MAINSTREAM TECHNOLOGIES

Cybersecurity Services

Table of Contents

Why Use Mainstream Cybersecurity? 3

Cybersecurity Services 4

Layered Cybersecurity 5

Cybersecurity Roadmap 6

Workforce Awareness Training 7

Risk Assessment 9

Vulnerability Assessment 10

Incident & Event Monitoring 11

Managed Compliance 12

HIPAA Compliance 13

How Governance Works 14

Vulnerability Management 15

Integrity Management 16

A La Carte Solutions 17

Working From Home Checklist 18

Why Use Mainstream Cybersecurity?

Organizations are faced with the growing need to secure their systems, their data, and their intellectual property.   Whether the driving force is meeting compliance requirements or rising cybersecurity demands, the expertise required to meet all of these obligations is overwhelming.

Mainstream Technologies' cybersecurity practice is designed to address a client's unique needs by targeting and addressing their most pressing needs first.

There are three fundamental components of our practice; NIST 800 standards, a Layered Cybersecurity Design Methodology, and an Agile approach to service delivery.

NIST

Best practices as defined by the **National Institute of Standards and Technology**

Layered Cybersecurity overlaps tools, people, and processes yielding the best defense.

A **custom agile approach** of assess, prioritize, deploy, evaluate, repeat keeps everything safe.

Security and compliance via: Identify, Protect, Detect, Respond, and Recover.

Achieve Compliance including HIPAA, PCI, along with many others.

Disaster Recovery, Incident Response Planning, and Consulting

Cybersecurity Services

Since 2010, Mainstream Technologies has been a certified provider. Put our experience as both a practitioner and a provider to help you navigate today's cyber risk.

Cybersecurity Roadmap

Identify your assets and relevant threats that put your organization at risk.

Workforce Awareness Training

Give your biggest security risk the training they need today.

Risk Assessment

Something something goes here

Vulnerability Assessment

Identify, quantify, and prioritizie the vulnerabilities in your system

Fully Managed Cybersecurity

Manage and report on all activities to assure your systems are protected.

Managed Compliance

Take steps now to improve your readiness.

Vulnerability Management

Respond quickly to reduce exposure, recovery time, costs and reputation.

