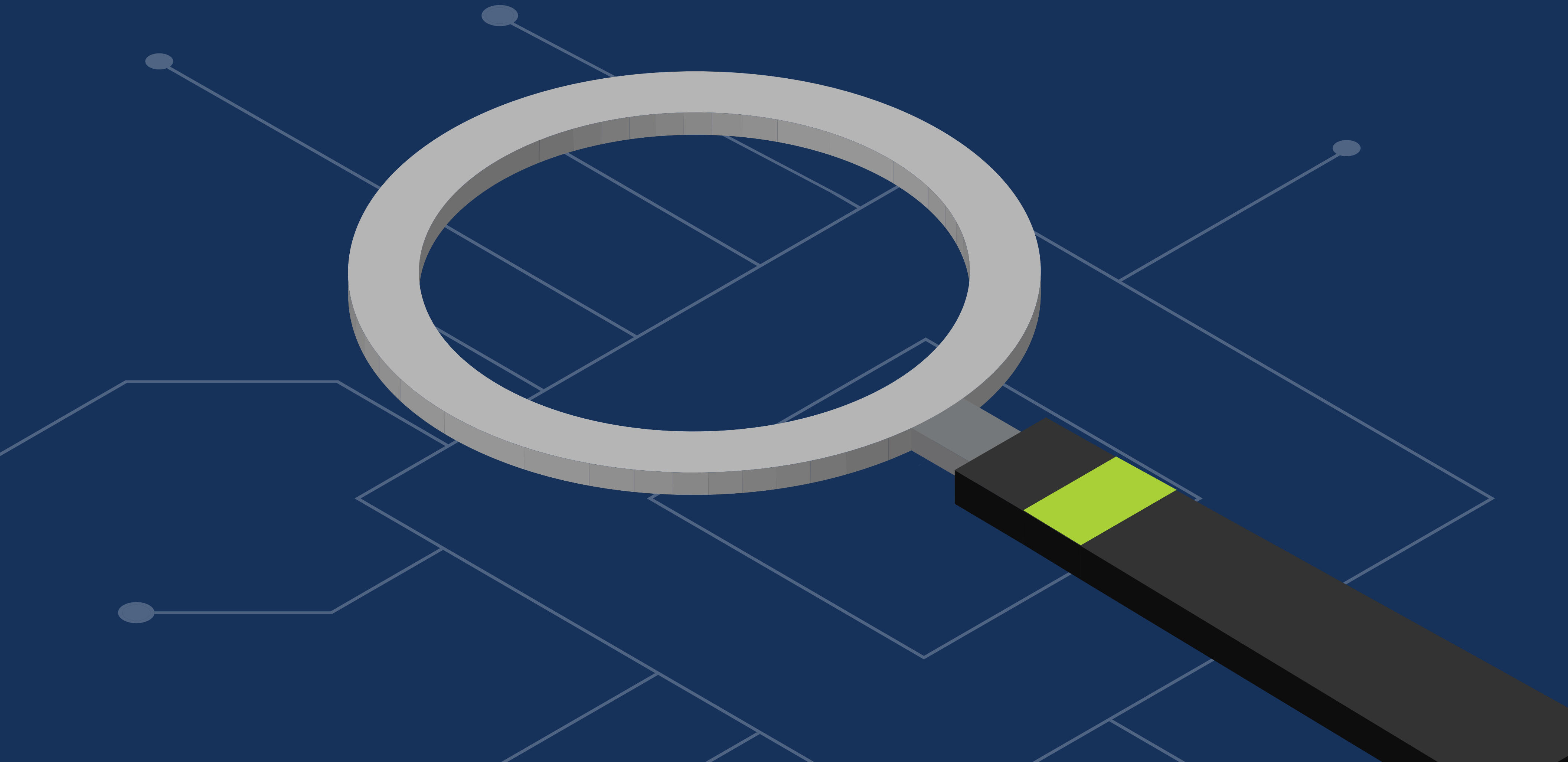
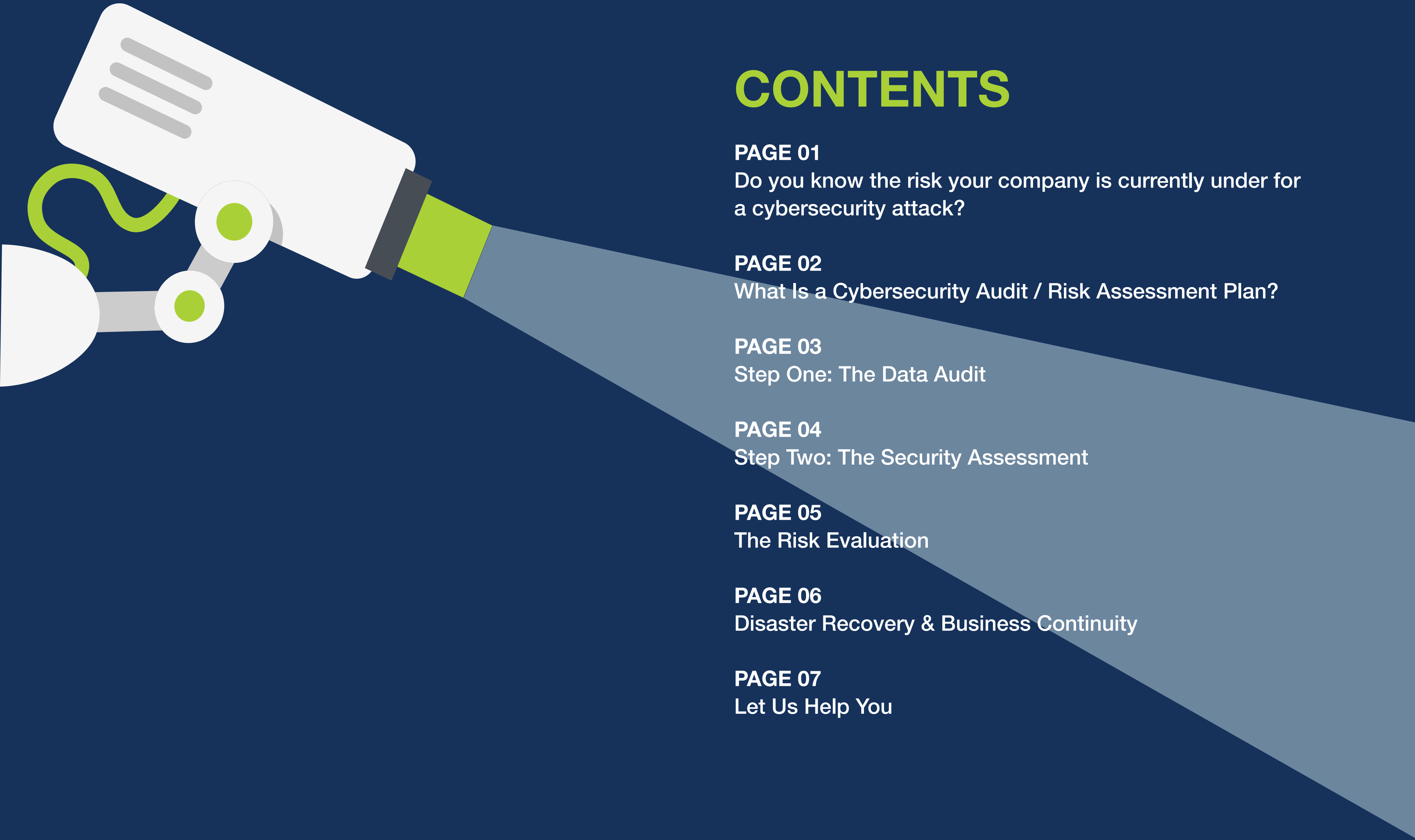
Building a

