Microsoft Security Baseline

Computer Solutions East, Inc.

Business Technology Simplified

Presented By:
Computer Solutions East
info@computersolutionseast.com

481 Main Street, Suite 100, New Rochelle NY 10801.
(914)355-5800 |info@computersolutionseast.com

Agenda

- Overview of **Microsoft Security Baseline.**
- Why it is a must in today's World.
- Components comprising Security Solution.
- Part these components play in Securing You.
- Cost of Security Vs Cost of being hacked.

Why are we here?

Cyber-attack hackers threaten to share US police informant data

U.S. agencies hit by massive cyberattack

Hackers allegedly linked to Russia targeted govt. departments; users warned against using SolarWinds

ed that hackers had June. ▪ISTOCKPHOTO

erattack. have been working with our agency s regarding recently red activity on go- nt networks," a spo-

tities as they work to identify and mitigate any potential compromises."

IT company SolarWinds over the weekend admitted that hackers had exploited a backdoor in an up some of its software between March and

"We have been this attack was lik ducted by an outsid state and intended narrow, extremely t and manually exec tack, as opposed to system-wide attack," said.

The hacks are p wider campaign tha major cybersecurity reEye, which said its fences had been bre sophisticated attack

targets across the globe. "Victims have included government, consulting, technology, telecom and extractive entities in North America, Europe, Asia and

Cyber-attack disrupts cancer care across U.S.

High-tech radiation treatment machines knocked offline following software breach

Cyber Attack Vectors

96%

Email continues to be the most common vector at 96%

In 2020, the number of data breaches in the United States came in at a total of 1001 cases. Are you the NEXT!!

Microsoft Exchange Cyberattack: Hafnium Email Hack Timeline and Incident Details

Microsoft Exchange Server cyberattack timeline covering patches, vulnerabilities, IOCs, Cybereason, DearCry ransomware, HAFNIUM, Huntress, FireEye, Mandiant, Prometei botnet & more.

90%

Phishing accounts for more than 90% of successful attack

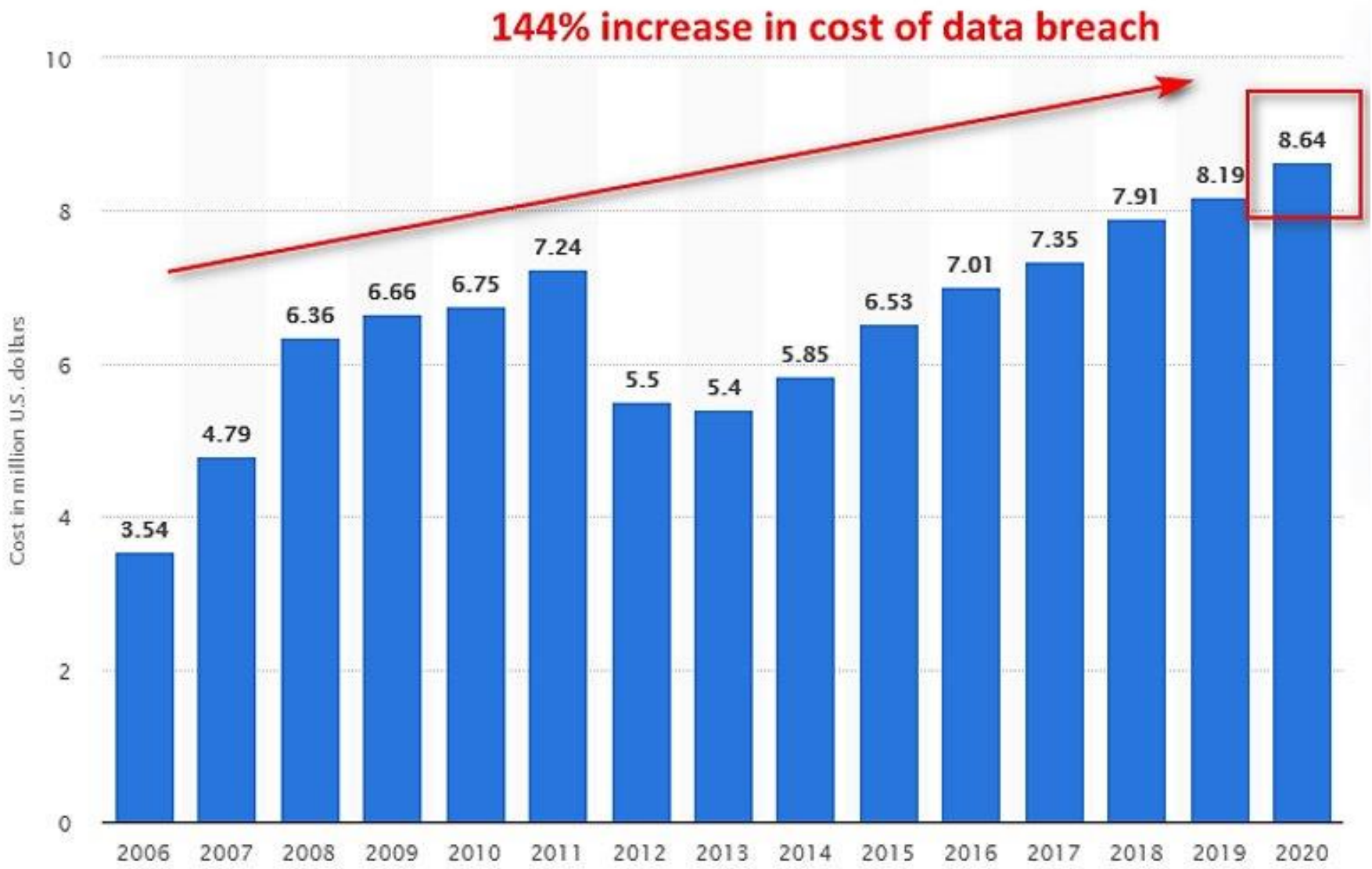
SOURCE: Advancing Cyber Risk Manage From Security to Resilience, FireEye and Marsh & McLennan Insights

