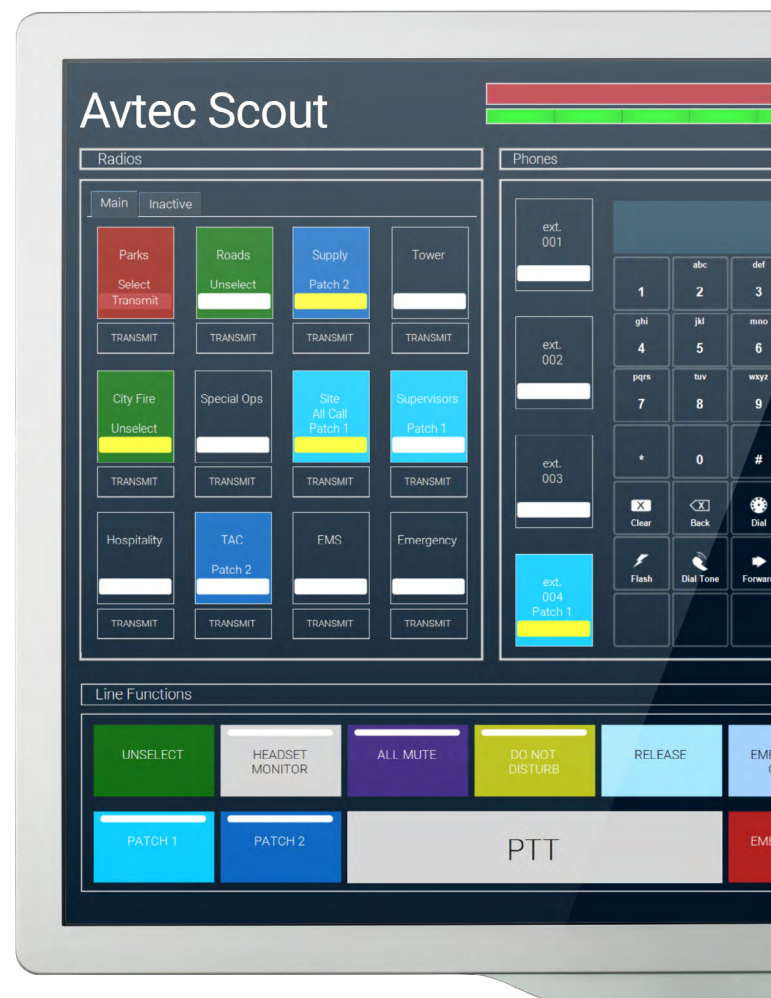
- Windows 11
- Windows Server 2022

Here's what we do once we've received a security patch:

- We evaluate the applicability of the patch within our operating environment
- We test the patch to ensure it doesn't break any feature or required process
- We update the list of approved patches during each Scout release cycle

### Security patching support

Safeguard your investment with Avtec Protect™, our comprehensive security patching service. Avtec Protect helps keep your computers and equipment up-to-date and fully protected with the latest OS patches and STIG settings, all while maintaining the full functionality of your Scout consoles.



# STIG and NERC CIP updates

STIG stands for Security Technical Implementation Guide. STIGs are distributed by the U.S. Department of Defense (DoD) and cover the configurations of an organization's routers, databases, firewalls, domain name servers and switches.

Implementing STIGs can harden a system and minimize network-based attacks and prevent system access.

## Avtec's STIG updates process

Three times per year, we update, apply and verify the following STIGs from the DoD:

- STIG for Windows 11
- STIG for Windows Server 2022
- STIG for Windows Firewall
- STIG for Windows Defender
- STIG for Microsoft NET framework

As you can see, the Avtec Scout dispatch console's baseline security hardening is on par with the U.S. Department of Defense's guidelines.

NERC stands for the North American Electric Reliability Corporation. Each of its Critical Infrastructure Protections (CIPs) guides include requirements for the utilities industry, such as securing remote access.

