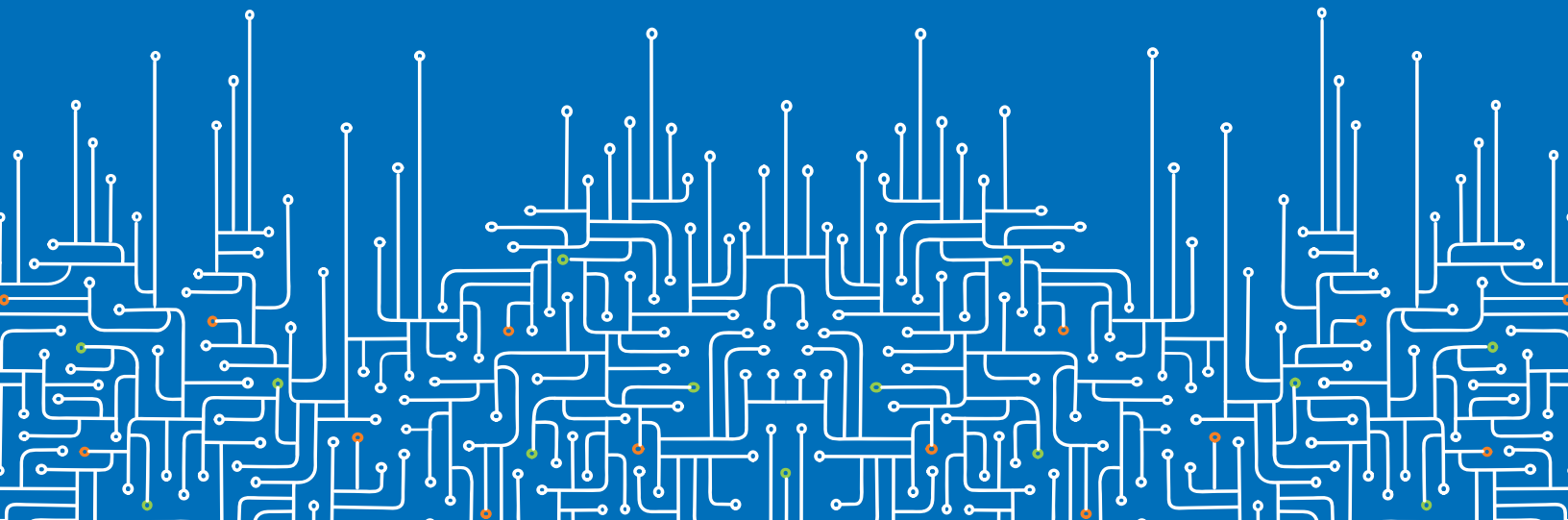
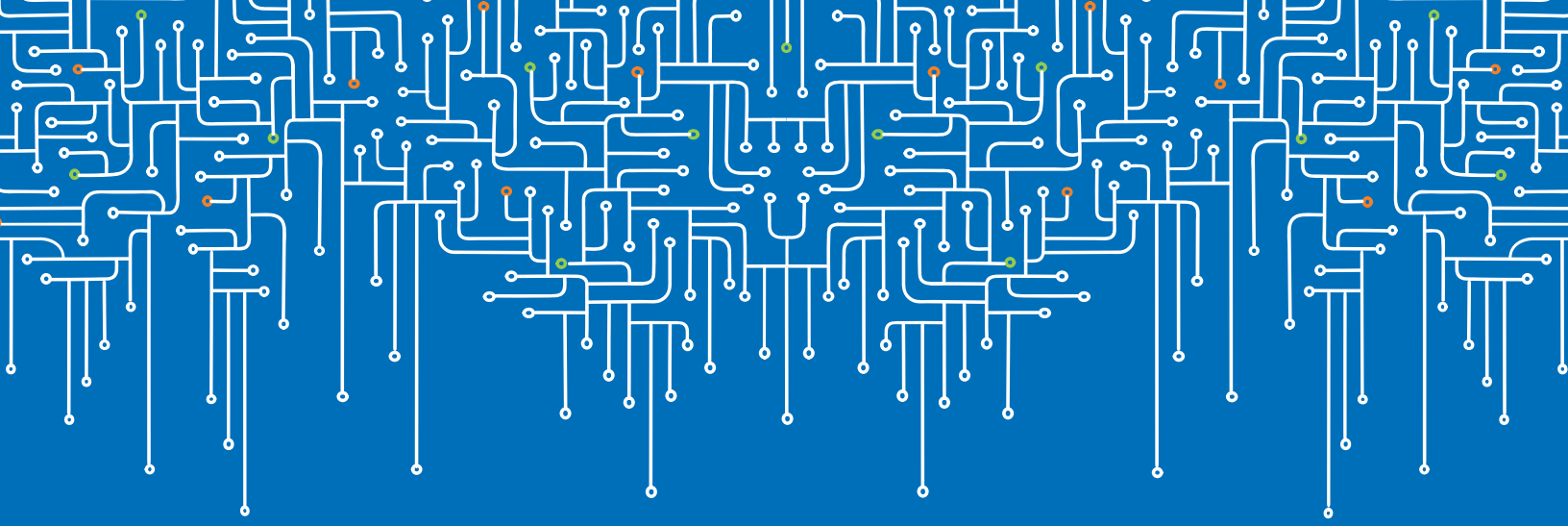
WEBROOT
Smarter Cybersecurity®