At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software

Hackers rushed in as Microsoft raced to avert cyber-attack

2021 Microsoft Exchange Server data breach

Cost to business from Cyber Attacks



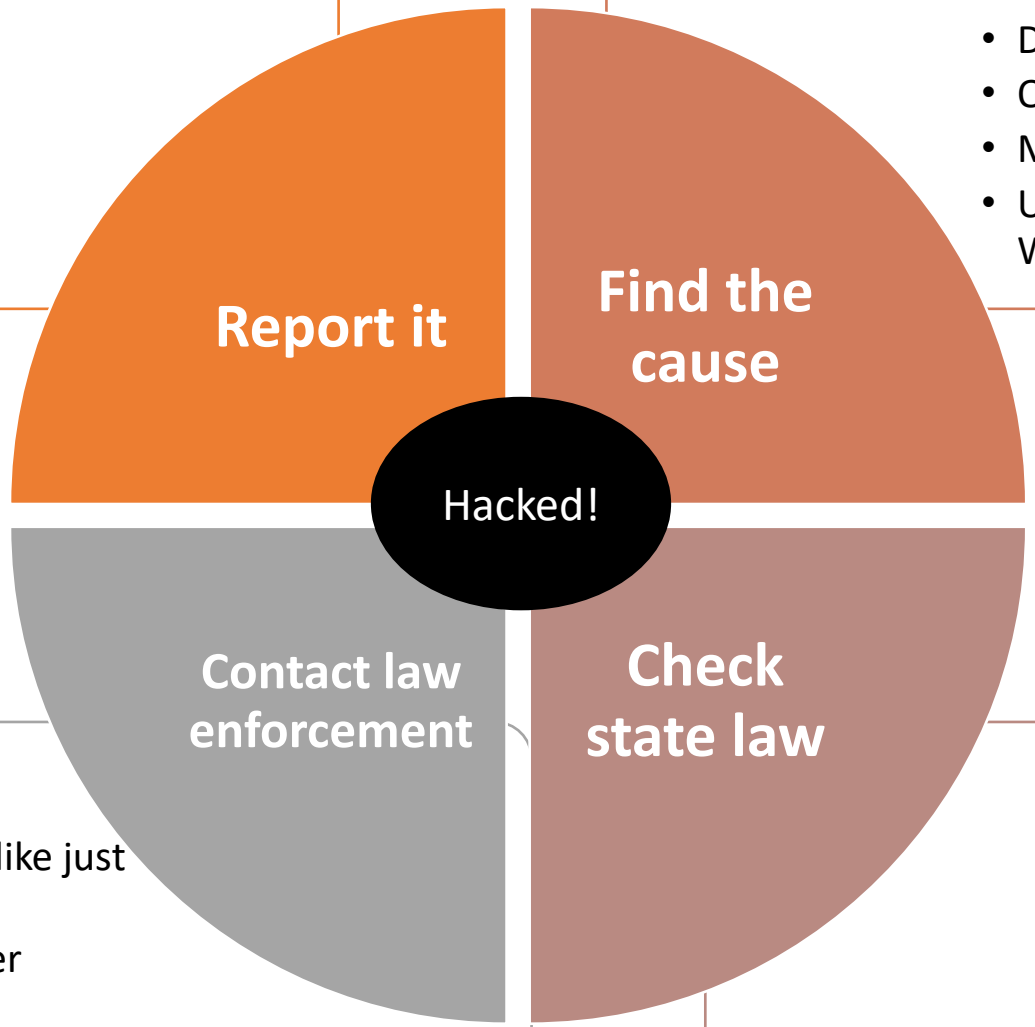
What to do if your business is hacked!

How much will it cost you to communicate to all your customers? Will they stay with you after this?

- A data breach has occurred
- The date it happened
- What kind of information has been compromised

How long will it take to figure out the breach and will it really be resolved without the right tools?

- Weak/stolen passwords
- Device loss/theft
- Out of date software and/or IT systems
- Malware (malicious software)
- Use of unsecured networks (like public WIFI)



How much time and distraction will this cost to your company?

- Getting the police involved might seem like just another drain on your time.
- maintaining your reputation after a cyber attack is vital.

How much time and distraction will this cost to your company?

- The length of time you're required to offer monitoring.
- File a notice with your attorney