Cybersecurity Risk Assessment Plan

ARISTA
Edge Threat Management





CONTENTS

Do you know the risk your company is currently under for a cybersecurity attack?

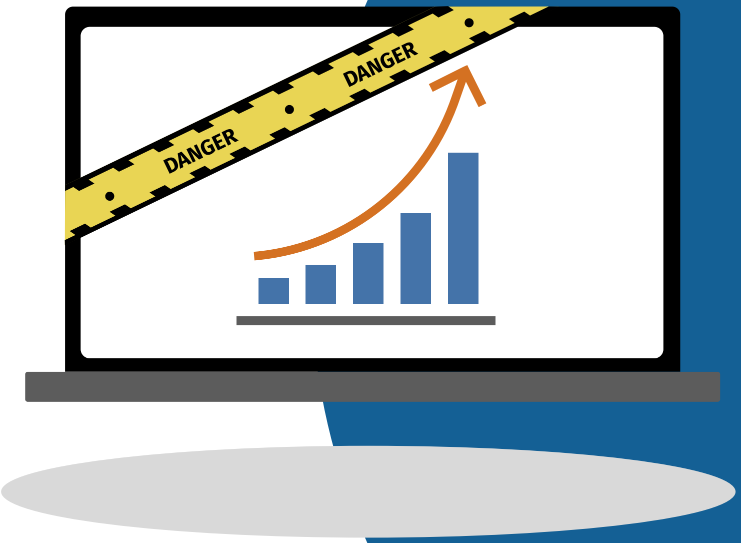
Organizations have learned to always be prepared for a cyberattack – and rightly so.