GAME CHANGERS:

AI and Machine Learning in Cybersecurity

A U.S. / Japan Comparison





Executive Summary

Artificial intelligence (AI) is a hot topic around the world, with potential benefits ranging from improved productivity to manufacturing efficiencies. The real breakthroughs, however, are being discovered when AI is used for cybersecurity. A recent survey of 400 security professionals in the U.S. and Japan, conducted by Wakefield Research for Webroot, shows a growing acknowledgement that AI and machine learning (ML) are vital to cybersecurity. However, the attitudes, experiences, and expectations of AI by professionals vary by region. Survey results underscore the increasing importance of AI for cybersecurity, especially AI that incorporates continuous ML and contextual analysis to illustrate big-picture trends and reduce false positives.

Key Findings

Key findings in this survey include a view of AI in today's environment, what's working and what isn't, a three-year prospective, and upcoming threats.

AI in Cybersecurity Today

The U.S. is an early adopter of AI for cybersecurity, significantly outpacing its usage in Japan. In fact, 88% of U.S. respondents' companies are using it today, as opposed to just 60% of their Japanese counterparts. Practitioners in both regions feel that AI can play a role in a variety of use cases. They agree that the specific application of AI in machine learning (which allows machines to learn based on inputs, and decide how to behave without being explicitly programmed) is a fundamental ingredient for security.

Fully 40% of the respondents from Japan indicated they are not using AI at all in their cybersecurity efforts, compared to only 13% of American respondents.