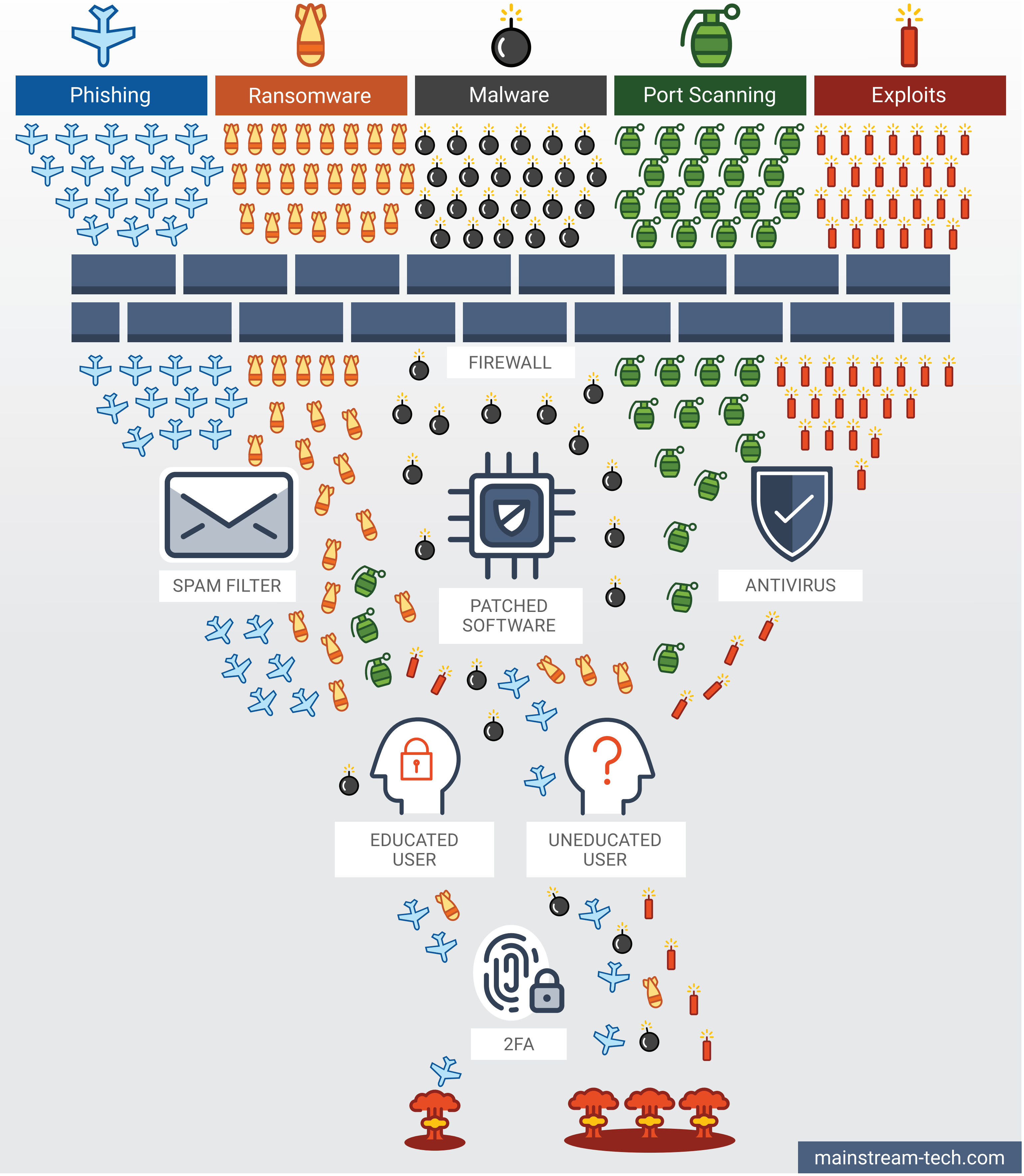
Integerity Monitoring

Automated threat intelligence and monitoring.

A La Carte Solutions

Select from a menu of services that fit your unique needs.

LAYERED CYBERSECURITY



mainstream-tech.com

Cybersecurity Roadmap

A Guide to Protecting Your Information

1. **Identify** Understand your assets and their role in your business. Identify any potential risks or threats to those assets

2. **Protect** Implement policies, procedures and tools to protect your assets.

3. **Detect** Tools and process to monitor your environment and raise alerts when potential/possible attacks are suspected.

4. **Respond** Develop an incident response plan before one occurs to mitigate negative effects while also performing forensics to learn more.

5. **Recover** Develop a recovery plan before an incident occurs.

Workforce Awareness Training

Phishing Attacks

Lower your company's risk of falling victim to a phishing attack.

The ultimate result of security training is an employee who is both aware of the danger posed by malware and actively able to avoid such cyberthreats.

The most effective means of instilling good cybersecurity habits is through a combination of education and training.

Our Workforce Education program provides each of your employees with a baseline knowledge of today's malware threats, and builds on that through formalized training sessions and testing emails.

Mainstream Technologies manages the entire process, and provide status updates and testing insights via your company's customized online portal.

Employee Security Training

- On-Boarding training for all new employees
- Bimonthly training to keep all users current on best practices
- Point-of-failure training auto-enrollment

On-Boarding

- Provision customized account and portal
- Synchronized active users
- Initial training campaign for current employees
- Training on accessing and using portal

Compliance

- Department specific campaigns
- Additional training campaigns
- USB Drive testing
- Custom email templates

Continuous Phishing Campaigns

- Keeps email security front of mind for users
- Random message delivery
- Over 2,000 templates available

Reporting & Dashboards

- Track security trends – See the improvement
- View status of training campaigns
- Reporting at company and user levels

Sample Report

Phishing Security Tests – Last 6 Months
Phish-Prone %
Clicks
Replies
Attachment Open
Macro Enabled
Data Entered
Exploited
Phish-Prone %
Industry Average

Workforce Awareness Training

Phishing Attacks

Awareness is the First Step

Your team must be an active part of your cybersecurity strategy.