> Gartner's 7 Top Trends in Cybersecurity for 2022 predicts that by 2025, **45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.**

Of course, it's not just big companies that are seen as attractive targets. Small- and medium- sized businesses also store valuable data, and often are more attractive to hackers, thanks to potentially weaker security.

> According to Accenture's Cost of Cybercrime Study, **43% of cyber attacks are aimed at small businesses, but only 14% are prepared to defend themselves.**

Because smaller businesses often employ less exhaustive security measures than do their larger brethren, they are easier targets to infiltrate. In addition, SMBs now have a more widely distributed workforce, meaning potentially more unsecured points of access.



What Is a Cybersecurity Audit / Risk Assessment Plan?

What can organizations do today to be better prepared for an attack tomorrow?

When it comes to IT security, proactive protection depends on a two-part approach:

A CYBERSECURITY AUDIT

By conducting an exhaustive audit of your company's current data security activities in relation to potential threats, you can significantly minimize the risk of future security incidents as well as associated costs.

Identify all business information assets that could be targeted by cyberattacks

Categorize risks that could affect those assets

A RISK ASSESSMENT PLAN

Developing a risk assessment plan should include creating preventative measures and policies to address the identified vulnerabilities and protect your data. **Your risk assessment should:**

Drive a corporate mindset that recognizes cybersecurity risks

Serve as a **roadmap for improving IT security**

Step One: The Data Audit

Your audit needs to dive deep into what data is stored by the company, the value of that data and the costs involved if that data gets stolen, damaged or destroyed.

THESE COSTS CAN CONSIST OF:

Revenues lost due to data being inaccessible

Losses due to customer churn after discovering the breach

Legal costs that may be incurred while defending against potential lawsuits

Costs of the public relations efforts necessary to restore damages to your reputation

WHILE PREPARING THE DATA AUDIT, ASK THESE QUESTIONS:

What data is being collected?

Where and how is this data stored?

How long does the data need to be stored?

How is the data currently documented and protected?

Which of this data is most likely to be targeted?

What data, if stolen, would cause the most harm financially, legally or reputationally?

Your company's compliance with government or industry entities regarding data privacy and protection should also be addressed. **Depending on your customers and industry verticals, you may need to follow guidelines for HIPAA, PCI-DSS, and the Sarbanes-Oxley Act (SOX).**

Step Two: The Security Assessment

Conduct a complete assessment of the current state of your data security. This assessment should examine your security preparedness, check for vulnerabilities in your IT systems and processes, and include the following tasks:

HARDWARE ASSESSMENT

Complete a detailed examination of the company's hardware infrastructure:

Network and data storage capabilities

Age and condition of key hardware

Suitability of current hardware for future needs

ACCESS CONTROL ASSESSMENT

Evaluate how your company data is accessed:

Who has access to what data

What authentication methods are used Current access policies

How is the data currently documented and protected?

VULNERABILITY ASSESSMENT

Evaluate what parts of your company's IT infrastructure are most vulnerable to attack, and zero in on potential weaknesses in:

Computer systems

Network infrastructure

Software and applications

Any vendors or partners you use should be subjected to the same scrutiny to effectively mitigate risk.

The Risk Evaluation

Consider all possible threats to your company's data and systems, then prioritize them in order of most likely and most potential harm.

IS YOUR COMPANY DATA OF INTEREST OR VULNERABLE TO ANY OF THE FOLLOWING?

Competitors

Criminals

Disgruntled former or current employees Foreign governments

Cyberterrorists

WHAT DO POTENTIAL ATTACKERS WANT?