Figure 1: Currently using AI in cybersecurity

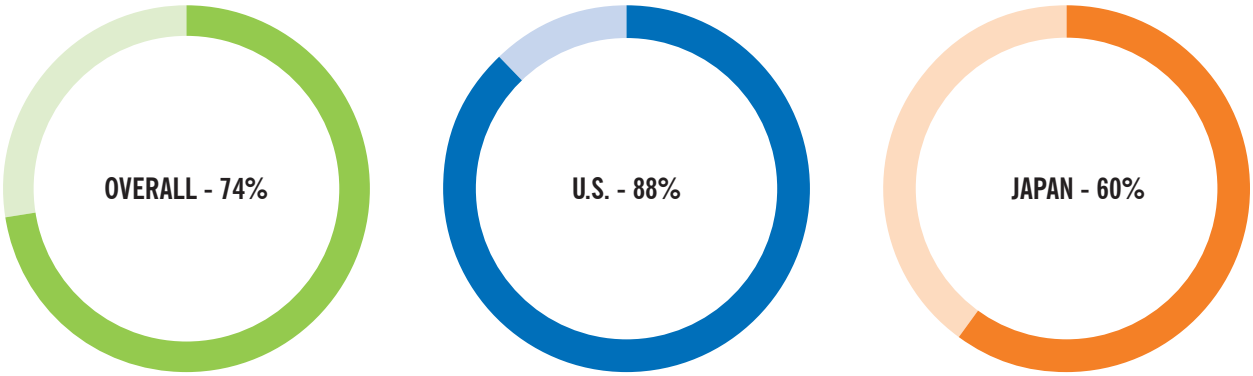


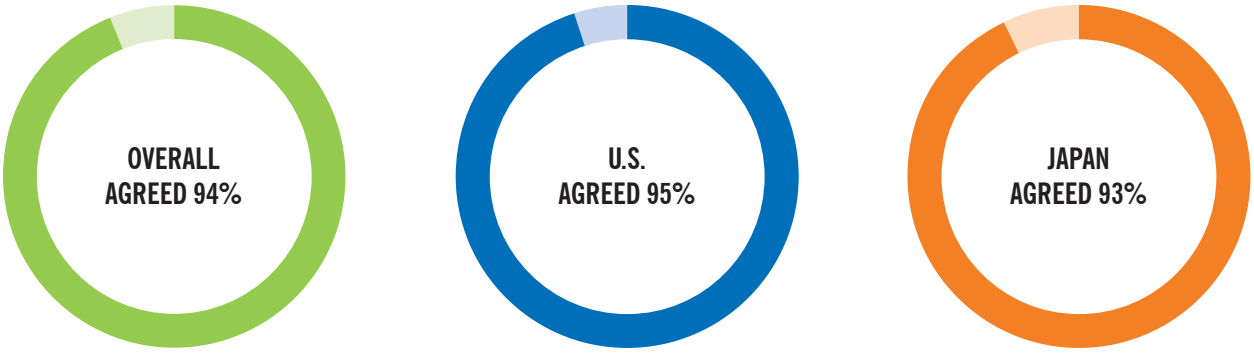
Figure 2: How are you using AI today?

	OVERALL	U.S.	JAPAN
MALWARE DETECTION	60%	76%	44%
MALICIOUS IP BLOCKING	47%	61%	33%
WEBSITE CLASSIFICATION	39%	46%	33%

Here we see a clear trend toward using AI for time-critical threat detection, which focuses on immediately detecting threats when users try to access malicious websites, and discovering malware at the moment it enters a network.

There is almost universal agreement that ML is vitally important for cybersecurity: respondents from both Japan and the U.S. score the importance in the high 90s. Over the past ten years, Webroot has found that the ability to continuously tune machine-learning models and learn from real-world experience allows threat intelligence to fulfill its promise for cybersecurity.

Figure 3: Is machine learning a critical component in a cybersecurity strategy?



What's Working and What Isn't

While there is a clear belief (93%) that AI can improve cybersecurity, individual experiences vary. Respondents from both Japan and the U.S. agree that AI could improve their organizations' cybersecurity, but there are mixed opinions about the reliability of AI solutions.