The Big Phish

An industry survey of **1,300 IT executives** identified phishing attacks as their biggest current cybersecurity threat.

Small Business Beware

43% of cyber-attacks are aimed at small businesses.

Inside Job

62% of professionals said they believe the largest insider threat comes from well-meaning but negligent end users.

SPAMalot

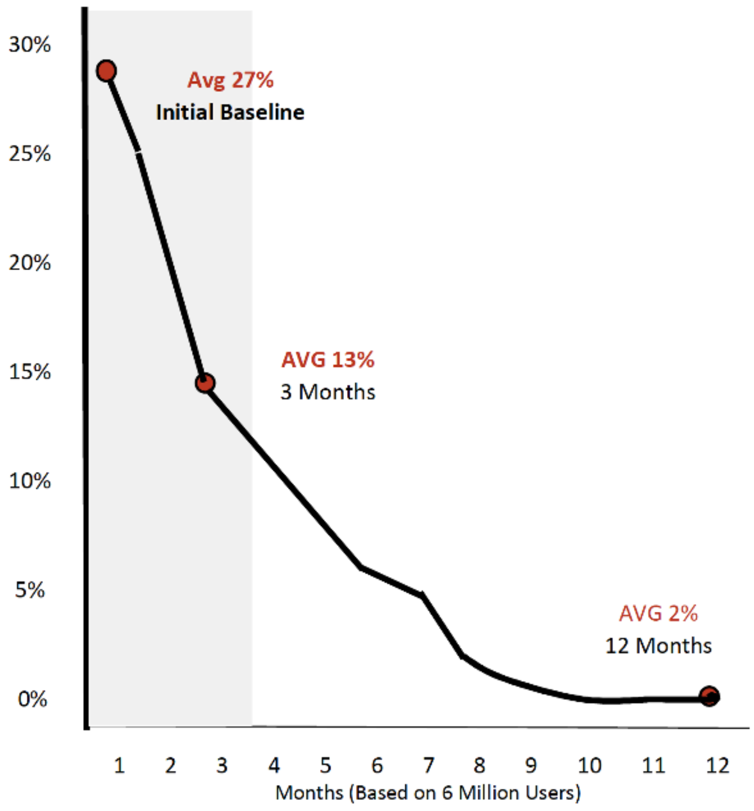
91% of successful cyber-attacks begin with a spear phishing email.

Costs Are Up

The Global Cost of a Data Breach Is Up in 2018 "In this year's study, the average cost of a data breach per compromised record was $148, and it took organizations 196 days, on average, to detect a breach."

Your staff is your biggest security risk. Protect your systems and data by training your staff now.

Without consistent training, roughly 27% of a company's employees are likely to click on any given phishing email. **Consistent training and awareness can lower that risk to less than 5%.**



Sources:

1 https://www.techrepublic.com/article/why-91-of-it-and-security-pros-fear-insider-threats/

2 https://www.cyberark.com/resource/cyberark-global-advanced-threat-landscape-report-2018/

3 https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html

4 https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email securityintelligence.com/ponemon-cost-of-a-data-breach-2018/ 30% 25% 20% 15% 10% 5% 0% 1 2 3 4 5 6 7 8 9 10 11 12

Months (Based on 6 Million Users)

Avg 27% Initial Baseline

Risk Assessment

Bad Things Can Happen

Have your security controls ever been verified?
How can you be certain they are effective?

Unattended gaps in your security and compliance practices leave you exposed. Mainstream Technologies' Risk Assessment services measures your current security posture using recognized industry best practices and regulatory compliance requirements and delivers a roadmap of how to address the security gaps discovered during the assessment.

- ✓ **Assess your existing security position**
- ✓ **Document security controls**
- ✓ **Identify security gaps in your architecture and controls**
- ✓ **Inform decisions to improve and align IT risk management with business goals**
- ✓ **Meet regulatory compliance obligations**
- ✓ **Prepare for cybersecurity incidents without disrupting operations**

Vulnerability Assessment

This is Where You Are Weak

Attackers are testing your security daily. Are you as focused on your security as they are?