To steal customer data, intellectual property or business secrets

To ruin the company's reputation or disrupt its business activities

To receive a ransom for locking you out of systems or encrypting your data

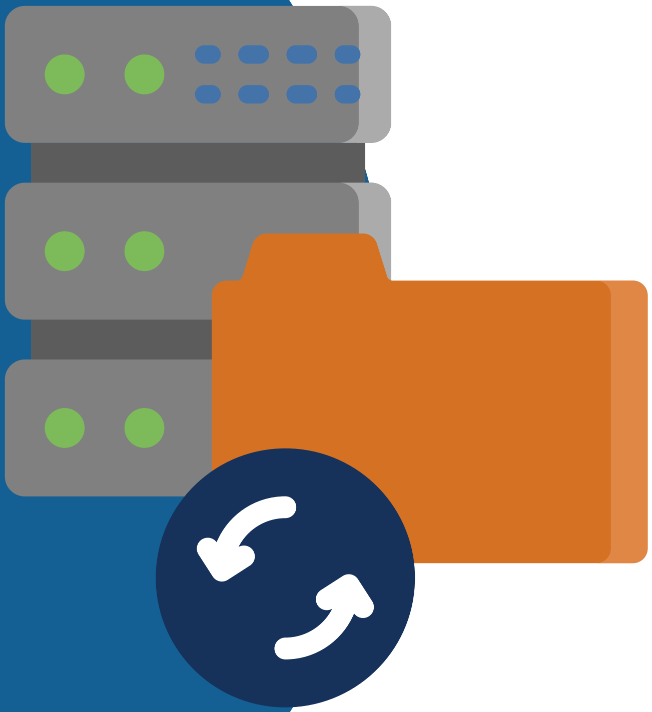
WHICH OF THE FOLLOWING ACTIONS WILL ATTACKERS BE LIKELY TO PURSUE?

A brute-force distributed denial-of-service attack

Phishing tactics or stolen credentials

Gain access via a compromised third party

By identifying all potential threats and predicting their moves, you can prioritize your security actions and be proactive in your defense.



Disaster Recovery & Business Continuity

As part of your cybersecurity risk assessment plan, you also need to develop a disaster recovery plan for your data and IT assets. This plan should include explicit instructions for:

IS YOUR COMPANY DATA OF INTEREST OR VULNERABLE TO ANY OF THE FOLLOWING?

Identifying and stopping ongoing cyberattacks

Bringing compromised systems back online as quickly as possible

Recovering lost or damaged data

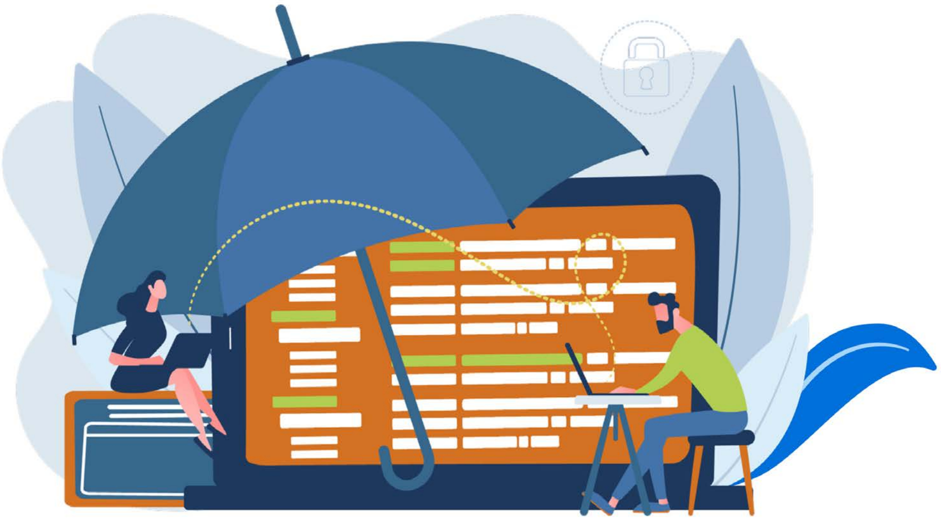
Restoring any damaged apps or systems

The goal of any disaster recovery plan is to return the organization to normal operating status as quickly as possible. By identifying various cyber risks, you can better construct a disaster recovery plan to address the effects of those potential attacks.

Finding the right risk mitigation partners can help you ensure business continuity by providing operational protection. Off-site servers and cloud data backups can help you regain access to your data and restore business activity promptly in the case of a disaster.

Let Us Help You

Arista provides a suite of solutions and apps designed to help you improve security and respond swiftly in the face of an incident.



After you've assessed your security risks, you can build your cybersecurity incident response plan that utilizes Arista's Edge Threat Management:

✓ **NG FIREWALL**
A Comprehensive Network Security Platform

✓ **ETM DASHBOARD**
A Cloud-Based Centralized Management Platform

✓ **MICRO EDGE**
A Lightweight Network-Edge Device for Branch Office Connectivity

Get Arista on your team!

Book your free demo now or contact us today for a free consultation

Edge Threat Management

edge.arista.com

Arista Networks Inc.
Santa Clara—Corporate Headquarters
5453 Great America Parkway
Santa Clara, CA 95054

Phone: +1-866-233-2296
Email: edge.sales@arista.com