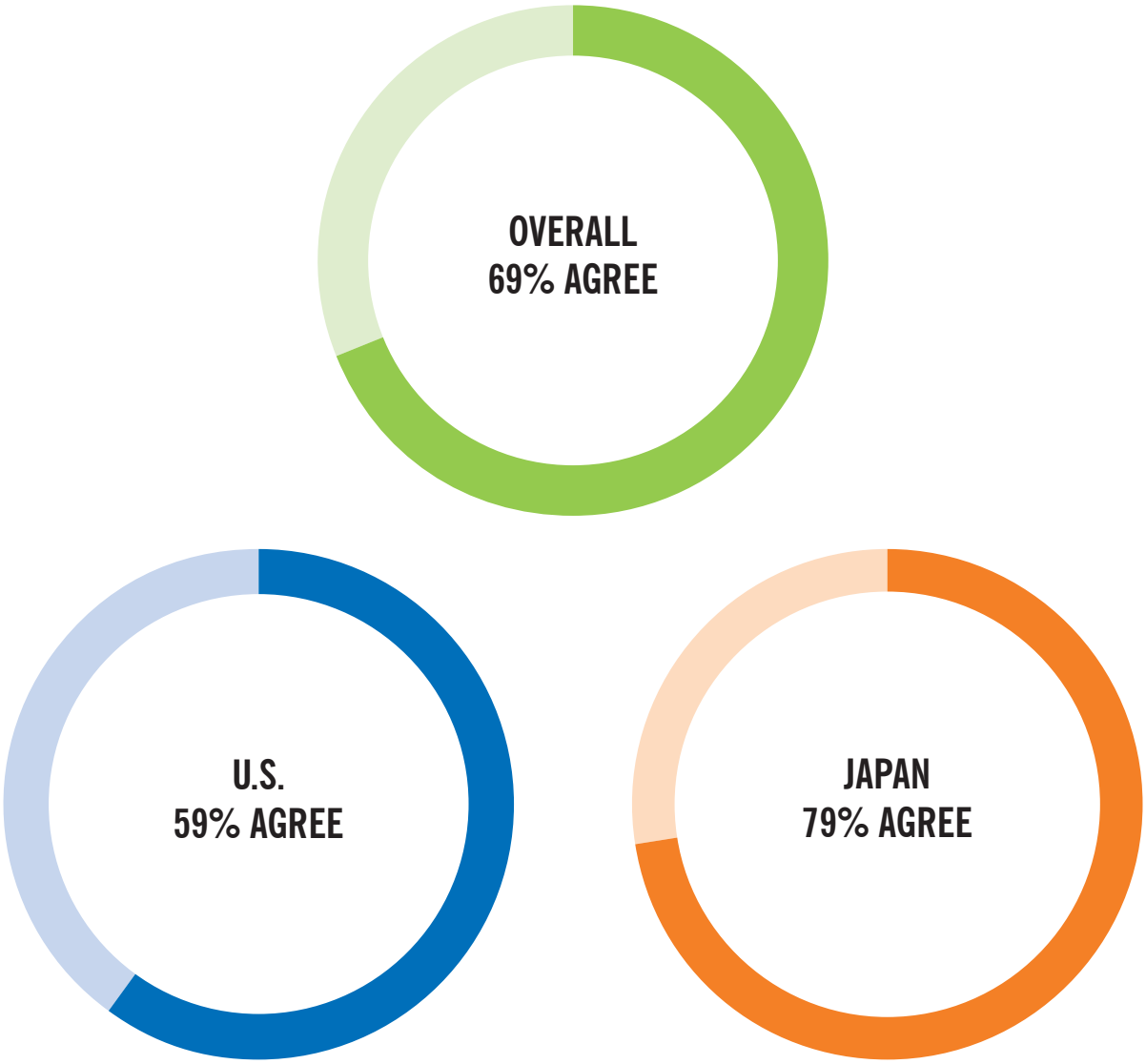
Figure 4 – How do you believe AI could improve your organization's cybersecurity?

	OVERALL	U.S.	JAPAN
HELP IN ANY WAY	93%	99%	88%
IDENTIFY THREATS OTHERWISE MISSED	68%	82%	54%
BETTER CONTROL OR LIMIT DAMAGE OF MALICIOUS ATTACKS	65%	75%	56%
REDUCE FALSE POSITIVES	62%	74%	51%

It is particularly telling that just half of Japan-based respondents believe AI can reduce false positives. This opinion sharply contrasts with the actual experience of Webroot customers, where very low false-positive rates improve productivity by reducing the time their high-value security experts spend chasing down false leads.

One of the most striking findings is that almost 80% of respondents from Japan believe current AI-based cybersecurity solutions are too unreliable to meet the industry's needs. This degree of distrust (perhaps associated with above-mentioned beliefs about false-positive rates) could explain the lower percentage embracing AI today.