Microsoft Intune

Multi Factor Authentication

Bring Your Own Device

Azure Information Protection

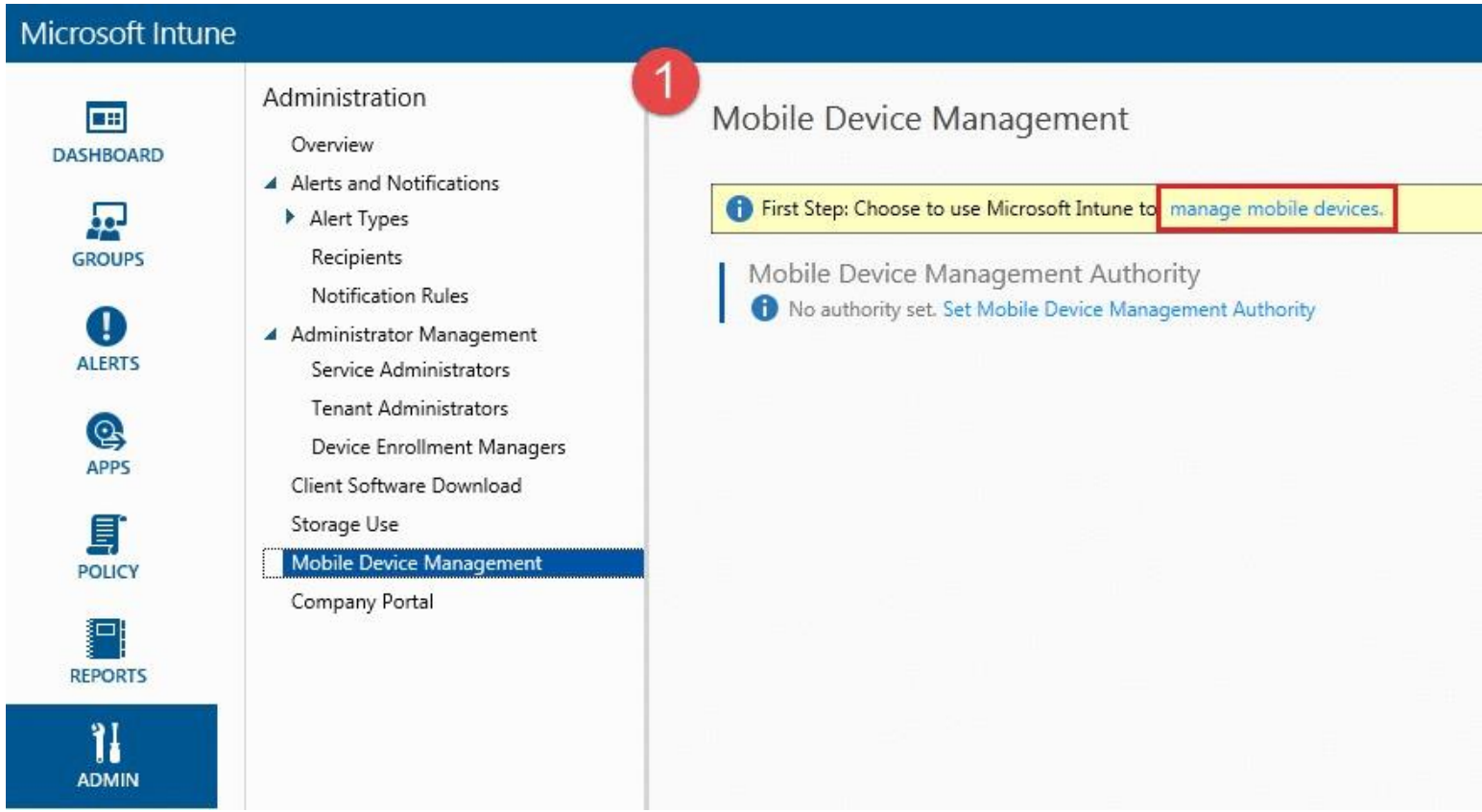
Advanced Threat Protection

Microsoft Security Baseline

SECURITY

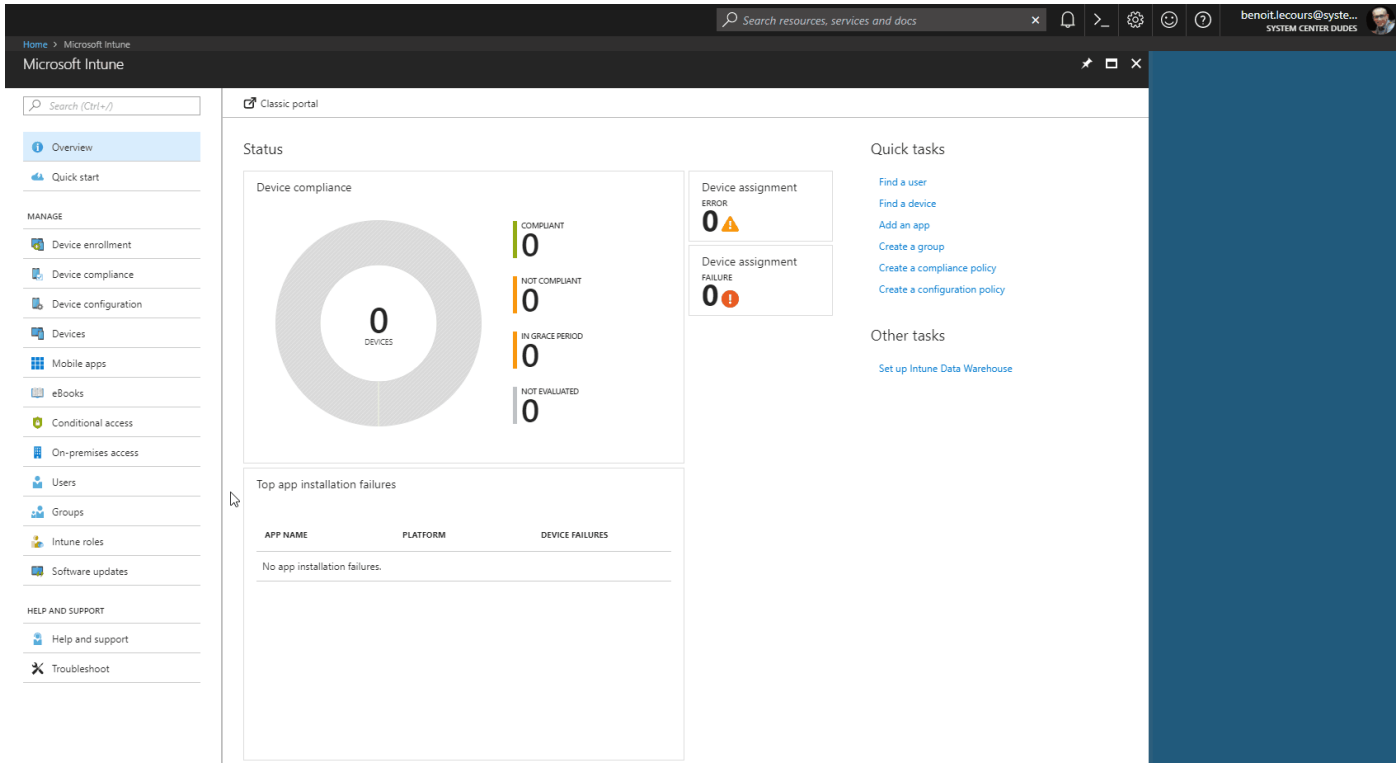
Stay protected with Microsoft Intune?