Technology is dynamic. So is risk. Security gaps are continually evolving and shifting. The challenge is finding these security gaps before attackers can exploit them.

A vulnerability assessment is the process of identifying, quantifying, and prioritizing the vulnerabilities in a system. Organizations that use them know they are at risk and want help identifying and prioritizing them.

Visibility Translates Into Action

You can't manage what you don't know. Knowing where your security gaps are and what is at risk gives you the insights you need to create a remediation plan.

The Assessment is Critical for Managing Vulnerabilities on an Ongoing Basis

An assessment is a first step. Since technology, processes and policies change, assessments should be scheduled on a regular basis.

Comprehensive

All assets both internal and external

Timely

One time or scheduled

Identify and Prioritize Vulnerabilities

Business critical or sensitive

Executive Summary

Detailed Reporting with Recommendations

Compliant

Meet security best practices and frequency regulatory requirements

Incident & Event Monitoring

Reducing Risk and Liability around Cyber Attacks

Is Your Business Safe from Cyber Attacks?

Do you think your business is too small to be targeted for cyber-attacks? Think again. It's not a matter of if, it's a matter of when; and 60% of all SMBs face bankruptcy within 6 months of a severe cyber breach.

Keep Your Data and Your Business Secure with Mainstream Technologies

We can dramatically reduce your chance of suffering a severe breach while meeting your regulatory audit and reporting requirements.

Our solution provides advanced threat intelligence and the same level of security enjoyed by the largest companies in the world, all at a low monthly cost. Your data is protected in real-time and meets your regulatory, audit and reporting requirements including specific compliance reports you'll need to pass HIPAA, PCI, FISMA and other audits.

Security Made Easy

- **More than a tool**, a commitment to best practices.
- **24x7 SOC correlation and analysis** of events removes noise and reacts fast.
- **Alerts of suspicious activity are triaged** removing false positives.
- Getting a **SIEM** plus a **SOC** for less than the cost of a security analyst.
- Crucial **detect** service complements your **identify & protect** activities bridging your **response** protocol.

24x7 Managed Network Security

Managed security for your entire network using trained experts & cutting-edge technology

Comprehensive Forensics

Gain the capability to conduct detailed forensic investigations helping remediate breaches

Regulatory Compliance

Meet your compliance & audit challenges for HIPAA, PCI and other regulations

Secure Your Business

Potentially lower the cost of cyber insurance while minimizing a successful attack

Managed Compliance

Automate Controls and Monitoring

Navigating the hierarchy of government regulations, industry standards, and audit methodologies is challenging.

Mainstream Can Help

Meeting compliance requirements is about aligning your people, processes, and technology so your operations are both secure and effective regardless of the underlying framework. Partnering with Mainstream Technologies helps you automate controls and controls monitoring.

- Monitor transactions, controls, and systems
- Establish consistency to minimize human subjectivity
- Generate timely reporting to assist ongoing management

Policy Compliance

Assess security configurations of IT systems throughout your network.

Assess and Address

Automation helps identify issues, prioritize them, and track remediation.

Policy Creation

You can quickly create policies using industry-recommended best practices.

Reporting

Customizable reporting documents progress meeting required control objectives.

HIPAA Compliance

Meet Your HIPAA Obligations and Secure Data

$111,000,000

Since inception there have been over 223,000 documented HIPAA complaints and over $111MM civil money penalties levied.

Don’t Just Be Compliant, Be Secure

Mainstream Technologies offers annual and periodic assessment services to help you meet HIPAA obligations and secure data in your possession. We provide timely intelligence to identify weaknesses and help you prioritize your workload.

We help you be more secure while meeting your compliance requirements. Periodic assessments help you respond to threats faster and reduce your compliance risk.