Figure 5 – Current AI solutions are unreliable

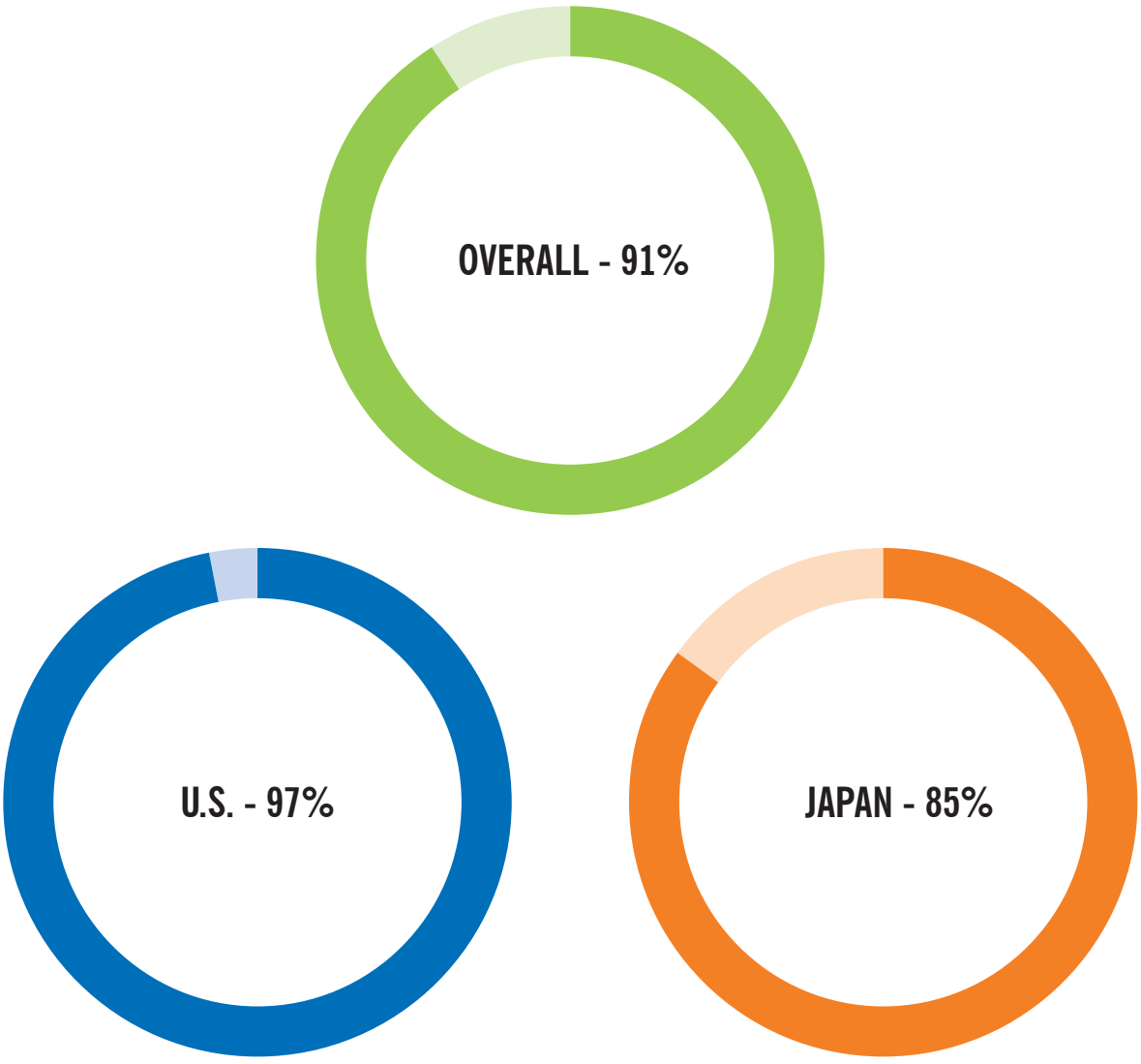


The Three-Year Horizon for AI in Cybersecurity

Security professionals in both regions share a bullish outlook over the next three years. Most (91%) plan to increase their budgets significantly — by 25% on average — for AI and ML tools. Expectations for increased automation via AI run high. In fact, the consensus is, without AI, companies will not be able to safeguard their digital assets in the coming years.