- **Mobile device management (MDM) and mobile application management (MAM).**
- **Control how your** organization's devices are used.
- Configure **specific policies to control applications**.
- **Being protected** and having the best user experience.
- **Protect data with or without device enrolment.**



Stay protected with Microsoft Intune?

- Choose to be **100% cloud with Intune.**
- **Set rules and configure settings** on personal and organization-owned devices.
- Deploy and **authenticate apps** on devices on-premises and mobile.
- **Protect your company information** by controlling the way users' access and share information.
- Be **sure devices and apps are compliant** with your security requirements.



Manage work data on mobile devices with Intune

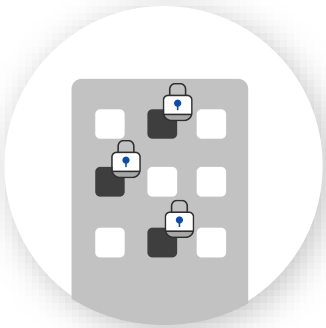
Mobile Device Management (MDM)

Conditional Access:
Manage access to company owned devices.

- Enroll devices for management
- Provision settings, certs, profiles
- Report & measure device compliance
- Remove corporate data from devices remotely

Mobile Application Management (MAM)

Conditional Access:
Manage which apps can be used to access work email or files on personal devices



- Publish mobile apps to users
- Configure and update apps
- Enforce that work data cannot be saved on personal apps
- Secure & remove corporate data within mobile apps

Device compliance - Noncompliant devices (preview)

The Noncompliant devices report provides data typically used by Helpdesk or admin roles to identify problems and help remediate issues.

Search (Ctrl+/)

Overview

Manage

Policies

Notifications

Locations

Monitor

Device compliance

Noncompliant devices (preview)

Devices without compliance po...

Setting compliance

Policy compliance

Audit logs

Windows health attestation rep...

Threat agent status

Setup

Compliance policy settings

Microsoft Defender ATP

Mobile Threat Defense

Partner device management

Help and support

Help and support

Refresh | Columns | Export

Search by device name, Azure AD device ID, email, user principal name, user display name, Az | Compliance status: All | OS: All | Ownership type: All