Policy Review

Verify that your policies are aligned with HIPAA regulations

Physical Security Review

Verify that the physical security of your organization complies with regulations

Vulnerability Assessment

Scan your technology infrastructure for security gaps

Infrastructure Assessment

Ensure that High Trust Standards and are implemented consistently throughout

Consulting

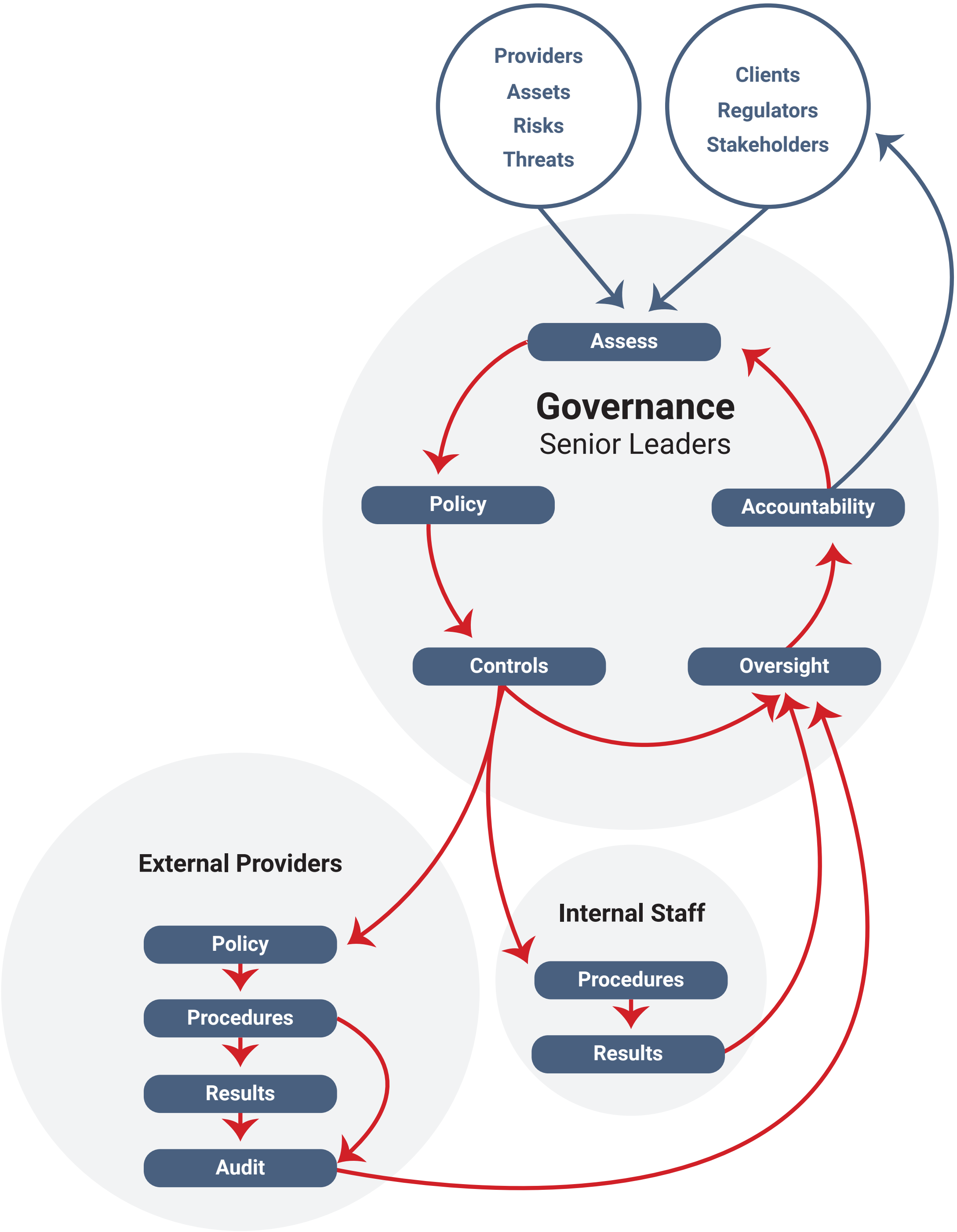
Advise on best practices to improve your readiness

Remediation

Make the adjustments to address detected gaps

How Governance Works

Establish the Foundation of High Performance



Vulnerability Management

Identify and Address Software Flaws

One in three breaches are caused by unpatched software vulnerabilities!