U.S. respondents indicated they are likely (56%) to increase AI budgets by 11-49% over the next three years, while Japanese respondents indicated a 37% likelihood of this level of increase. Average increase: 23-24%

Figure 6 – Plans to increase budget for AI and ML over the next 3 years

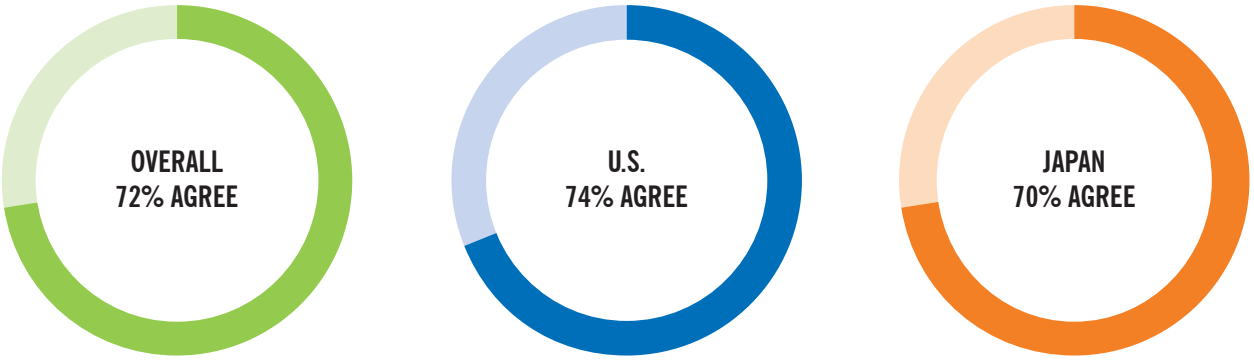


U.S.-based respondents are much more likely (97%) to use AI to automate tasks in the future than their Japan-based counterparts (83%). More than a third (36%) of U.S.-based respondents expect to see one-fourth to one-half of all tasks automated, while in Japan only 19% expect to see such a large boost.

Figure 7 – Percentage of tasks to be automated using AI

RESPONCE	OVERALL	U.S.	JAPAN
0%	10%	4%	17%
1-24%	45%	44%	46%
25-49%	27%	36%	19%
50% OR MORE	18%	17%	19%

Figure 8 – AI will be required for cybersecurity within 3 years



Almost three-quarters of respondents agree that their organizations will become dependent on AI to safeguard their digital assets within the next three years. In the U.S., 26% of respondents agree strongly, while that figure is 22% for Japanese respondents.

AI: Not Just for the Good Guys Anymore

The security cat-and-mouse game continues with AI. As soon as a security innovation comes to market, it is seized by bad actors and becomes part of their arsenal. The vast majority of cybersecurity professionals in both the U.S. and Japan are concerned that hackers will start using AI against them in cyberattacks.

Figure 9 – Hackers will use AI in cyberattacks

Conclusion

AI is only as good as the depth and breadth of its intelligence sources, the maturity and precision of its machine learning, and its contextual analysis. Webroot has a ten-year lead over cybercriminals, with its advanced machine learning capabilities and broad, deep sources of real-world data and cross-domain context, augmented by experienced security analysis. As AI takes center stage, companies need to understand the difference, and select the right AI-based tools to provide effective, proactive cybersecurity that stays a step ahead.

About Webroot

Webroot delivers network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® network behavioral analytics protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at www.webroot.com.

385 Interlocken Crescent Suite 800 Broomfield, Colorado 800.870.8102 webroot.com