Showing 1 to 50 of 8,941 records

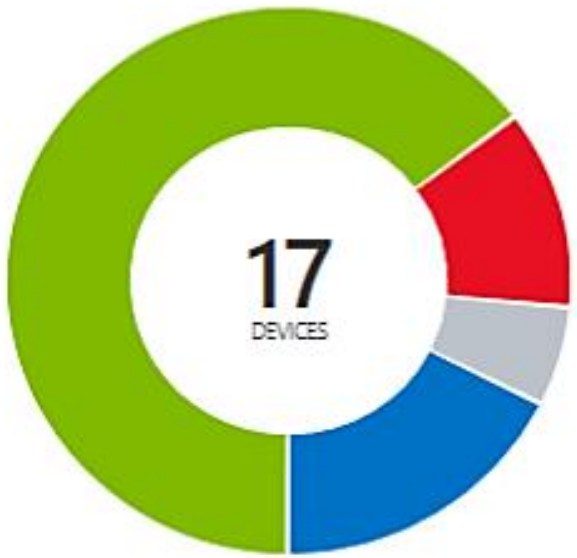
< Previous | Page 1 of 179 | Next >

Device name	User principal na...	Compliance status	OS	OS version	Ownership	Last check-in	Management ag...
Aaden's Macbook Pro	AadenMccarty@Conto...	Not evaluated	macOS	10.14.5 (18F132)	Company	11/3/2019, 3:12:56 PM	
Aaden's iPad	AadenHughes@Conto...	Not compliant	iOS	11.3.1	Company	11/4/2019, 7:46:49 AM	
Aaden's iPad	AadenWard@Contoso...	Not compliant	iOS	12.1.3	Company	11/3/2019, 8:03:29 PM	
Aaliyah's Macbook Pro	AaliyahSerrano@Cont...	Not compliant	macOS	10.14.5 (18F132)	Company	11/3/2019, 12:54:55 PM	
Aaliyah's Macbook Pro	AaliyahFriedman@Co...	Not compliant	macOS	10.14.5 (18F132)	Company	11/3/2019, 6:34:45 PM	
Aaliyah's Macbook Pro	AaliyahPatrick@Conto...	Not compliant	macOS	10.14.5 (18F132)	Personal	11/4/2019, 5:38:40 AM	MDM
Aaliyah's iPad	AaliyahGalvan@Conto...	Not compliant	iOS	11.3.3	Company	11/3/2019, 6:06:53 AM	
Aaliyah's iPad	AaliyahCase@Contoso...	Not compliant	iOS	11.2.1	Company	11/2/2019, 9:16:25 PM	
Aarav's Macbook Pro	AaravMccoy@Contos...	Not compliant	macOS	10.14.5 (18F132)	Personal	11/4/2019, 2:21:53 AM	MDM
Aarav's Macbook Pro	AaravWatts@Contoso....	Not evaluated	macOS	10.14.5 (18F132)	Company	11/3/2019, 12:38:24 AM	
Aarav's iPad	AaravBaldwin@Contos...	Not compliant	iOS	11.2.3	Company	11/3/2019, 2:18:46 AM	
Aarav's iPad	AaravCooper@Contos...	Not compliant	iOS	12.1.3	Company	11/4/2019, 7:10:50 AM	
Aarav's iPad	AaravLang@Contoso.c...	Not compliant	iOS	13.1.1	Company	11/3/2019, 3:27:58 AM	
Aarav's iPad	AaravKent@Contoso.c...	Not compliant	iOS	12.2.2	Company	11/3/2019, 6:53:34 PM	
Aarav's iPad	AaravHawkins@Conto...	Not compliant	iOS	13.3.1	Company	11/3/2019, 8:09:10 PM	
Abagail's Macbook Pro	AbagailSullivan@Cont...	Not compliant	macOS	10.14.5 (18F132)	Company	11/4/2019, 6:09:37 AM	
Abagail's Macbook Pro	AbagailCarlson@Cont...	Not evaluated	macOS	10.14.5 (18F132)	Personal	11/3/2019, 9:11:05 PM	MDM
Abbey's Macbook Pro	AbbeyGriffith@Contos...	Not compliant	macOS	10.14.5 (18F132)	Company	11/3/2019, 8:35:56 PM	MDM

Device compliance ...

Columns | Export

Report generated on: 3/23/2021, 8:37:14 PM



Compliant
11 devices

Not compliant
2 devices

In grace period
0 devices

Not evaluated
1 devices

Managed by ConfigMgr
3 devices

Total
17 devices

Compliance status: All

OS: 1 selected

Ownership: 2 selected

Generate again

Search by device name, Azure AD device ID, primary user email address, primary UPN, primary user display name, Azure AD user ID, IMEI, o

Showing 1 to 17 of 17 records

Device name	Primary UPN	Compliance status	OS	OS version
73-2919-09		Compliant	Windows	10.0.18363.592

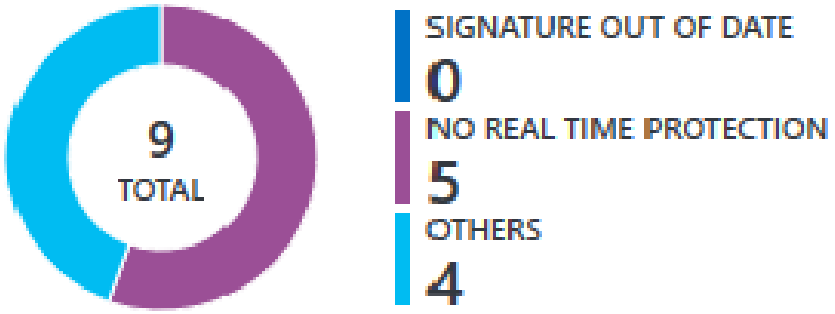
Columns

- [x] Primary UPN
- [x] Compliance status
- [x] OS
- [x] OS version
- [x] Ownership
- [x] Last check-in
- [ ] Compliance grace period expiration
- [ ] Device threat level
- [ ] Primary user email address
- [ ] Primary user display name
- [ ] Intune device ID
- [ ] Azure AD device ID
- [ ] Azure AD user ID
- [ ] IMEI
- [ ] Serial number
- [ ] Retire after
- [ ] Management agent