When software flaws are left open, they leave an organization at risk. You rely on software to operate. New vulnerabilities are constantly being uncovered. Software vendors respond by publishing updates but it's up to you to install them.

Mainstream Technologies' Vulnerability Management service identifies these software flaws so they can be addressed. Your biggest risks are the ones you are unaware of; don't let these issues overwhelm you. Let Mainstream help identify, prioritize and determine where to start.

Mainstream is flexible, we can arm your team with the information they need to resolve issues, or we can do it all for you.

Network Asset Profile

Discover, document your network assets so nothing falls through the cracks

360 Protection

Assets, regardless of location are identified and protected

Threat Intelligence

Stay up to date on the latest advisories and software vulnerabilities

Flexible Management

We can triage for your or turn everything over to your team to take action

Continuous Scanning & Alerts

Identify, assess and remediate all software flaws in your enterprise

Reporting

Know where you stand from the initial alert to the final completion with a full history

Integrity Monitoring

A tool to give you visibility when changes are made

The success of an attacker depends on making changes to your systems without your knowledge

Change is a constant. Systems and data are dynamic. Constantly being tweaked or updated. The purpose of tool so you will know when updates are made to sensitive information, system access rights, and configurations. Visibility into blind spots (dark corners) Attackers rely on your blind spots to establish a presence, steal information, and take control of your resources.

Mainstream shines a light so you can have visibility into the blind spots of your systems and data. You have full control to take the steps you need to preserve system/data integrity.

We use industry leading tools configured to give you visibility to system changes so you can address critical security and compliance needs and reduce the risk of a data breach or compromise.

Track all the Changes to your System

- Changes to Database Configurations
- Changes and Access to Sensitive Files
- Changes to System Access Rights
- Changes to System Configurations