## Avtec's NERC CIP updates process

Three times per year, Avtec provides robust security documentation of how we adhere to each section and requirement in the following NERC CIP standards:

- NERC CIP-005 Electronic Security Perimeter
- NERC CIP-007 Standard Cyber Security — Systems Security Management
- NERC CIP-010 Configuration Change Management and Vulnerability Assessments

If you're a utilities provider, the Avtec Scout console provides a dispatch solution with all the security documentation you'll need to pass security audits.

Our Scout console is compliant with NERC CIP and the security controls of the National Institute of Standards and Technology (NIST) Special Publication 800-53, as well as other industry standards that have been developed over the past 30 years.

In the last 10 years:

**146M**

consumers compromised  
by data hacks

**\$1.4M**

increase in average business  
loss to cybercrime

**68%**

oil and gas producers with at least  
one security compromise

Source: BTB Security and The Ponemon Institute



# Security documentation

Reporting on the status and the operation of each system and application is another standard cybersecurity effort Avtec regularly employs. We do this to properly understand the security profile and needs of our customers. We also track any variables to help support long-term IT health and security.

## Avtec's security documentation process

Avtec documents all our various configurations, including changes in inputs, outputs, uses and environment. Throughout the calendar year, we regularly share the following information as indicators of the Scout console's security hardening:

- Network documentation
- Configuration guides
- NERC-CIP compliance
- Code signing
- Release notes

# Internal quality assurance testing

Performing quality assurance (QA) testing is necessary to ensure all security checks have been addressed. Equally important during this testing phase is evaluating whether a particular security check has a negative effect on the system.

The idea is that the Scout dispatch console has to be secure and functional. Most dispatch console vendors don't do this. We do.

## Avtec's internal QA testing process

Avtec conducts internal audits of the Scout console's security configuration prior to each release. These audits ensure the console's adherence to emerging security requirements. This is a vital step in our system hardening process, as it demonstrates how well the requirements are being met by the software as well as showing how well the code is operating as intended.

For QA testing purposes, we utilize a number of industry standard tools including Nessus, a remote security scanning tool that scans for any vulnerabilities that malicious hackers could use to gain access.





# Code signing

Code signing is an operation where a software developer or distributor digitally signs the file being sent out to assure users that they are receiving software that does what the creator says it will do. The signature acts as proof that the code has not been tampered with or modified from its original form.

## Avtec's code signing process

At Avtec, we sign everything we can with a digital certificate to confirm the integrity and the authenticity of our files.

All Scout installers are digitally signed by Avtec using a code signing certificate. Additionally, the database checker is digitally signed to avoid false positives from anti-viruses.

Providing digitally signed files provides assurance that the files are from an authentic source and not modified in transit. The digital signatures are applied to executable files, installers and libraries.







# Third-party security audits

A security audit conducted by a qualified and impartial third-party source provides Avtec – and you – with an external view into the operation of our Scout console. It ultimately proves that the system is secure and functioning properly. These evaluation efforts are designed to provide us and customers with the evidence needed for compliance to user requirements, development standards and regulatory mandates.

## Avtec's third-party security audit process

Once per year, usually during the fourth quarter, Avtec employs a qualified, impartial company to conduct a compliance audit to verify the Scout console's security posture. The verifier's audits are performed using industry standard tools and test practices.

Any items discovered in the compliance audit are added to our internal security roadmap to be addressed.

For reference, we've provided an excerpt from the results summary from our recent audit:

- "All STIGs assessed were found to be compliant and only contained exceptions where absolutely required for system operation.
- No critical or 'high' findings when scanning patch compliance with Nessus.
- Based on the testing performed, [we] found the system to be configured to provide as small a potential attack footprint as possible while still maintaining proper functionality. There were very few findings overall, and no high-level findings."







To learn more, visit:  
[www.motorolasolutions.com/AvtecScout](http://www.motorolasolutions.com/AvtecScout)



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. [motorolasolutions.com](http://motorolasolutions.com)

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2025 Motorola Solutions, Inc. All rights reserved. 09-2025 [BG03]