Apply | Reset filters

PROTECTION STATUS

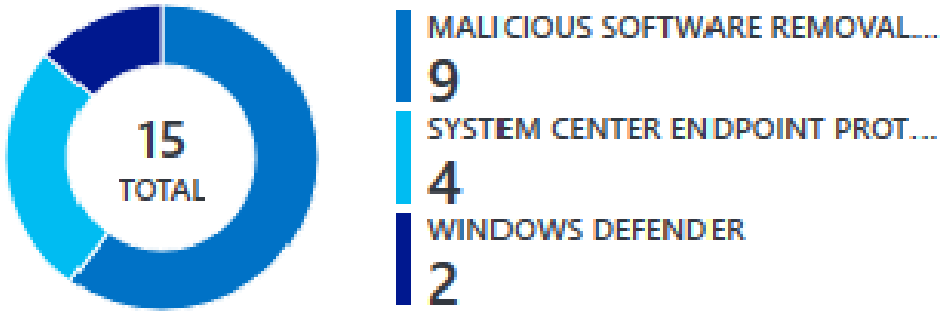
Computers with insufficient protection



PROTECTION STATUS	COMPUTERS
No real time protection	5
Not reporting	4

TYPE OF PROTECTION

Computers with antimalware protection



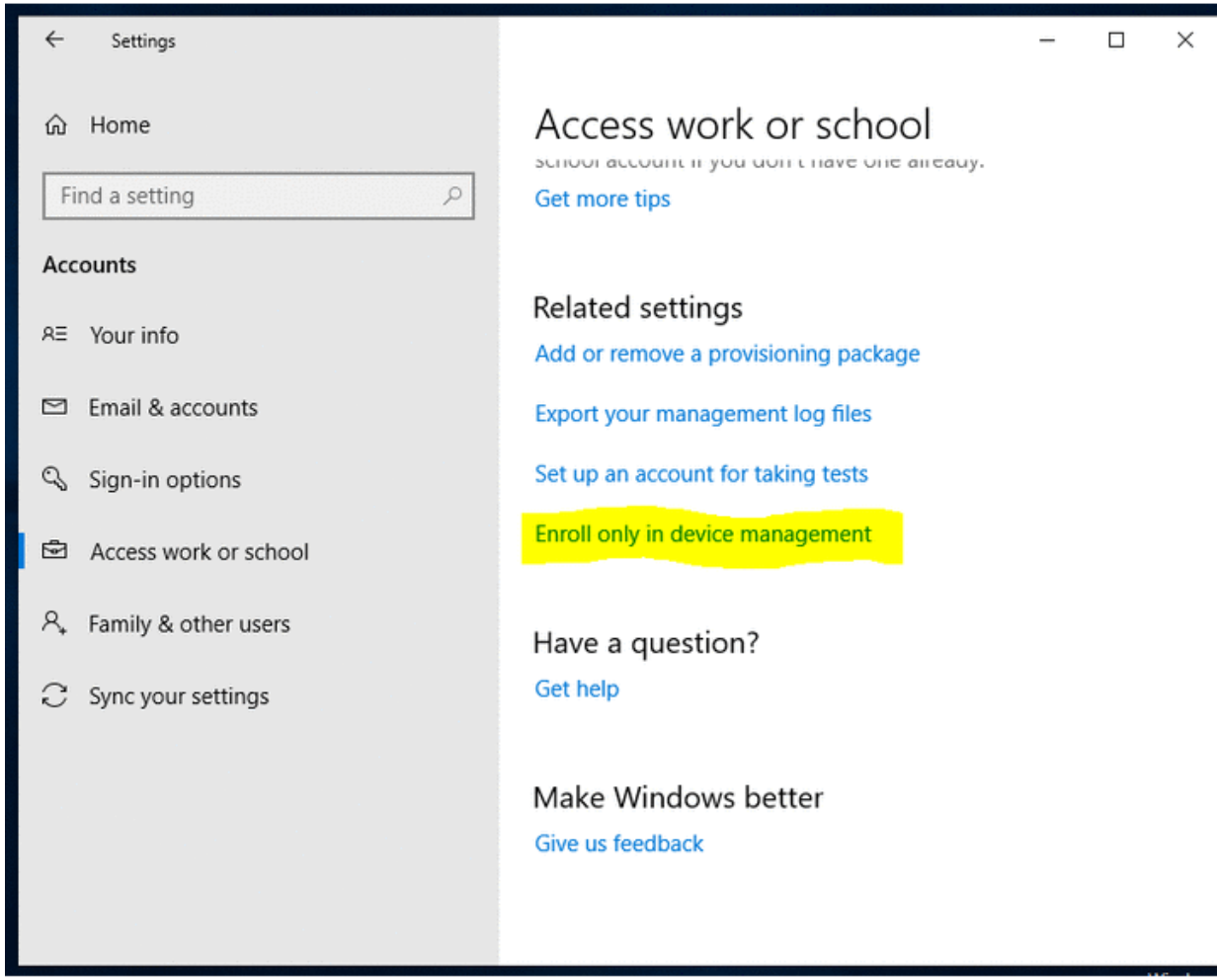
PROTECTION TYPE	COMPUTERS
Malicious Software Removal Tool	9
System Center Endpoint Protection	4
Windows Defender	2

The data found in this report is timely and shows the following details:

- If a device has real-time or network protection, as well as the state
- The status of Windows Defender
- If Tamper protection is enabled
- If the device is a virtual machine, or a physical device.
- Calls out the unhealthy device, the user name, and severity.