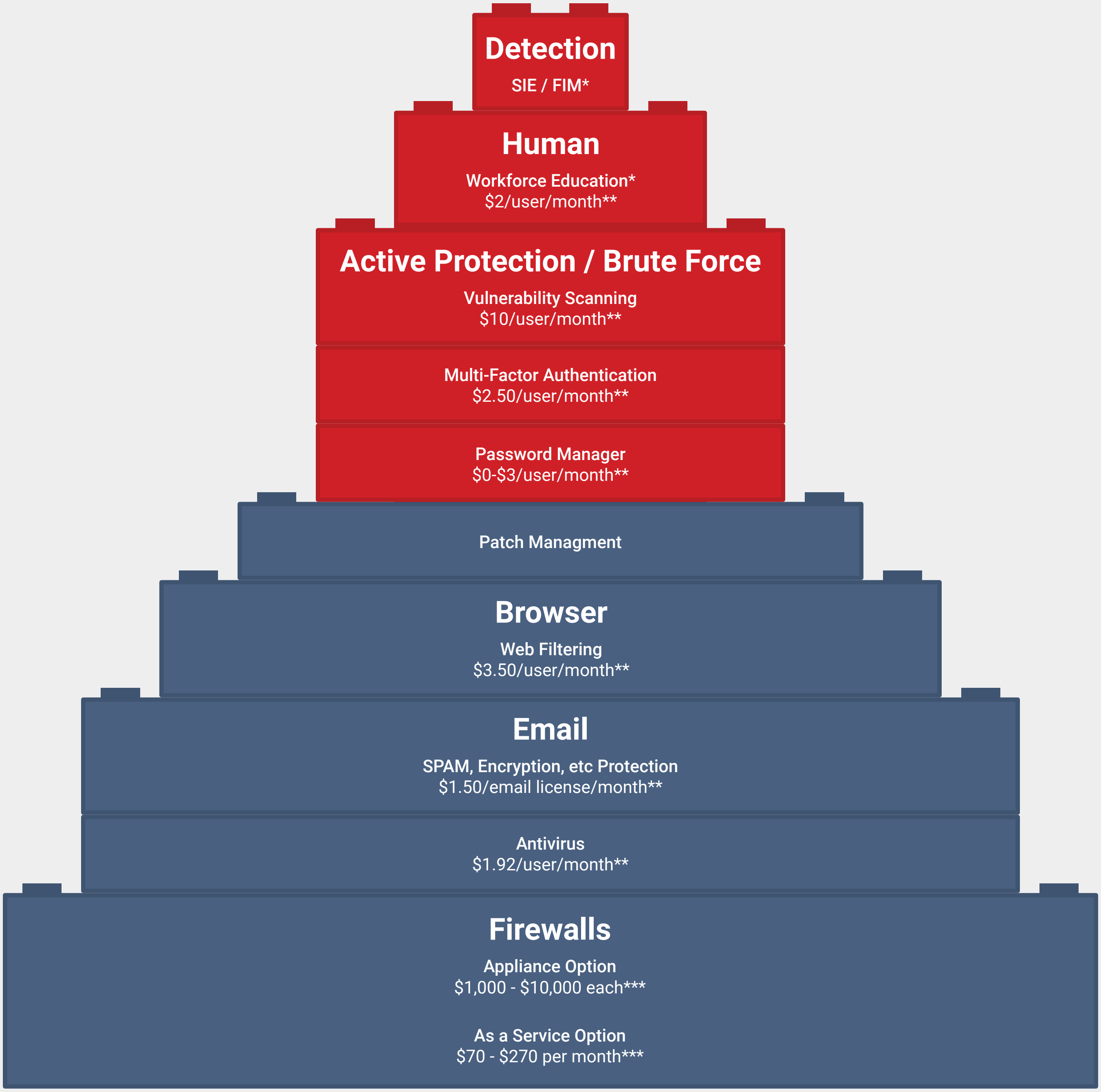
Integrity Monitoring Service

Mainstream Technologies provides continuous IT monitoring, actionable intelligence, and regulatory compliance support.

- 7x24 monitoring
- Real-time alerts
- Reports required for compliance purposes including PCI-DSS and HIPAA

BLOCK BY BLOCK

A LAYERED APPROACH TO CYBERSECURITY



Detection
SIE / FIM*

Human
Workforce Education*
$2/user/month**

Active Protection / Brute Force
Vulnerability Scanning
$10/user/month**

Multi-Factor Authentication
$2.50/user/month**

Password Manager
$0-$3/user/month**

Patch Managment

Browser
Web Filtering
$3.50/user/month**

Email
SPAM, Encryption, etc Protection
$1.50/email license/month**

Antivirus
$1.92/user/month**

Firewalls
Appliance Option
$1,000 - $10,000 each***

As a Service Option
$70 - $270 per month***

🟥 **Managed Security Services**
Detection, Workforce Education, and Active Protection

🟦 **Managed IT Services**
Patch Management, Browser, Email, Antivirus, Firewalls

* Must be accessed prior to estimate
** All prices quoted are estimates
*** Based on user count from 5 - 500 users.

MAINSTREAM
TECHNOLOGIES

Working From Home Checklist

A Roadmap for Remote Success

In today's world, working from home is the new norm.

The challenge leaders face is making sure it's done safely and securely.

Connectivity

- □ **VOIP** (handset, softphone, company #)
- □ **Mobile phones** (convenient, individual #)
- □ **Collaboration tools** (maintain teamwork, facilitate workflow and connect staff)

Hardware / Software

- □ **Computing device(s)**
- □ **Accessories** (monitors, printer/scanner)
- □ **Access to organizational infrastructure** (services/resources, VPN, licensing)

Security

- □ **Endpoint Security**
- □ **Patching** (routine)
- □ **Anti-malware**
- □ **Policy** (rules and expectations about behavior and usage)

Home Network Security

- □ **VPN**
- □ **Firewall**
- □ **Wireless Security**
- □ **Eliminate default settings**
- □ **Segmentation**
- □ **Authentication** (Unique IDs, Strong passwords, Multi-factor)
- □ **Monitoring**
- □ **Tool and environment familiarity** (reduce risk from phishing/spoofing attacks)
- □ **Security Awareness Training** (recognize threats and understand expectations)