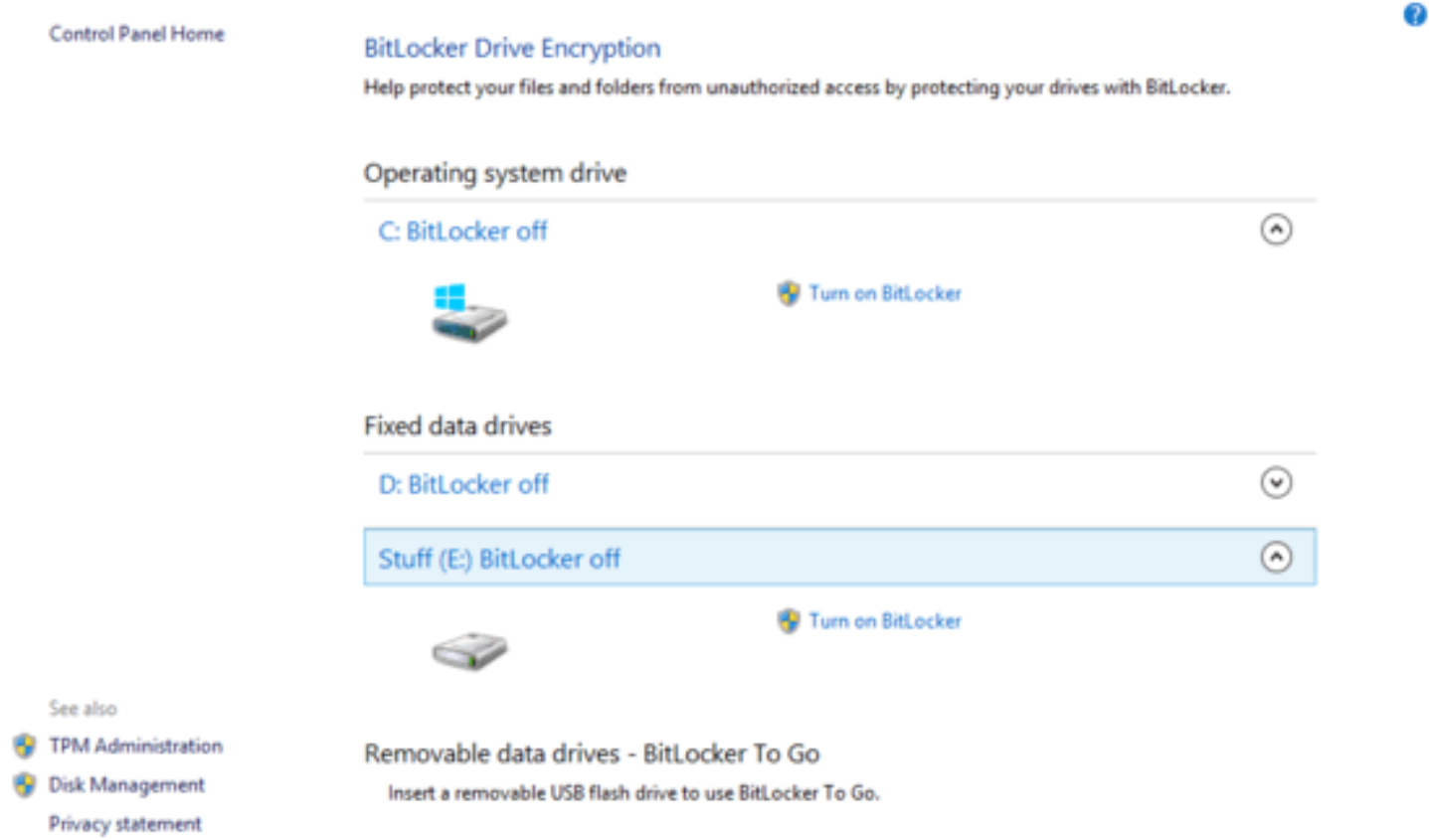
BYOD in the Workplace

- Allow employees to use their own **laptops, smartphones, tablets, or other devices in a work environment**.
- **Monitor Unprotected and Unmanaged Devices.**
- **Data Encryption Capabilities.**
- **Enable Multi Factor Authentication.**
- **Protect data from Ex Employees on data theft.**
- **Enable Flexibility in Work from home with BYOD Policy.**



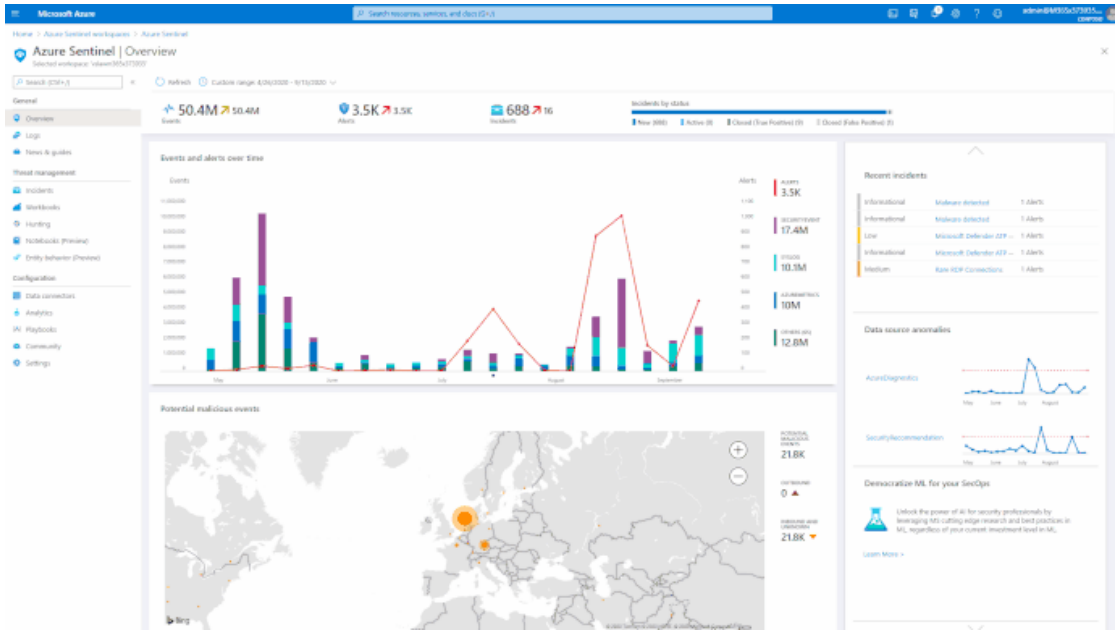
What is BitLocker Encryption?

- Integrates with the **operating system** and addresses the **threats of data theft.**
- BitLocker helps **mitigate unauthorized data access** by enhancing file and system protections.
- It provides an extra level of protection around your files.
- **Hard disk encryption** capability.
- Enables security officers to quickly **determine the compliance state** of individual computers.



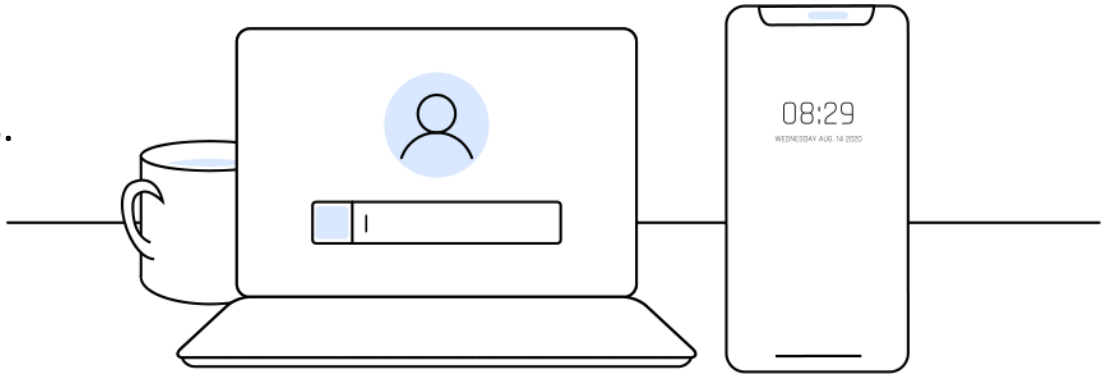
Advanced Threat Protection

- **Anti-phishing checks** incoming messages for indicators that a message might be a phishing attempt.
- Protect against **malicious links in email or Teams** with real time scanning using ATP Safe Links.
- Powerful experiences help **identify, prioritize, and investigate threats.**
- Extensive **incident response** and automation capabilities.
- **Real Time Reports and Insights.**
- **Apply Safe attachment policies to make sure the files coming in are not malicious.**
- **Scan URLs and Links.**



Azure Information Protection

- **Configure policies** to classify, label and protect data based on its sensitivity.
- **Automatically classify emails** and documents based on preset rules.
- **Track activities on shared data** and revoke access if necessary.
- **Share data safely** with co-workers as well as your customers and partners.
- **Protect company's confidential files** with Rights Management
- **Encrypt the files** to a specific set of recipients.
- Remove the **challenge of unauthorized users** viewing sensitive content.



.

Manage Endpoint Security

- Review the **status of all your managed devices.**
- Use the **All devices vi**ew where you can view device compliance from a high level.
- **Deploy security baselines** that establish best practice security configurations for devices.
- **Manage security configurations** on devices through tightly focused policies.
- **Establish device and user requirements** through **compliance policy**.
- **Email gateway** to block phishing and social engineering attempts targeting your employees.
- **Integrated firewall** to block hostile network attacks
- **Proactive web security** to ensure safe browsing on the web

Endpoint security | Overview

- Home
- Dashboard
- All services
- FAVORITES
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Search (Ctrl+/)

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and resp...
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Setup

- Microsoft Defender ATP

Protect and secure devices from one place

Enable, configure, and deploy Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) to help prevent security breaches and gain visibility into your organization's security posture

Microsoft recommended security settings

Assign baselines quickly and securely using our recommended settings.

View Security Baselines

Simplified security policies

Select any of the following categories to jump right in and start securing your devices.

Antivirus
Disk encryption
Firewall
Attack surface reduction
Endpoint detection and response
Account protection

Remediate endpoint weaknesses

Remediate endpoint vulnerabilities reported by Microsoft Defender ATP and Threat and Vulnerability Management.

Enable Microsoft Defender ATP

Computer Solutions East
Business Technology Simplified

Microsoft 365 Security Baseline Service

$3,999
One-Time Fee

- Configure Office ATP
- Configure Intune MDM Enrollment – Computers and Mobile Devices
- Configure AIP Base Policies
- Configure Bitlocker
- Configure Baseline Compliance Policy
- Configure MAM
- Configure 2-Factor Authentication
- Configure One-Drive Redirection – Desktops
- Configure End-Point Security

*Requires M365 Plans
**Up to 25 users

Reach us
NOW!

Computer Solutions East, Inc.
481 Main Street, Suite 100, New Rochelle, NY 10801 | (914) 355-5800 | info@computersolutionseast.com

Computer Solutions East
Business Technology Simplified

Managed Security Services

$ 999.00

Monthly **Recurring**

- Monthly Security Monitoring & Audits
- Threat Management
- IT Compliance Requirements and Support
- Vulnerability Management
- Network Attack Simulator
- Remote Computer Support
- Firewall Management
- Manage End-Point Security

Reach us NOW!

Computer Solutions East, Inc.
481 Main Street, Suite 100, New Rochelle, NY 10801 | (914) 355-5800 | info@computersolutionseast.com

What would You Choose??

License	Cost/month	Cost/Year	Cost for 25 years
Microsoft 365 Business Premium	$20.00	$240.00	**$6,000.00**
Windows 10 pro (One time)			**$200.00**
Microsoft Security Baseline Service (Onetime)			**$3,999.00**
Total Cost for 25 Yrs.			**$10,199.00**
Separate Individual licenses			
Advance Threat Protection			
Plan 1	$2.00	$24.00	$600.00
Plan 2	$5.00	$60.00	$1,500.00
Windows 10 pro (One time)			$200.00
Microsoft 365 Business Premium	$20.00	$240.00	$6,000.00
One drive	$20.00	$240.00	$6,000.00
Microsoft Intune	$6.00	$72.00	$1,800.00
Azure Information Protection	$2.00	$24.00	$600.00
Microsoft Security Baseline Service (Onetime)			**$3,999.00**
Total Cost for 25 Yrs.			**$20,699.00**

Minimum Average Ransomware Attack Recovery Cost

$300,000/Incident

Computer Solutions East
Business Technology Simplified

Computer Solutions East

thank you.

Address

481 Main St #100, New Rochelle, NY 10801,

United States

Schedule a visit!

You can find us Online

https://www.computersolutionseast.com/

https://www.facebook.com/computersolutionseast

https://twitter.com/CSE_Info

Sales

sales@computersolutionseast.com

(914) 355-5800